UNIVERSITÀ
DI PARMA

Dipartimento di Scienze Matematiche, Fisiche e Informatiche

Corso di Laurea Triennale in Informatica

Cybersecurity, malware e social engineering: rilevamento e prevenzione

Cybersecurity, malware and social engineering: detection and prevention

Candidato:
Tommaso Pellegrini

Relatore:
Prof. Roberto Alfieri

Anno Accademico 2021–2022

ai miei genitori, ai miei amici, alla mia compagna

Indice

Elenco delle figure

Abstract

In questo testo si parla di information security, malware e social engineering. Si mostrano in particolare i loro vettori di attacco, come rilevarli, prevenirli e risolverli. Dalla loro storia, evoluzione e diffusione fino al loro ruolo nel mondo di oggi, si vuole mostrare con precisione come l'utilizzo del social engineering ed i malware siano fortemente interlacciati fra di loro e l'impatto che hanno avuto sulla società e sulle organizzazioni mondiali, sia in passato sia nei giorni odierni. Si pone particolare attenzione anche a come si giunge alla simbiosi tra malware e social engineering. Dopo aver dimostrato molteplici esempi di attacchi di diverso tipo ed i pericoli da loro derivati si fornisce una soluzione agli stessi, oltre a molteplici misure preventive e buone pratiche da utilizzare per proteggere al meglio la propria rete, sia questa quella di un privato od una rete aziendale. Oltre a misure difensive comunemente usate come firewall ed antivirus si presta particolare attenzione ad un determinato tipo di strumento, ovvero quello dei SIEM (security information and event management). Si parla di questi sistemi di sicurezza in modo approfondito, di modo da fornire abbastanza informazioni per capire cosa sono, come operano e quali sono le loro capacità. Il testo si conclude poi con un esempio ben dettagliato di come progettare, installare, configurare e mantenere un sistema come quello sopracitato, come parte integrante del tirocinio svoltosi presso l'Ateneo dell'Università degli studi di Parma in congiunzione fra l'autore ed il team di sicurezza dell'Ateneo.

Introduzione

Quando si parla di hacker ed attacchi informatici, spesso si pensa ad individui od organizzazioni che sfruttando falle informatiche riescono a prendere il controllo di computer, cellulari, bloccare banche dati, accedere ad informazioni segrete e minacce simili. Si tende comunemente ad ignorare il vero operato di un hacker, coprendolo con un velo di mistero spesso alimentato da telegiornali e testate giornalistiche. Nella maggior parte dei casi però non si tratta solamente di vulnerabilità dei sistemi, configurazioni errate o password di default non modificate. Si tratta piuttosto di sfruttare l'anello debole della catena della sicurezza per ottenere quello che si desidera: l'essere umano.

La cybersicurezza è un argomento che negli ultimi anni sta guadagnando sempre più attenzione sia da parte delle aziende che dai privati. Il motivo è banale: il mondo si sta informatizzando a grandissima velocità ed è innegabile che le informazioni personali, anche quelle del singolo individuo quali interessi ed abitudini stiano crescendo di valore a dismisura, per non parlare dell'importanza di informazioni private di una eventuale azienda o organizzazione. Quelle informazioni che, se cadute nelle mani sbagliate, sono sufficienti ad un hacker per prendere il controllo totale di un computer o addirittura un intero sistema.

"Un'azienda potrebbe aver acquistato le migliori tecnologie di sicurezza che i soldi possano comprare, addestrato ogni singolo dipendente talmente bene che quest'ultimo nasconda i suoi dati alla perfezione prima di andare a casa la sera e perfino aver assunto le migliori guardie di vigilanza disponibili. Questa azienda è ancora vulnerabile. Gli impiegati potrebbero seguire le migliori pratiche di sicurezza raccomandate dagli esperti, installare ogni prodotto atto a proteggere dati e password ed essere attenti ad installare sempre l'ultimo aggiornamento o patch che sia. Questi individui sono comunque vulnerabili."[85]

Stando alle statistiche pubblicate da Purplesec, gli attacchi informatici hanno avuto un enorme incremento negli ultimi dieci anni. Dal 2010 con 12.4 milioni di attacchi l'anno, al 2014 con 308.96 milioni fino al 2018 con ben 812.67 milioni. Di questi attacchi, il 98% fa utilizzo, seppur in piccola

parte, del social engineering (o ingegneria sociale).[104] In questo testo viene spiegato cosa sono i malware ed il social engineering, come funzionano, quali sono le tecniche maggiormente diffuse ed utilizzate; si parla della loro storia e della loro evoluzione, di esempi concreti e si termina con l'analisi di possibili metodi per mettere al sicuro le informazioni.

Capitolo 1

malware, la loro storia ed evoluzione

Un malware è un "software che, una volta eseguito, danneggia il funzionamento e la sicurezza del sistema operativo"; il termine deriva dalla contrazione di malicious e software e significa letteralmente "programma malvagio"[118]. Esistono diversi tipi di malware, tra cui il tipo più noto e spesso usato erroneamente per definirli tutti, virus. Nonostante la definizione ci dica che il funzionamento e la sicurezza di una macchina infetta venga danneggiato, i malware possono avere diversi scopi. Alcuni sono stati creati come scherzo, altri hanno compromesso sistemi di enorme dimensione ed importanza. La realtà è che ogni malware ha un obiettivo ben definito, normalmente pensato dal creatore del malware stesso, e questo può variare a seconda del fine dell'autore.

1.1 I primi malware

La diffusione di malware tramite internet (al tempo ARPANET) risale al 1971, data in cui Bob Thomas della BBN ha sviluppato il malware "The Creeper Program"[33]. Data la capacità del malware di creare copie di se stesso, verrà considerato di tipo worm. Nonostante il programma in questione non avesse reali intenzioni malevole e fosse solamente un test per constatare se un programma che si replicasse infinite volte in automatico fosse possibile, viene comunemente considerato come il primo malware creato. Nei successivi anni diversi malware vengono creati seguendo le impronte del loro predecessore come il "The Rabbit Virus" o Wabbit, creato nel 1974 da una fonte sconosciuta, anche questo è un malware di categoria worm che si replica centinaia di volte sulla macchina infettata rallentandone conside-

revolmente le prestazioni [113]. Nel 1975 viene poi creato da John Walker il primo Trojan, chiamato "ANIMAL". Quest'ultimo non era nulla più che uno dei tanti giochi per computer famosi al tempo dove il programma cercava di indovinare a quale animale l'utente stesse pensando. Durante l'installazione di ANIMAL però, veniva installato un secondo programma chiamato PREVADE, che durante l'esecuzione della sua controparte, esamina tutte le directory presenti sulla computer ed installa una nuova copia di ANIMAL in ognuna di esse. Nascosto dentro ad ANIMAL è presente un altro programma che compie azioni non autorizzate dall'utente.[126] Pochi anni più tardi nel 1986 due fratelli di nome Basit e Amjad Farooq Alvi, proprietari di un negozio di computer in Pakistan, crearono il primo virus riconosciuto come tale: "Brain". Il virus aveva come bersaglio i floppy disk da 5.2" e ne sostituiva la partizione di boot con un virus che nonostante non fosse malevolo, conteneva un messaggio di copyright.[64] Tre anni più tardi, nel 1989, venne alla luce il primo ransomware, tipologia di malware destinata a diventare una delle più utilizzate dai cyber criminali per mettere in difficoltà le aziende ed anche una delle più pericolose. Creato dal Dr. Joseph Popp, il trojan di nome "AIDS" fu spedito tramite posta fisica a diversi ricercatori in tutto il mondo dell'omonima malattia, al tempo molto rilevante, utilizzando oltre ventimila floppy disk infetti. Il trojan conteneva inizialmente un questionario riguardo l'AIDS, ma dopo il diciannovesimo reboot i filename di sistema venivano cifrati e nascosti all'utente, al quale veniva chiesta una cifra di 189$ per una licenza annuale o 385$ per una licenza perpetua.[38]

Andando avanti di pochi anni arriviamo nei primi anni '90, dove per la prima volta un malware per computer ottenne una fama tale da farne parlare sia sui giornali che su diversi canali televisivi. E' nel 1991 che viene sviluppato, da una fonte anonima, il virus Michelangelo. Questo virus opera a livello BIOS ed infetta sistemi DOS ma non esegue nessuna chiamata al sistema ne interagisce con il sistema operativo.[128] Nonostante il virus fosse pressoché innocuo, diede vita ad una sorta di isteria di massa essendo programmato per attivarsi il 6 Marzo dello stesso anno, con conseguenze sconosciute al tempo, data del compleanno del famoso pittore. John McAfee stimò che il virus avesse infettato oltre cinque milioni di computer ed i media portarono la storia in prima pagina numerose volte, sensibilizzando per la prima volta le masse riguardo ai malware e le loro possibili conseguenze. In realtà i computer infetti furono poco meno di qualche migliaio, ma Michelangelo rimase il primo malware in grado di far parlare di sé a livello mondiale, quando ancora gli utenti di personal computer erano pochi.[120] A metà degli anni '90 gli utenti di internet erano decisamente aumentati rispetto ai decenni precedenti ed è proprio qui che vediamo i primi attacchi di tipo phishing, quando nel '94

o '95 un gruppo di hacker decise di impersonare il personale di AOL e procedette nel rubare diversi account utente tramite mail fasulle e messaggi sul servizio di messaggistica istantanea di AOL.[97] Vedremo poi come negli anni successivi gli attacchi di tipo phishing, come altri diversi malware, si siano evoluti e abbiano modificato i metodi di creazione e soprattutto diffusione per rimanere al passo coi tempi.

1.2 La diffusione

Il metodo di diffusione dei primi malware era confinato all'utilizzo dell'allora ARPANET, come nel caso di The Creeper Program o dei floppy disk per ANIMAL ed altri. Non esistevano metodi efficaci quanto la distribuzione di dischi infetti o lo sfruttamento di network di compagnie private, ed allora l'utilizzo del social engineering era ancora scarso, salvo negli ultimi anni del '90 dove, come abbiamo visto nel capitolo precedente, iniziarono a presentarsi sporadicamente file Microsoft Words infetti spesso da Trojan e Worms ed i primi attacchi phishing. Un grande passo a favore della diffusione di malware avvenne nel Marzo del 2000, quando apparve per la prima volta LoveLetter. Creato da Onel de Guzman, il worm si presentava nella casella di posta elettronica non come documento Word infetto, ma come file VBS, un linguaggio di scripting il cui codice poteva venire eseguito direttamente da Windows come OS o da Internet Explorer. Una volta aperto il malware era disegnato per trovare ogni singolo file presente sul sistema e sovrascriverlo con una copia di se stesso, un semplice file di testo contenente la frase "I LOVE YOU".

Le copie del file erano poi inviate automaticamente a tutti i contatti email dell'utente infetto. [137] Nonostante si tratti di un malware semplice e diretto, gli utenti ancora incauti non erano abituati a dover diffidare dell' allegato di un'email inaspettata. Questo errore viene ripetuto molto spesso ancora oggi, ed è così che in una grande quantità di casi gli hacker riescono ad ottenere l'accesso a dati, computer o sistemi. Statistiche pubblicate dal Kaspersky Virus Lab mostrano che nel 2001 gli attacchi informatici consistenti in malware allegati a mail, oltre che essere incrementati del 5% dall'anno precedente, risultano essere quasi il 90% degli incidenti causati da malware in quell'anno[32]. L'apertura di un file malevolo come allegato di una mail è il perfetto esempio di phishing (se ne parlerà in dettaglio più avanti), che oltre ad essere uno degli esempi più classici del social engineering, è ancora vastamente utilizzato insieme al suo corrispettivo tramite SMS o notifica push. E' infatti nei primi anni del nuovo millennio che vediamo come la diffusione di malware si fosse ampliata anche a dispositivi mobili, usando nuove

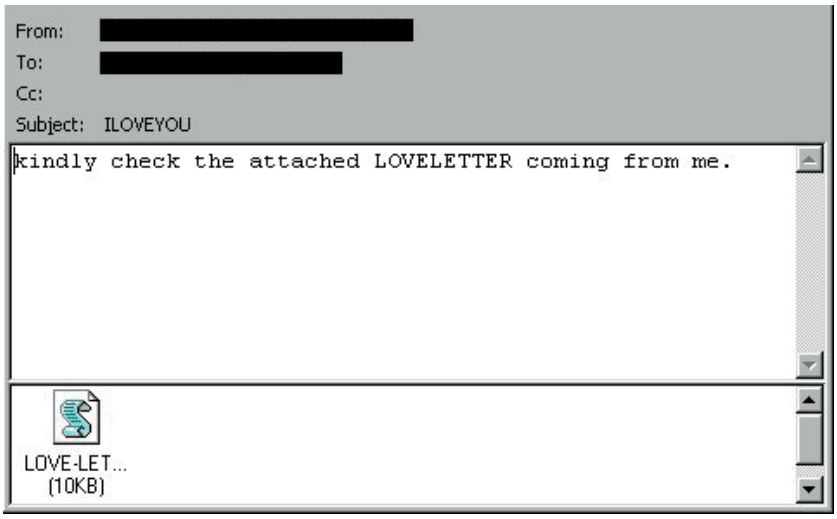


Figura 1.1: Una mail contenente il malware I LOVE YOU. Fonte: Kaspersky

tecnologie, ancora giovani e con diversi problemi di sicurezza. Nel 2004 venne alla luce Cabir, il primo malware di tipo worm in grado di infettare telefoni cellulari basati su OS Symbian, usato principalmente da Nokia. Il worm era in grado di riprodursi spedendo una copia di se stesso utilizzando il bluetooth integrato nei telefoni cellulari o tramite MMS. A differenza di molti altri primi malware, Cabir fu creato come "proof of concept" e al posto di distribuirlo tra i privati venne subito mandato a diverse ditte di cybersecurity per poter trovare una soluzione al problema.[136] E' evidente come al sorgere di nuovi metodi per collegare dispositivi fra loro, dall'ArpaNet, al bluetooth, fino ai dispositivi di ultima generazione per le smart home, nascano anche nuovi metodi per distribuire i malware.

1.3 L'evoluzione

L'anno 2001 non è solamente l'anno che vide l'ascesa al successo del phishing, ma anche l'anno in cui altre nuove forme di diffusione di malware nacquero. Prima di allora la stragrande maggioranza dei malware diffusi in quegli anni, spesso worms e trojan, sfruttavano gravi vulnerabilità di programmi ampiamente utilizzati in ambito lavorativo come Microsoft Word, Outlook ed altri e venivano distribuiti via mail, ma per essere infettati si doveva compiere un grosso errore, spesso evitabile: scaricare il malware. Da quel momento però non c'era più bisogno di scaricare qualche strano file mandato da un presunto collega di lavoro. Bastava visitare un sito internet infetto per venire infettati

di conseguenza. Le pagine web venivano sostituite con controparti malevoli, contenenti codice che sfruttando falle di MS Internet Explorer, poteva venire eseguito direttamente dal client. [70] Un altro passo per il social engineering avvenne in contemporanea, quando diversi siti internet iniziarono a fornire versioni gratuite di programmi a pagamento che venivano però accompagnate da un malware. Nuovamente, si vede come sfruttare l'ingenuità ed i difetti della personalità umana porti un grandissimo vantaggio. Offrire gratuitamente un qualcosa di costoso si rivela un'offerta difficile da rifiutare. Presi dall'avarizia e dalla curiosità, sono milioni gli utenti che infettano le loro macchine ogni anno.

Nonostante i primi anni del 2000 videro una grande evoluzione di sistemi antivirus, la quantità di malware creata e condivisa continuava ad aumentare, dimostrando come l'esplosione dell'internet ed il suo sempre più semplice accesso nel mondo portava con sé i suoi rischi e pericoli per i suoi ancora ineducati utenti. Un ultimo strumento che vide un enorme sfruttamento da parte degli hacker volto a diffondere malware fù la messaggistica istantanea, o "IM". Dalle IRC che fecero i loro primi passi nel 1988 ad AIM di AOL, MSN di Microsoft, i servizi di messaggistica istantanea guadagnarono milioni di utenti fino a superare i 300 milioni di utenti nel 2005.[71] Data la tale popolarità e il vasto impiego anche da parte di business (si pensi a Skype per esempio), le piattaforme IM diventarono bersaglio e fonte di numerosi attacchi informatici. Solamente nel primo quarto del 2004, il numero di attacchi volti alle maggiori piattaforme IM vedono un aumento del 400%. Al posto di file word infetti però, si vede un anche un enorme incremento nell'utilizzo del social engineering, visto che la stragrande maggioranza di questi attacchi vengono perpetrati con lo stesso modus operandi usato nel phishing. [102] I numeri che abbiamo visto finora sono destinati ad aumentare, come le vittime del phishing ed in generale del social engineering.

1.4 L'alba della cyber-criminalità

Abbiamo visto come tra la creazione di una nuova tecnologia ed un suo possibile utilizzo a scopo malevole o fraudolento passi davvero poco tempo. Non bisogna confondere però i primi malware ed i primi attori malevoli come attività di criminalità organizzata. Nonostante diversi malware nacquero con lo scopo di guadagnare denaro in modo illecito, rimangono per lo più operazioni compiute da singoli o piccoli gruppi di individui. Ma come in ogni cosa, quando certe novità vengono portate all'attenzione di molti, anche i malware e l'internet attirarono diversi gruppi criminali che videro una nuova potenziale fonte di guadagno a rischio nettamente più basso rispetto alle at-

tività criminali compiute di persona. Studi dimostrano come diversi gruppi di criminalità organizzata sfruttarono queste nuove tecnologie per inserirsi in giri di truffe e gioco d'azzardo online.[127] Per esempio, si hanno prove di come nel 2016 diversi membri appartenenti alla Camorra e 'Ndrangheta furono arrestati a causa di un giro di scommesse online illegali.[94] Sono inoltre presenti diversi casi in cui gruppi criminali abbiano iniziato a compiere cyber crimini per poter facilitare i lori crimini offline, come un gruppo di trafficanti di droga che nei primi anni del 2010 assoldò un gruppo di hacker per ottenere l'accesso alle infrastrutture informatiche del porto di Antwerp in Belgio, con lo scopo di ottenere informazioni relative ai containers, per poter spedire carichi di droga in modo non sospetto.[10] E' quindi facile immaginare come diversi gruppi criminali possano nascere solo per operare online o trasferire le loro attività completamente o parzialmente online. Nonostante diversi di questi gruppi si siano formati online, ricerche relative alla creazione e lo sviluppo di reti di cyber-criminalità organizzata mostrano come le aree geografiche e i contatti offline giochino un ruolo estremamente importante nella loro formazione ed espansione.[124] Sono stati infatti trovate diverse zone calde e centri di ritrovo per gruppi di criminalità organizzata online nell'est europa[2], ed è stato inoltre rivelato dall'Europol come la maggior parte delle truffe che utilizzano social engineering rivolte verso i paesi europei siano principalmente eseguite da gruppi criminali residenti nelle zone dell'ovest dell'Africa.[1]

Un'altro strumento che ha favorito la creazione di tali gruppi è sicuramente il cosiddetto Dark Web, in forte congiunzione con la nascita della prima criptovaluta, il BitCoin. Il Dark Web è quella parte dell'internet il cui contenuto non è indicizzato dai motori di ricerca a cui siamo abituati, ovvero Google, Bing, Yahoo etc.[50] Si tratta di una collettiva di siti internet accessibili solamente utilizzando web browser specializzati, tra cui il più famoso Tor. Il dark web non nasce però con un intento criminale, in quanto la sua origine è quella di creare una rete criptata e completamente anonima con cui le spie statunitensi potessero comunicare tra loro proteggendo i contenuti sensitivi che gli attori si scambiavano.[69] Quando però nel 2002 Tor, un browser privato per la navigazione, venne rilasciato al mondo intero tutti poterono usufruire dei servizi di anonimizzazione di cui abbiamo parlato.[65] Mentre alcuni utenti lo usano per evadere le censure governative, è diventato molto conosciuto per essere utilizzato per compiere attività altamente illegali. Dalla compravendita di enormi banche dati rubate da aziende private e governative, alla vendita e spedizione di grandi quantità di droga ed armi online fino ad il suo utilizzo per assoldare hacker o addirittura gruppi di assassini, il Dark Web diviene ad oggi una delle reti più utilizzate per il

compimento di attività illegali, sia da singoli che grandi gruppi di criminalità organizzata.[30]

1.5 Oggi

Vediamo ora un po' di statistica: Il 92% dei malware viene recapitato via mail. I malware e le varianti per dispositivi mobili sono in crescita, con aumento del 54% solamente nel 2018. Nell'ultimo anno i malware per MacOS sono aumentati del 165%. Tutt'ora i trojan sono circa il 50% dei malware presenti in rete. Più di 18 milioni di siti internet vengono infettati da mal-

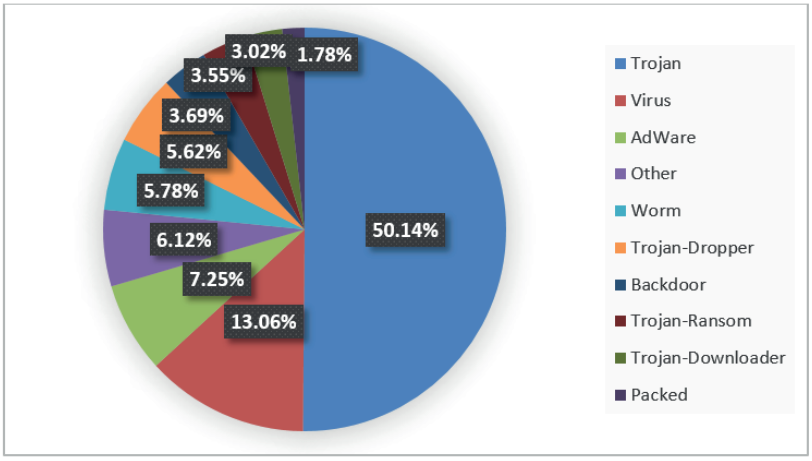


Figura 1.2: Statistiche sul tipo di malware. Fonte: Kaspersky

ware ogni settimana. Il 90% delle istituzioni finanziarie ha riportato almeno un attacco informatico nel 2018. Come detto in precedenza, il 95% degli attacchi informatici fanno utilizzo del social engineering.[103] Riprenderemo più avanti questo dato importante. Una menzione necessaria va inoltre ad un tipo di malware che negli ultimi anni ha avuto un incremento spaventoso del 358% nel 2018[80], il ransomware: in grado di criptare i dati dell'utente e di prevenirne l'accesso da parte dell'utente minacciandone la distruzione previo conto alla rovescia a meno che non venga pagato un riscatto, spesso non rintracciabile perché pagato tramite criptovalute.[123]. I numeri non mentono, le minacce informatiche sono aumentate spropositatamente negli ultimi 20 anni e sono destinate ad aumentare. Per questo motivo è importante formare gli utenti, dal privato al dipendente statale, riguardo la possibilità di essere vittima di questi attacchi nella speranza di portare gli utenti ad un livello di conoscenza tale da poter evitare situazioni di crisi.

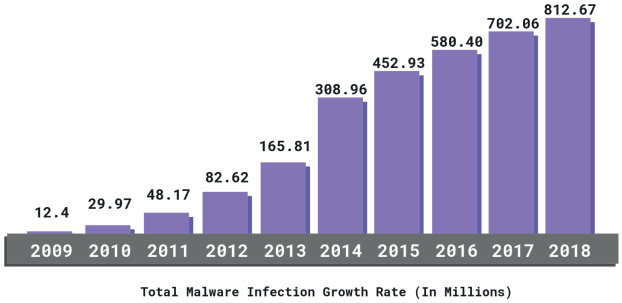


Figura 1.3: La crescità negli anni dei malware. Fonte: Purplesec

1.6 I tipi di malware

Segue una lista che spiega nello specifico i tipi di malware più conosciuti ed utilizzati ad oggi. Tratteremo più avanti tipi di attacco non riconducibili direttamente a malware, ma quanto più a vettori di attacco (DDoS, iniezioni SQL etc.), attacchi alle password (come brute forcing) e Man in the Middle (o MitM), molto importanti nel social engineering, ma non appartenenti alla categoria malware. Si vuole definire una linea di separazione netta fra un malware ed un attacco ad una infrastruttura informatica. La lista seguente non contiene ogni singolo tipo di malware esistente, ma è sufficientemente corposa per dare un'idea generale delle più grandi categorie presenti.

Virus: è un tipo di programma malevolo che una volta eseguito inizia a replicarsi modificando altri programmi presenti dentro alla macchina infetta. Di norma i virus hanno bisogno di un host program, un programma base da cui iniziare l'infezione, per poi diffondersi negli altri. I virus possono poi far parte di altre categorie di malware, diventando di fatto anche keylogger, trojan o ransomware.

Trojan: un trojan horse è un tipo di malware che rispecchia il comportamento del cavallo usato dai greci: fingendosi un programma legittimo, tramite social engineering gli utenti vengono ingannati ad eseguirlo. La payload del trojan può essere qualsiasi, spesso un backdoor, e vengono di norma usati per rubare informazioni. A differenza di worm e virus, i trojan non iniettano del codice malevolo nei file né cercano di replicarsi.

Worm: più simili ai virus, i worm cercano di infettare altri computer duplicandosi mentre rimangono attivi anche sulle macchine infettate in precedenza. I worm usano principalmente la rete per diffondersi, sfruttando vulnerabilità per poi arrivare alla prossima vittima. Come i virus, an-

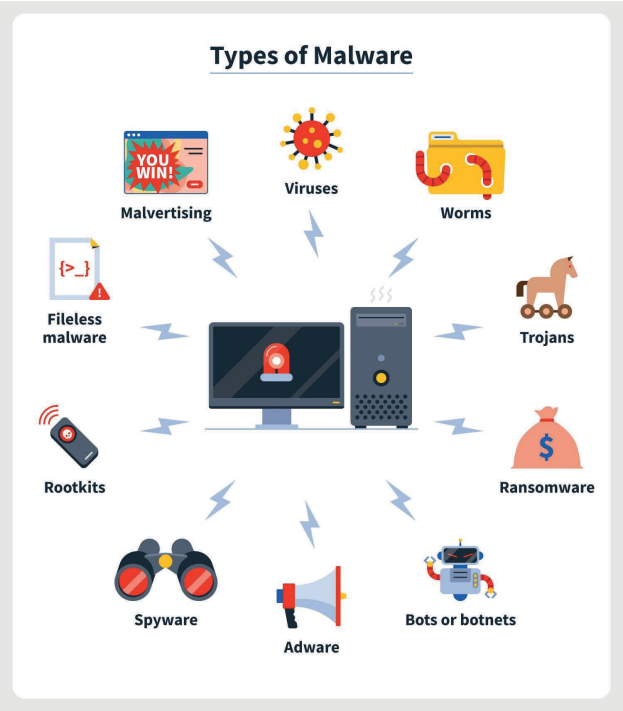


Figura 1.4: Diversi tipi di malware. Fonte: Norton

che i worm possono prendere delle sottoforme: possono creare botnet, keylogger e molto altro.

Ransomware: sono una forma di malware disegnata per criptare e negare l'accesso ai dati della macchina infetta finché un riscatto non viene pagato. Spesso associato con un countdown, le vittime di ransomware vengono spesso invitate ad eseguire il pagamento sotto forma di criptovalute, estremamente difficili da rintracciare.

Rootkit: tra i più pericolosi, sono un insieme di malware atto a prendere il controllo totale del sistema mascherandosi come programmi legittimi già esistenti sulla macchina. Possono essere installati manualmente post bruteforce, tramite phishing o con attacchi diretti a vulnerabilità. Particolarmente difficili da rilevare e quasi impossibili da rimuovere, alcuni rootkit possono installarsi nel kernel o nei firmware, richiedendo la sostituzione di parti hardware della macchina per poterli rimuovere.

Keylogger: semplici malware che tengono traccia di ogni tasto battuto sulla macchina infetta per poi spedire i log contenenti i dati all'hacker. Anch'es-

si spesso trasmessi tramite social engineering risultano particolarmente pericolosi per il possibile furto di dati, password, info bancarie etcetera.

Grayware: termine coniato nel settembre 2004, i grayware descrivono un tipo di malware che non ha particolari intenzioni malevole ma che peggiora le performance della macchina infetta. Sono una categoria più grande di malware che allude per esempio ad adware e spyware.

Fileless malware: come intuibile dal nome, sono tipi di malware che utilizzano programmi legittimi per infettare una macchina, ma non lasciano tracce sul sistema e non scrivono sul disco rigido. Essendo caricati solo su memorie volatili come la RAM, sono difficili da rilevare e muoiono al reboot della macchina. Possono essere particolarmente tediosi perché una volta svaniti lasciano poche o nessuna traccia utile agli investigatori forensi.

Adware: sono un tipo di grayware creati per produrre annunci pubblicitari indesiderati spesso su browser, desktop o popup. Seppur non pericolosi, risultano essere particolarmente fastidiosi e possibilmente complicati da rimuovere se installati fra i registri di sistema. Gli adware risultano essere il tipo di malware meno pericoloso ma più proficuo per gli hacker, essendo capaci di generare reddito semplicemente mostrando annunci. Spesso vengono caricati da altri programmi durante la fase di installazione se non si presta attenzione. Anche questa risulta essere una forma di social engineering.

Spyware: sono malware che raccolgono informazioni riguardo una persona od un'organizzazione senza che questi ne siano a conoscenza e ne spediscono i risultati all'hacker senza permesso. Spesso l'obiettivo è poter vendere i dati raccolti a terzi, ma anche rubare dati bancari o personali. Di norma, non venendo installati nei firmware o nel kernel, una volta scoperti risultano semplici da rimuovere.

Backdoors: si tratta di un metodo nascosto per bypassare l'autenticazione in un computer, prodotto o embedded device (routers etc.). I backdoor vengono comunemente usati per stabilire un accesso remoto ad un computer o accedere a file criptati e da lì può essere usato per accedere, corrompere, cancellare o trasferire dati sensitivi. Possono far parte di un programma o essere installati direttamente nei firmware o sistemi operativi.

Cryptojacking: è un tipo di malware appartenente ai grayware. Similmente ad uno spyware o adware, sfrutta la potenza computazionale della macchina che viene infettata per fare mining di criptovalute senza che l'utente

ne sia a conoscenza. Le prestazioni della macchina subiscono notevoli rallentamenti e la longevità delle componenti hardware può diminuire molto in fretta.

Capitolo 2

Il social Engineering

Con il termine "social engineering" si intende la manipolazione psicologica attraverso trucchi o inganni, volta a far compiere alle persone particolari azioni o rivelare informazioni confidenziali.[29] Lo scopo è spesso quello della raccolta di dati o credenziali, usati poi per accedere ad un computer o un intero sistema a scopo di frode. E' importante notare però che l'accezione del termine non deve per forza essere negativa, in quanto il social engineering è ampiamente utilizzato non solo da criminali informatici ma anche dalle forze dell'ordine, investigatori privati, trova persone e giornalisti. Vedremo più avanti nel testo come il social engineering sia una pratica necessaria, nel suo bene e nel suo male, utilizzata vastamente da agenzie che da sempre danno la caccia al crimine informatico e non solo, dai servizi segreti italiani all'FBI ed Interpol. [27][26]

2.1 Introduzione al social engineering

Ad oggi le tecniche fornite dal social engineering sono le più comunemente usate per commettere crimini informatici tramite l'intrusione e conseguente infezione di computer ed infrastrutture IT.[4] Essendo gli attacchi del social engineering composti da una combinazione di interazioni sociali ed exploit di tecnologie, gli esperti di cybersecurity di compagnie private e del governo faticano a realizzare contromisure efficaci. Il fattore umano rimane la vulnerabilità più difficile da risolvere, dato che non basta una semplice patch come in un sistema software. Nella stragrande maggioranza dei casi, l'hacker o attaccante non si trova mai faccia a faccia con la vittima, anche se questa situazione rimane possibile quando vengono perpetrate tecniche di attacco attive, di cui discuteremo più avanti. E' inoltre importante notare che spesso le vittime del social engineering non sono preparate correttamente ad affrontare

simili minacce e questa è spesso la causa del loro successo.[7] Bersagli comuni come impiegati di aziende potrebbero essere attaccati da un hacker senza che nemmeno se ne rendano conto, venendone a conoscenza ormai a danno fatto. Queste tecniche di attacco hanno una grande varietà di applicazione essendo indipendenti dal tipo di sistema operativo, software o piattaforma utilizzati. Che si tratti di un sistema operativo Windows, MacOS o Linux, la parte più vulnerabile rimane come detto in precedenza l'utente, ed è per questo che diventa automaticamente il bersaglio di maggiore importanza. In casi simili sia antivirus che sistemi aggiornati all'ultima versione non sono in grado di fornire un'adeguata protezione. Nella information security, come nella sicurezza informatica, ogni singolo settore è esposto a rischi quando si parla di social engineering. Per quanto al giorno d'oggi si parli tanto di intelligenza artificiale e dei rischi che questa comporta, un ipotetico sistema protetto unicamente da una IA, dove anche l'accesso admin di più alto livello è previo autorizzazione della suddetta, sarebbe il sistema più sicuro da attacchi relativi al Social Engineering. Una intelligenza artificiale, se programmata in modo tale, non disporrebbe di tutte quelle vulnerabilità comportamentali comuni dell'essere umano.[46] Questo, e molto altro, sono l'arte del social engineering. L'arte del soggiogare, di sfruttare banali dettagli e sfumature a proprio vantaggio.

Figura 2.1: Tattiche comunemente usate nel social engineering. Fonte: Norton

2.2 Cenni storici

La storia della pratica del social engineering può essere interpretata secondo due diverse chiavi di lettura. Nonostante la tecnologia ed i computer si siano evoluti in modo tale da generare il concetto social engineering basato sulla InfoSec solamente negli ultimi decenni, le persone hanno usato i principi della psicologia umana per manipolare gli altri per centinaia di anni.[84] Il social engineering è una pratica antica quanto l'alba dell'umanità. Da quando esistono informazioni ambite, esistono anche persone che vogliono sfruttarle. Basti pensare alla mitologia greca dove Ulisse, dopo una guerra lunga dieci anni contro i troiani, cambiò tattica e usando il famoso cavallo di Troia (da cui il malware origina il suo nome) riuscì a conquistare la città dall'interno, terminando la guerra.

Il termine "social engineering" è stato coniato per la prima volta dall'industriale olandese J.C. Van Marken nel 1984.[79] Van Marken suggerì che fossero necessari degli specialisti di "problemi umani", tanto quanto ci fosse il bisogno degli ingegneri per occuparsi di tutti quei problemi tecnici. Nel 1911, ancora prima che Van Marken coniasse il termine, Edward L. Earp usò il termine "Social Engineer" (ingegnere sociale) come termine per incoraggiare le persone a gestire le relazioni sociali similmente al modo in cui ci si approccia ad una macchina.[28] E' quindi solo dai tempi moderni che il social engineering diventa una referenza (e guadagna la sua definizione ufficiale) al processo di manipolazione delle presone per ottenere informazioni, solitamente seguito da un attacco informatico. Prima di allora l'ingegneria sociale usava molti degli stessi vettori d'attacco che si usano ad oggi, ma con la mancanza di un evoluzione (e tanti nuovi metodi) che sarebbe arrivata da lì a poco con l'introduzione di telefoni nelle case del comune cittadino, email e poi sms e via dicendo. Essendo gli attacchi di ingegneria sociale spesso condotti su dispositivi complicati ed interconnessi, è difficile tracciare una linea evolutiva definita dagli anni '90 ai primi anni del 2000. Inoltre molti di questi attacchi vengono condotti furtivamente e sono difficilmente rivelati, anche dopo essere stati portati a termine. Questo comporta una non consapevolezza dell'attacco da parte della vittima e/o azienda, che potrebbe scoprirlo in futuro come rimanerne totalmente ignara per anni.

2.3 Ingegneri sociali famosi

Per quanto sia complicato tenere traccia dei vari casi di social engineering, siamo a conoscenza di quelli che vengono considerati i primi casi del social engineering nell'era dei computer e di internet. Nel 1982 un giovane di quin-

dici anni creò quello che può essere registrato come uno dei primi casi di social engineering con lo scopo di diffondere un virus. "Elk Cloner" era un virus di tipo worm creato per scherzo, ma il fatto che si diffondesse tramite floppy disk con il pretesto di essere un videogame lo classifica come uno dei primi casi di social engineering mai registrati.[43] Nonostante questo giovane sia ancora oggi senza nome, possiamo elencare quelli che invece vengono considerati i primi ingegneri sociali dell'era moderna: Frank Abagnale Jr. è un consulente di cybersecurity conosciuto per il suo passato da forgiatore di assegni, impostore e truffatore. Impersonando varie identità fra cui pilota, medico, dottore, avvocato e molte altre è famoso per essere riuscito ad evadere dalla custodia della polizia ben due volte, tutto ciò prima di compiere 22 anni. Dopo anni di fuga ed un eventuale arresto, Abagnale iniziò a lavorare per l'FBI come agente sotto copertura.[98]

Susan Headly era una "phreak" ovvero phone hacker, attiva fra gli anni '70 e '80. E' conosciuta per le sue grandi doti di ingegneria sociale, che le hanno permesso di brecciare diversi sistemi informatici militari e addirittura oltrepassare diversi checkpoint della base militare americana Area 51.[34] In passato ha inoltre dichiarato di essere riuscita ad ottenere informazioni rilevanti sugli orari di lavoro dei siti di lancio di missili balistici intercontinentali[5] e, possibilmente, altre informazioni relative di grande importanza.

In tempi più recenti, James Linton, è un hacker britannico e ingegnere sociale che nel 2017 fu in grado di utilizzare la OSINT (open source intelligence) e diversi attacchi phishing per truffare diversi bersagli di grande importanza, tra cui diversi CEOs di banche nazionali molto importanti, oltre che diversi membri della amministrazione Trump.[74]

Unendo passato e presente, possiamo poi parlare di quello che viene considerato il più grande ingegnere sociale di sempre: Kevin Mitnick. Nato nel 1963 in California, Mitnick è un consulente di cybersecurity, autore e hacker. Nella metà degli anni '90 però, era l'hacker più ricercato del mondo.[68] Alla giovane età di 12 anni Mitnick convinse un autista di autobus a farsi spiegare dove poter comprare una pinza perforatrice per un "progetto scolastico". Dopo aver trovato un cedolino di trasferimento inutilizzato in una discarica vicina ai garage di una compagnia di autobus, fu in grado di viaggiare per molto tempo gratuitamente in tutta Los Angeles.[86] All'età di 16 anni Mitnick riuscì a penetrare la rete interna della società Digital Equipment Corporation e ne copiò il software, crimine per cui fu arrestato e condannato a dodici mesi di reclusione. Verso la fine del suo rilascio supervisionato, Mitnick riuscì ad inserirsi nei sistemi della Pacific Bell, una sussidiaria di AT&T. Dopo che un mandato di arresto fu rilasciato, Mitnick iniziò una fuga durata

due anni e mezzo. Durante il periodo di fuga Mitnick riuscì ad introdursi nei sistemi informatici di oltre quaranta aziende estremamente importanti, non per scopi economici ma solamente per la sfida.[62]

2.4 Statistiche, il social engineering nel mondo di oggi

Come abbiamo detto, il social engineering non si appoggia tanto sull'hacking dei computer, quanto più sulla manipolazione delle persone. Nonostante questo il social engineering gioca un ruolo fondamentale nella riuscita di un attacco hacker. Al giorno d'oggi, il 98% degli attacchi hacker utilizza una qualche tecnica di social engineering. Una volta ottenuta la fiducia, seguono poi gli altri attacchi. Che sia furto d'identità, di credenziali o distribuzione di malware, è il social engineering che funge da ponte.[105] In media, durante un anno lavorativo, una determinata organizzazione viene normalmente presa di mira da attacchi di social engineering oltre 700 volte. Considerando che di norma in un anno i giorni lavorativi sono 260, questo vuol dire che avvengono 2.7 attacchi al giorno.[48] Sul fronte della violazione delle banche dati il social engineering è l'approccio più utilizzato in assoluto per accedere ai sistemi bersaglio. Spesso è più facile ingannare un dipendente di un'azienda a farsi dare le credenziali di accesso che utilizzare un attacco brute force. Il risultato è che tra il 70% e il 90% delle violazioni di banche dati avviene tramite social engineering.[49] Tornando a parlare del phishing, tecnica preferita del social engineering, questa tecnica viene usata il 25% delle volte in cui avviene una violazione di una banca dati tramite social engineering.[125] Sappiamo inoltre che nel 2021 approssimativamente l'83% delle organizzazioni negli Stati Uniti sono state vittima di almeno un attacco phishing, riuscito, via mail; si tratta di un incremento del 43% rispetto al 2020,[99] anno in cui Google ha eliminato dai propri risultati di ricerca ben 2.1 milioni di finte pagine web sospette di phishing.[100] Purtroppo, nonostante la grande importanza dell'argomento, solamente il 27% delle compagnie fornisce ai dipendenti un addestramento su come riconoscere determinati tipi di phishing e come proteggere dati sensibili.[15]

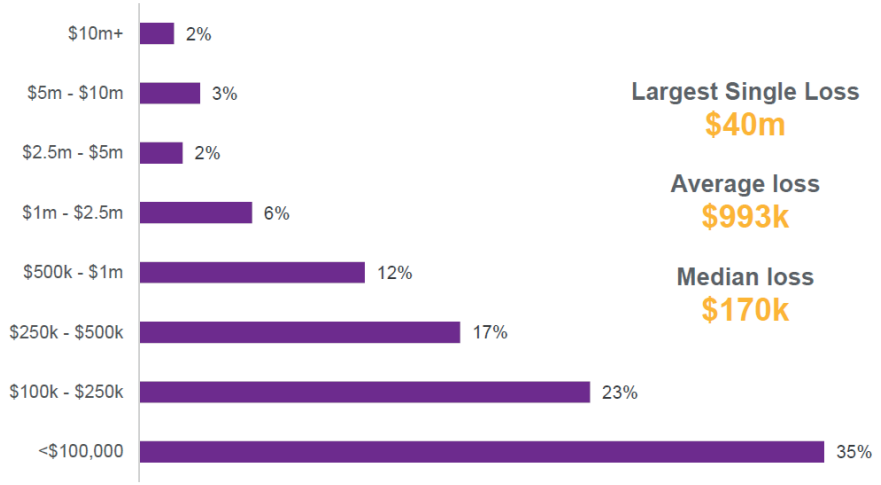


Figura 2.2: Perdite, in dollari, di diverse istituzioni finanziarie nel 2020 dovute a social engineering. Fonte: Willis Towers Watson Claims database

2.5 Terminologia e concetti

Tutte le tecniche di social engineering si basano su attributi specifici del processo decisionale umano, noti come bias cognitivi.[67] Questi bias vengono talvolta chiamati "bug dell'hardware umano" e vengono sfruttati in varie combinazioni per creare tecniche di attacco. Di norma il processo si basa sempre sul hacker che guadagna la fiducia dell'obiettivo o ne sfrutta la sua ignoranza e poi la utilizza per ottenere l'accesso alle informazioni sensibili di cui era a caccia. L'ingegneria sociale fa forte affidamento sui sei principi di influenza stabiliti da Robert Cialdini. La teoria dell'influenza di Cialdini spiega i principi chiave come autorità, intimidazione, consenso, scarsità, urgenza e familiarità. Il principio dell'autorità ci dice che l'attaccante potrebbe fingersi una figura di autorità (polizia, capo di dipartimento etc.) per aumentare le chance di successo dell'attacco. Il principio di intimazione si basa sul infondere paure di cattive conseguenze se certe azioni, volute dall'attore malevolo, non vengono completate. Il principio di consenso spiega come le persone, generalmente, tendono a compiere determinate azioni se vedono altre persone fare la stessa cosa. Per esempio, un passante per strada guarderà verso il cielo se dovesse vedere altre decine di persone fare lo stesso. Il principio di scarsità ci dice in modo semplice che una scarsità percepita genera domanda. La famosa frase "fino ad esaurimento scorte" capitalizza sul senso di scarsità. Il principio di urgenza, simile a quello di scarsità, viene usato dall'attore malevolo come attacco psicologico sulla vittima, con lo scopo di confonderla generando ansia. Infine il principio di familiarità ci spiega come

le persone siano più facilmente persuase da coloro a cui piacciono. In questo caso anche lo stereotipo del bell'aspetto fisico può essere molto importante.

2.6 Il ciclo di vita del social engineering

Proprio come nello sviluppo software e nel risk management, molti attacchi informatici seguono un approccio basato sul ciclo di vita, con un ciclo di input e output che migliora costantemente il processo. Il social engineering non è diverso ed ha perfino alcuni modelli di cicli di vita dedicati. Nella sua forma più semplice, il ciclo di vita del social engineering segue quattro fasi di base: quella iniziale viene detta *investigation*, seguita dalla fase di *hook*, per passare poi a quella di *play* ed infine la fase di *exit*.[51]

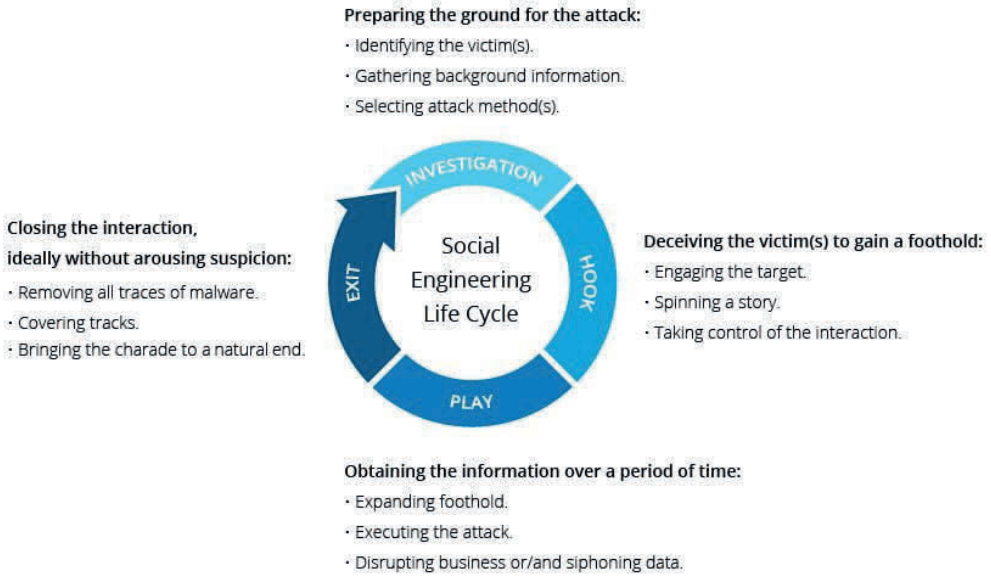


Figura 2.3: Il ciclo di vita del social engineering. Fonte: Imperva

La prima fase è quella investigativa, dove l'attaccante si concentra sulla ricognizione e la raccolta di dati. Questa fase è fondamentale per la riuscita dell'attacco pianificato e può essere anche la fase di maggiore durata temporale. Durante questo periodo l'attaccante si concentra non soltanto a capire quali sono le possibili falle di sicurezza fisiche o informatiche che possono essere sfruttate, ma si cerca anche di capire quali individui possono essere sfruttati e come. Con le giuste informazioni, l'attaccante può determinare quali vettori di attacco utilizzare, possibili password richieste,

risposte da aspettarsi dai vari attori e rifinire i propri obiettivi. In questa fase è molto importante definire anche un obiettivo chiaro, di modo da capire quali sono le informazioni importanti e quali possono essere ignorate.[115] Durante la raccolta di informazioni, piccoli pezzi di intelligence scollegati fra loro possono formare poi un puzzle completo se uniti correttamente.[117] Per completare questa fase l'attaccante utilizza spesso l'OSINT,[139] il google dorking[130] e diverse altre tecniche di investigazione, dalla ricerca sui social alla ricognizione fisica se necessaria.

La seconda fase detta "hook" (gancio o uncino), è la fase dove l'attaccante "getta l'esca" ovvero inganna le vittime prescelte e mette in atto l'attacco di social engineering. Per esempio, se dopo la prima fase l'attaccante avesse scelto di procedere sulla strada del phishing, questa fase potrebbe comprendere il mettersi in contatto con le vittime tramite mail forgiate per guadagnare la fiducia delle suddette, o raccogliere ulteriori informazioni. L'attaccante potrebbe quindi mettersi in contatto con il team di risorse umane di un'azienda e vista l'ampia ricerca effettuata nella fase precedente, potrebbe riuscire a creare email estremamente realistiche, esattamente come se fossero state mandate da un qualche altro membro interno al team o all'azienda.[109]

La terza fase, "play", è quella dove si sfruttano tutte le informazioni ottenute ed i rapporti instaurati con le vittime. È il momento in cui l'attaccante utilizza sia le informazioni che le relazioni per infiltrarsi attivamente nell'obiettivo. In questa fase, l'attaccante si concentra sul mantenimento del ritmo di conformità stabilito nella seconda fase senza destare sospetti. Lo sfruttamento può avvenire attraverso la divulgazione di informazioni apparentemente non importanti o l'accesso concesso/trasferito all'attaccante. Per fare qualche esempio di sfruttamento riuscito, si può pensare a delle credenziali di accesso divulgate all'attaccante via telefono, l'aprire una mail infetta con malware, l'inserire una chiavetta USB infetta da malware in un computer aziendale o anche solamente l'atto di tenere aperta la porta o di consentire in altro modo l'ingresso dell'aggressore all'interno della struttura[116]. Alla fine di questa fase, l'obiettivo dell'attaccante dovrebbe ora essere completo, qualunque esso fosse.

La fase finale, "exit", è quella di uscita. Questa indica la fine del ciclo di vita. L'ingegnere sociale cercherà di rimuovere tutte le tracce della sua presenza e di porre fine alla sua farsa. Tutto ciò che l'aggressore ha acquisito o imparato durante il processo viene poi utilizzato durante un nuovo ciclo di attacco per truffare più efficacemente un'altra vittima. L'ingegneria sociale e gli utenti inconsapevoli offrono una vasta superficie di attacco che può essere facilmente sfruttata.[52] È quindi necessario fare tutto il possibile per essere preparati e proteggersi dai truffatori dell'era digitale, e come abbiamo

visto, la consapevolezza di questi pericoli è ancora vastamente ignorata sia dal grosso delle attività commerciali che dai privati.

Capitolo 3

Esempi di attacchi malware e social engineering

3.1 La connessione fra malware e social engineering

Nei capitoli precedenti abbiamo visto in modo approfondito sia i malware che il social engineering. E' stato anche menzionato come i malware ed il social engineering funzionino insieme, essendo quest'ultimo il tramite che spesso viene utilizzato per portare i malware alla loro destinazione finale. Prima di fornire diversi esempi relativi ad entrambi gli argomenti menzionati, si vuole sottolineare l'importanza della simbiosi tra malware e social engineering e come le due cose si interfacciano fortemente. Per quanto possano esistere separatamente, la vera forza di diversi vettori d'attacco nasce quando malware ben creati vengono uniti a tecniche di social engineering ben studiate ed applicate. Nella stragrande maggioranza dei casi, i cyber criminali utilizzano una combinazione di tecniche di social engineering e metodi di implementazione di malware di modo da massimizzare le chance di infettare la macchina (o le macchine) bersaglio:[63] le tecniche di social engineering aiutano ad attrarre l'attenzione della potenziale vittima, mentre le tecniche di implementazione di malware aumentano la possibilità nel riuscire a penetrarla. Da qui notiamo anche la grande differenza nota di menzione fra i due argomenti. Da un lato i malware sfruttano tutte quelle che sono le falle di sicurezza informatica, mentre il social engineering sfrutta invece tutte le possibili debolezze umane, che si tramutano poi in falle altrettanto importanti. Se mitigare un attacco hacker composto da malware è difficile di suo, riuscire a mitigare un attacco ben gestito grazie all'uso del social engineering diventa ancora più complicato.

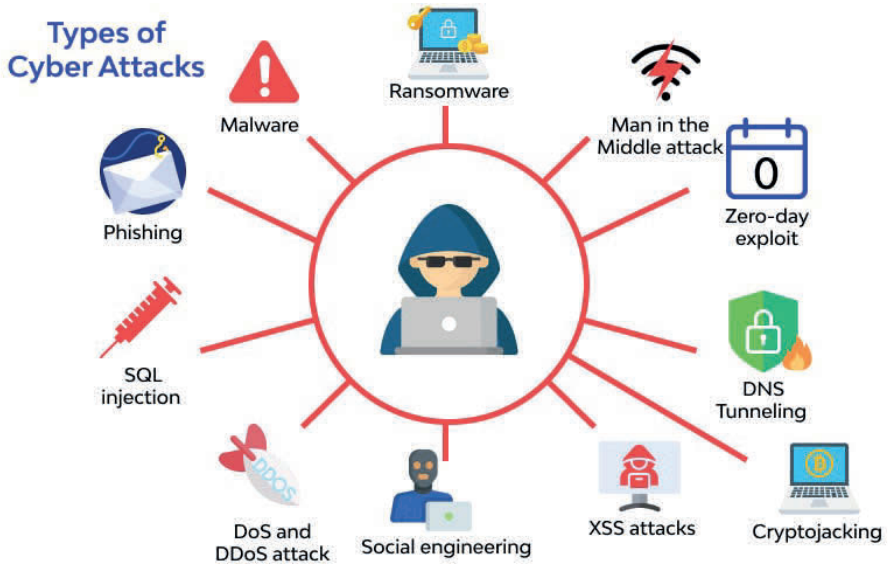


Figura 3.1: Diversi tipi di vettori d'attacco. Fonte: Wallarm

Prima di mostrare i diversi vettori d'attacco possibili, diamo una definizione chiara: nella sicurezza informatica, un vettore di attacco è un percorso, un metodo o uno scenario specifico che può essere sfruttato per introdursi in un sistema informatico, compromettendone la sicurezza. Un vettore di attacco può essere sfruttato manualmente, automaticamente o attraverso una combinazione di attività manuali e automatiche.[131] Vogliamo definire anche un altro termine importante, per non confonderci: una superficie di attacco è il numero totale di vettori di attacco che un aggressore può utilizzare per manipolare una rete o un sistema informatico o per estrarre dati.[122]

3.2 Vettori di attacco classici

Abbiamo visto nel primo capitolo una distinzione fra malware e vettori di attacco. Una volta vista la definizione precedente, dovrebbe essere quindi chiaro come le due cose siano differenti: da un lato abbiamo un programma malevolo che compie determinate azioni una volta eseguito, dall'altro abbiamo una particolare procedura che una volta sfruttata consente l'esecuzione di un malware o permette un intrusione in un sistema. I malware sono quindi uno dei tanti vettori di attacco, che però non elencheremo visto che sono già stati spiegati esaustivamente nei capitoli precedenti. Segue una lista, esclusi i malware, dei più comuni vettori d'attacco utilizzati dagli hacker[8]:

- *Credenziali compromesse*: username e password sono tuttora il tipo più

comune di credenziali di accesso e continuano ad essere periodicamente esposte in data leaks, attacchi phishing e malware. Quando perse, rubate o esposte le credenziali forniscono all'attaccante un accesso immediato. Per questo motivo le organizzazioni stanno investendo in strumenti che possano monitorare continuamente dati esposti e credenziali fuoriuscite in leaks. Autenticazione a due fattori (2FA), autenticazione multi fattore (MFA) e scan biometrici rimangono la soluzione migliore per proteggersi da questo tipo di vettore d'attacco.

- *Credenziali e password deboli*: in questo caso le credenziali di accesso sono semplici da indovinare o da brecciare tramite brute force, un attacco che utilizzando un dizionario e modifiche di diverse parole cerca di indovinare la password mandando molteplici richieste di login. Anche le password riutilizzate per diversi servizi comportano un rischio di sicurezza. Per motivi di sicurezza ad oggi sono molti i servizi che richiedono che le password scelte siano lunghe almeno otto caratteri e contengano simboli e numeri.

- *Crittografia debole o mancante*: Metodi di crittografia comuni come certificati SSL e DNSSEC possono prevenire attacchi di tipologia MiTM (man in the middle, di cui discuteremo più avanti), e possono proteggere dati confidenziali durante la loro trasmissione. Una crittografia debole o mancante per i dati significa che questi possono venire sniffati da un potenziale hacker o che vengano esposti in una fuga o violazione di dati.

- *Zero-day exploit*: uno zero-day (noto anche come 0-day) è una vulnerabilità in un software o hardware precedentemente sconosciuta a coloro che dovrebbero essere interessati alla sua mitigazione, come il fornitore del software o hardware in questione. Finché la vulnerabilità non viene mitigata, gli hacker possono sfruttarla per influire negativamente su programmi, dati, altri computer o una rete. Di norma l'unica via per mitigare uno zero-day è il rilascio di una patch successiva alla immissione sul mercato del prodotto. E' il venditore ad incaricarsi che la falla venga resa nota essendo la patch di estrema importanza.

- *Dispositivi mal configurati*: Le errate configurazioni di sicurezza derivano dall'incapacità di implementare correttamente i controlli di sicurezza su dispositivi, reti, applicazioni cloud, firewall e altri sistemi. Possono includere qualsiasi cosa, dalle credenziali di amministrazione predefinite alle porte aperte, dalle pagine web inutilizzate ai file non protetti. Un buon esempio è un protocollo di desktop remoto (RDP) che funziona correttamente, ma che presenta ancora il nome utente e la

password di amministrazione iniziali. Questo tipo di vettore di attacco passivo è un problema che riguarda l'organizzazione stessa e può portare a violazioni di dati, accessi non autorizzati e altri gravi incidenti di sicurezza.

- *Attacchi DDoS*: i Distributed Denial of Service sono tipi di attacchi network che vengono messi in atto contro altre risorse in un network come data center, server, siti internet o applicazioni web e possono limitare la funzionalità e disponibilità del sistema stesso. In questo caso l'hacker manda una quantità smisurata di messaggi alla risorsa, che non essendo in grado di gestire l'enorme numero di richieste rallenta o addirittura va in crash, rendendolo inaccessibile ai clienti. Per farlo vengono spesso sfruttate botnet create in precedenza dall'attore malevolo. CNDs e proxies sono possibili metodi per mitigare i rischi relativi agli attacchi DDoS.

- *Iniezioni SQL*: lo structured query language è un linguaggio di programmazione utilizzato per comunicare con i database. Molti server contenenti dati sensibili utilizzano questo linguaggio per gestire i loro database. Una iniezione SQL utilizza codice SQL maligno per costringere il server ad esporre dati che altrimenti non sarebbe possibile recuperare. Questo rischio diventa molto importante se il database contiene credenziali personali, numeri di carte di credito o altri dati privati importanti. Una corretta configurazione dei database è mandatoria per stare al sicuro da questo tipo di vettore d'attacco.

- *Vulnerabilità di sicurezza server e software*: nuove vulnerabilità vengono scoperte ed aggiunte al CVE ogni giorno. Se uno sviluppatore non ha rilasciato una patch per una possibile vulnerabilità generica, sia questa una zero-day o altro, diventa difficile potersi difendere da attacchi che sfruttano questo tipo di problemi. Molte falle scoperte possono colpire diversi sistemi, basti pensare, per esempio, alla recente falla di log4j.[72] Il CVE è la "common vulnerabilities and exposures", una lista di vulnerabilità divulgata pubblicamente e lanciata nel 1999 dalla MITRE, per identificare e categorizzare vulnerabilità in software e firmware.[121]

- *Cross site scripting*: questo tipo di attacco, conosciuto anche come XSS, comporta l'iniezione di codice dannoso in un sito web, ma non è il sito stesso a essere attaccato, bensì l'obiettivo è quello di colpire i visitatori del sito. Un modo comune in cui gli aggressori possono utilizzare attacchi di cross-site scripting è iniettare codice dannoso in

un commento, ad esempio incorporando un link a un codice JavaScript contenente malware nella sezione dei commenti di un blog.

3.3 Vettori di attacco del social engineering

Abbiamo visto diversi tipi di vettori di attacco classici che sfruttano diversi tipi di vulnerabilità generiche, siano queste zero-day o credenziali deboli. Questi tipi di vettori di attacco però non rientrano nella categoria dei vettori utilizzati dal social engineering, perché sfruttano falle informatiche e configurazioni errate. In questo caso vediamo invece quali sono i classici vettori di attacco usati dagli ingegneri sociali e come le diverse tecniche si concentrano non tanto su falle informatiche quanto sulle debolezze umane. Come abbiamo detto in precedenza, i malware sono un vettore d'attacco, ma possono rientrare in diverse categorie. Questo perché diversi vettori d'attacco del social engineering possono poi fare affidamento a malware per completare l'intrusione informatica, ma ovviamente la stessa cosa può succedere dopo aver utilizzato un vettore classico visto in precedenza.

Una delle grandi differenze fra le due categorie di vettori è che quelli relativi al social engineering possono essere delle procedure fisiche, dove l'attaccante compie azioni di persona e non a distanza usando un computer. Segue una lista dei più comuni vettori d'attacco utilizzati dagli ingegneri sociali ed hacker per portare a termine il loro obiettivo malevolo:[93]

- *Scareware*: come indica il nome, lo scareware è un malware che ha lo scopo di spaventare l'utente e spingerlo ad agire, e ad agire in fretta. Spesso si presenta sotto forma di pop-up o e-mail che indicano la necessità di "agire subito" per sbarazzarsi di virus o malware sul proprio dispositivo. Se ignorati gli scareware sono generalmente innocui, dato che si tratta di semplici pop-up o mail che non possono effettivamente compromettere un sistema. Se però l'utente dovesse cascare nel trabocchetto scaricherà in seguito altri malware potenzialmente molto pericolosi.

- *Email hacking e spam ai contatti*: è nella nostra natura prestare maggior attenzione ai messaggi ricevuti delle persone che conosciamo e da cui ci fidiamo. E gli ingegneri sociali lo sanno fin troppo bene: si appropriano di account di posta elettronica e spammano le relative liste di contatti con truffe e messaggi di phishing. In questo caso è molto difficile riuscire a mitigare l'attacco visto che la fonte è una persona di cui ci si fida. Il risultato può essere una distribuzione di massa del malware che l'hacker ha creato o una serie di truffe che rimbalza da

persona a persona portando un possibile grave danno economico sia al singolo che a una eventuale azienda.

- *Access tailgating*: conosciuto anche come piggybacking, l'access tailgating si verifica quando un ingegnere sociale segue fisicamente un individuo autorizzato in un'area a cui non ha accesso. Può trattarsi di un atto semplice come tenere aperta una porta per qualcun altro. Una volta entrati, hanno una ampia possibilità di accedere ai dispositivi contenenti informazioni importanti, che possono essere ulteriormente sfruttati se impiantati con chiavette USB contenenti codice malevolo autoeseguibile.

- *Phishing*: Il phishing è forse il metodo più famoso per rubare informazioni o dati sensibili da una vittima inconsapevole. Descriviamo brevemente il suo funzionamento tipico: un criminale informatico, in questo caso il phisher, invia un messaggio a un bersaglio chiedendo un tipo di informazione o di compiere un'azione che potrebbe essere utile per compiere poi un crimine più significativo. La richiesta può essere anche semplice come incoraggiare l'utente a scaricare un allegato (contenente un malware tipo keylogger) o verificare un indirizzo postale o ancora un codice di sicurezza. Vale la pena di notare che esistono molte forme di phishing tra cui gli ingegneri sociali possono scegliere, tutte con mezzi diversi per colpire l'utente. Lo spam phishing spesso assume la forma di un'unica grande e-mail "a tappeto", non necessariamente rivolta a un singolo utente. Lo spear phishing si rivolge invece a singoli utenti, magari impersonando un contatto fidato. Il whaling, ancora un'altra forma, prende di mira celebrità o dirigenti di alto livello riferendosi a quest'ultimi come whales o balene, data la loro importanza.

  E' inoltre importante menzionare anche le diverse forme di consegna in cui il phishing può presentarsi. Il *vishing*, ovvero phishing vocale, è quando una telefonata dove vengono rivelati dati sensibili da una vittima all'attaccante viene registrata. Nello *smishing* (ovvero sms phishing) vengono inviati messaggi di testo contenenti link malevoli, che portano al download di malware una volta cliccati. Nell'*angler phishing* l'ingegnere sociale posa come addetto al servizio clienti per intercettare comunicazioni e dati importanti. Ci sono poi casi di *in-session phishing*, che si verifica quando si è già su una piattaforma o un account e viene chiesto, ad esempio, di effettuare nuovamente il login. In questo caso il nuovo login trasmetterà le credenziali di accesso all'ingegnere sociale. In sostanza, abbiamo visto come il phishing sia una delle forme

più utilizzate ed evolute per compiere truffe e come possa presentarsi in molti modi diversi fra loro.

- *DNS spoofing*: conosciuto anche come cache poisoning (ovvero avvelenamento della cache), lo spoofing DNS si verifica quando un browser viene manipolato in modo che gli utenti online vengano reindirizzati a siti Web dannosi intenzionati a rubare informazioni sensibili. In altre parole, lo spoofing DNS è quando la cache viene avvelenata con reindirizzamenti malevoli. Questo vettore d'attacco è più comune quando la rete wifi che si utilizza è pubblica, come quella di un bar o di un hotel.

- *Bating*: Il bating (adescamento) si basa sulla premessa che qualcuno abbocchi all'esca, ossia offrire un qualcosa di desiderabile davanti a una vittima, sperando che abbocchi. Questo avviene più spesso su siti peer-to-peer come i social media, dove qualcuno potrebbe incoraggiare una vittima a scaricare un videogioco, documenti importanti o anche un film per poi infettare la vittima con un malware tramite il file scaricato in precedenza. Questo tipo di attacco ha anche una controparte fisica, chiamata dead drop. In questo caso un hacker potrebbe lasciare per terra, magari vicino all'entrata di un ufficio o un bar, una chiavetta usb con del malware all'interno. I file malevoli potrebbero ulteriormente essere categorizzati con nomi interessanti come "dati carta di credito" o "documenti importanti". Un bersaglio che abbocca all'esca raccoglierà la chiavetta e procederà nell'inserire nella sua macchina, infettandola, e potenzialmente mettendo a rischio l'intera rete a cui è collegato.

- *Pretexting*: il pretexting si tratta dell'uso di un pretesto interessante, o di uno stratagemma, per catturare l'attenzione di qualcuno. Una volta che la storia, di solito inventata, ha catturato l'attenzione della persona, l'ingegnere sociale cerca di ingannare la potenziale vittima per convincerla a fornirgli qualcosa di valore. Spesso l'ingegnere sociale si spaccia per una fonte legittima, come un agente di polizia o un addetto ai controlli degli impianti elettrici di un condominio business.

- *Attacchi watering hole*: Un attacco watering hole è un attacco a spazzata che infetta una singola pagina web con del malware. La pagina web si trova quasi sempre su un sito molto popolare per garantire che il malware possa raggiungere il maggior numero possibile di vittime.

- *Quid pro quo*: quid pro quo significa un favore per un favore, in sostanza "io ti do questo e tu mi dai qualcos'altro". Nel caso dell'ingegneria sociale, la vittima fornisce informazioni sensibili come i login dei conti o i metodi di pagamento e poi l'ingegnere sociale non restituisce la

sua parte dell'accordo. Per fornire un esempio nel mondo della compravendita online, si potrebbe trovare un prodotto normalmente molto costoso ad un prezzo estremamente basso. Si potrebbe mandare un versamento di denaro al venditore, che però non spedirà mai nulla e scomparirà con i soldi una volta ricevuti.

- *Violazione fisica*: come indicato dal nome, le violazioni fisiche si verificano quando un criminale informatico è in bella vista e si presenta fisicamente come una fonte legittima per rubare dati o informazioni riservate. Potrebbe trattarsi di un collega o di un addetto all'IT (magari un ex dipendente scontento) che si comporta come se stesse aiutando l'utente a risolvere un problema sul suo dispositivo. In realtà, l'obiettivo è quello di rubare i login dell'account dell'utente, o quante più possibili informazioni.

3.4 Falle informatiche degne di nota

Finora abbiamo parlato di diversi vettori di attacco e quali sono le possibili vulnerabilità che questi sfruttano. E' anche importante però notare che la scelta del vettore dipende dal tipo di vulnerabilità che si vuole sfruttare. Fra queste spiccano, data la loro importanza, alcune vulnerabilità scoperte in anni recenti che hanno colpito migliaia se non milioni di macchine tra computer e server.

Il bug Heartbleed, scoperto nell'aprile 2014, è apparso come una delle più grandi falle nella storia di Internet, ed ha compromesso la sicurezza di ben due terzi dei server mondiali, al tempo più di mezzo milione di server. Heartbleed, scoperto da una società di cyber security di nome Codenomicon e da un ricercatore Google di nome Neel Mehta, è una grave vulnerabilità della popolare libreria software crittografica OpenSSL.[66] Questa vulnerabilità consente di rubare le informazioni protette, in condizioni normali, dalla crittografia SSL/TLS utilizzata per proteggere le comunicazioni tramite Internet. SSL/TLS garantisce la sicurezza e la privacy delle comunicazioni su Internet per applicazioni quali web, e-mail, messaggistica istantanea (IM) e alcune reti private virtuali (VPN). Il bug Heartbleed consente a chiunque su Internet di leggere la memoria dei sistemi protetti dalle versioni vulnerabili del software OpenSSL. Ciò compromette le chiavi segrete utilizzate per identificare i fornitori di servizi e per crittografare il traffico, i nomi e le password degli utenti e il contenuto stesso. Di conseguenza consente agli aggressori di spiare le comunicazioni, rubare i dati direttamente dai servizi e dagli utenti e anche di impersonare tali servizi e utenti. Il bug nello specifico

si trova nell'implementazione di OpenSSL dell'estensione heartbeat di TLS/DTLS (Transport Layer Security Protocols) (RFC6520), da cui prende il nome. E' interessante notare come questo non si tratti di una falla del design del protocollo SSL/TLS, ma di un problema di implementazione, ovvero un errore di programmazione umano. Per mitigare la falla, è stata rilasciata una nuova versione di OpenSSL, ma questo significa che se la versione vulnerabile fosse ancora in uso da parte di qualche entità, questa sarebbe tutt'oggi vulnerabile.[3]

Figura 3.2: Il logo assegnato da Codenomicon alla falla. Fonte: Codenomicom

Pochi anni più tardi, il 14 Aprile 2017, il gruppo hacker conosciuto come Shadow brokers diffonde tramite leak un exploit, originariamente sviluppato dalla National Security Agency (NSA) statunitense. EternalBlue, nome dell'exploit in questione, sfrutta una vulnerabilità nell'implementazione del protocollo Server Message Block (SMB) di Microsoft. La vulnerabilità è dovuta al fatto che il server SMB versione 1 (SMBv1) in varie versioni di Microsoft Windows gestisce male i pacchetti appositamente creati da aggressori remoti, consentendo loro di eseguire codice in remoto sul computer di destinazione.[132] Per fare chiarezza, il protocollo SMB è un sistema standard, generalmente sicuro, che crea una connessione tra client e server inviando risposte e richieste. Quando si stampa un documento, una persona può

utilizzare il proprio computer, il client, per inviare una richiesta al computer di un collega, il server, con la richiesta di stampare il documento. Il client e il server comunicano tramite il protocollo SMB.[110] L'NSA non ha avvisato Microsoft dell'esistenza di EternalBlue per un periodo di cinque anni, fino a quando una violazione dell'agenzia stessa, a mano del gruppo sopracitato, ha costretto l'agenzia a farlo. Microsoft incolpa l'agenzia dell'esistenza di EternalBlue e delle sue conseguenze ed anche se la falla si basa su una vulnerabilità di Windows, L'NSA ha rifiutato di parlarne in dettaglio.[54] Il leak di questo exploit unito al lungo silenzio dell'NSA ha portato ad un attacco hacker globale nel Maggio del 2017 dove è stato diffuso il ransomware WannaCry, che ha infettato più di 230000 computer. Questo attacco si è diffuso attraverso i computer non patchati contro la falla EternalBlue che utilizzano Microsoft Windows. Come nei classici ransomware, i file degli utenti sono stati criptati e per la loro restituzione è stato chiesto un riscatto in Bitcoin. Quando il ransomware si è diffuso oltre l'Europa, i sistemi informatici di oltre 150 paesi sono stati paralizzati. L'attacco del ransomware WannaCry ha avuto un notevole impatto finanziario a livello mondiale. Si stima che questo crimine informatico abbia causato perdite per 4 miliardi di dollari in tutto il mondo. Se non fosse stato per il continuo utilizzo di sistemi informatici obsoleti e per la scarsa educazione alla necessità di aggiornare il software, i danni causati da questo attacco sarebbero potuti essere evitati.[31]

In anni ancor più recenti, il 14 Novembre 2021, viene scoperta una gravissima vulnerabilità nel codice di una libreria software usata per il logging, conosciuta come Log4Shell. Si tratta di una vulnerabilità zero-day in Log4j, un popolare framework di logging scritto in Java appartenente ad Apache, che comporta l'esecuzione di codice arbitrario. Si stima che questa falla fosse presente in oltre 100 milioni di istanze a livello globale. Gli esperti di sicurezza considerano Log4Shell una delle minacce più gravi degli ultimi anni.[37] Questa considerazione è dovuta a due fattori: l'enorme numero di sistemi vulnerabili e la facilità con cui un aggressore può compromettere una rete. Log4j registra prima i messaggi nel software e poi li analizza alla ricerca di errori. Le sue capacità di logging gli consentono di comunicare con altre funzioni interne ai sistemi, come i servizi di directory ed è questo che crea l'apertura per la vulnerabilità. L'attacco principale consiste nell'inviare a Log4j messaggi che istruiscono il sistema a scaricare ed eseguire malware da un server remoto, garantendo così all'aggressore un maggiore accesso al sistema della vittima. Questo può, a sua volta, portare alla completa compromissione della rete e al furto di informazioni sensibili, nonché alla possibilità di sabotaggio. La libreria Log4j è in utilizzo dal 2001 e pare che la falla esistesse già da 13 anni.[16] Sorprendentemente, la vulnerabilità è stata scoperta da Chen Zhao-

jun di Alibaba (il sito di e-commerce più importante della cina) nel popolare videogioco Minecraft: Java edition, dove dei giocatori hanno scoperto che l'inserimento di una riga di codice dannosa nella chat del gioco fa sì che questa venga registrata da Log4j in modo da consentire l'esecuzione di comandi. Se un utente malintenzionato è in grado di inserire una stringa di codice in un modulo che viene registrato da Log4j, anche se si tratta di un campo di nome utilizzato per l'accesso ai servizi cloud, è possibile sfruttare questa vulnerabilità. Gli ambienti Windows, Linux e Mac sono tutti ugualmente vulnerabili.[73] Da dicembre dello stesso anno della sua scoperta, la maggior parte dei fornitori ha pubblicato aggiornamenti di sicurezza che risolvono la falla di Log4j all'interno delle loro applicazioni e Apache stessa ha rilasciato correzioni e versioni aggiornate che rimediano alla vulnerabilità.[41]

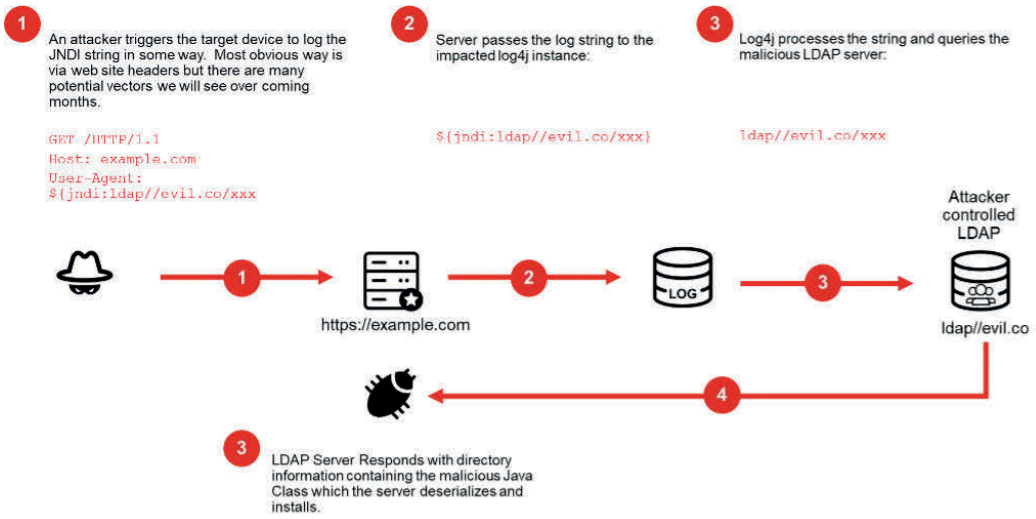


Figura 3.3: Diagramma che dimostra il funzionamento della falla log4j. Fonte: Fortinet

Capitolo 4

Misure preventive ed information security

In questo capitolo vogliamo parlare di quali sono le possibili misure preventive e tecniche difensive che un utente o un'impresa può utilizzare per difendersi da attacchi hacker e tutti i pericoli che derivano da falle e problemi di sicurezza, compresi eventuali attacchi di tipo social engineering. Parleremo di antivirus, sistemi di sorveglianza, monitoring, dns sinkhole (etc) ma anche dell'attenzione che l'utente e l'impiegato aziendale devono prestare a determinate cose, ovvero spiegare le "good practices" su come rimanere sicuri.

4.1 Misure preventive per i privati

Quando si tratta di privati, quindi dei singoli utenti che utilizzano i loro dispositivi nella comodità della loro casa e non per scopi lavorativi, questi godono automaticamente di un vantaggio rispetto ad eventuali dipendenti di aziende: non essere bersaglio di attacchi hacker rivolti direttamente all'azienda, che potrebbero rendere qualsiasi dipendente un potenziale bersaglio per ottenere credenziali o informazioni. Il privato che utilizza dispositivi IoT per scopo ludico deve comunque stare attento a proteggere nel modo corretto le varie piattaforme che utilizza. Per fare un esempio, tanto è maggiore il numero di dispositivi smart che l'utente utilizza, maggiore è l'attenzione che si deve prestare per assicurarsi che non ci siano falle di sicurezza. Dispositivi di ultima generazione dedicati alle smart homes, dalle telecamere di sorveglianza, termostati e luci regolabili tramite smartphone a dispositivi come Alexa, possono rivelarsi un pericolo se non configurati correttamente. Una ricerca condotta nel 2021 rivela che queste nuove smart homes sono altamente vul-

nerabili a diversi tipi di attacco. Tra i casi segnalati di attacchi alle smart homes vediamo hacker che controllano a distanza luci e smart TV, sbloccano porte abilitate all'IoT e accendono e trasmettono a distanza video da telecamere smart.[6] Come se questo non bastasse, bisogna tenere a mente che un dispositivo smart compromesso in una rete domestica, anche una semplice lampadina, può portare ad una penetrazione completa della rete domestica.

E' di fondamentale importanza quindi assicurarsi che tutte le credenziali possibili associate a diversi dispositivi installati in casa non siano lasciate impostate a quelle di default e che le varie password non siano semplici da indovinare. Un'altra buona prassi riguardo alle credenziali, è quella di non riutilizzare le stesse password per troppi servizi. Nel caso una password venga rubata sarebbe semplice per un hacker riuscire ad accedere a diversi altri account e dispositivi dell'utente. Per continuare il discorso delle misure preventive possibili per i privati abbiamo poi una funzione fondamentale da utilizzare e mantenere sempre attiva, ovvero il firewall. Un firewall è un software di sicurezza di rete che monitora e filtra il traffico di rete in entrata e in uscita in base ai criteri di sicurezza precedentemente stabiliti. Nella sua forma più elementare, un firewall è essenzialmente la barriera che si frappone tra una rete interna privata e la rete Internet pubblica. Lo scopo principale di un firewall è quello di consentire l'ingresso di traffico non pericoloso e di escludere quello pericoloso.[17] Oltre ad essere built-in per dispositivi Windows e MacOS, tutti i router che si utilizzano ad oggi dispongono di un firewall preinstallato.[95] Questo avviene perché non si vuole filtrare il possibile traffico pericoloso solamente dal nostro computer, ma dalla nostra intera rete locale, a cui si accede proprio dal router che utilizziamo come access point all'internet.

Un'altra misura di sicurezza fondamentale per l'utente medio è l'utilizzo di un software anti-virus. Il software antivirus (abbreviato in software AV), noto anche come anti-malware se si vuole usare correttamente il termine, è un programma informatico utilizzato per prevenire, rilevare e rimuovere eventuali malware. Gli antivirus sono stati originariamente sviluppati per rilevare e rimuovere i virus informatici, da cui il nome. Tuttavia, con la proliferazione di altre minacce informatiche, il software antivirus ha iniziato a proteggere da altre minacce informatiche, una gran parte di altri tipi di malware. Alcuni prodotti includono anche la protezione da URL dannosi, spam e phishing.[83] Bisogna tenere a mente però che un antivirus può comportare anche alcuni problemi quando lo si utilizza. Dallo stare attenti ai termini di rinnovo di una licenza che si ha acquistato a non scaricare "rogue AVs" (malware che si spacciano per antivirus, ma non lo sono), gli antivirus possono comportare anche problemi causati da falsi positivi. Per falsi

positivi intendiamo quando il software identifica un file non pericoloso come malware. Se l'antivirus è configurato per mettere in quarantena o eliminare immediatamente un file ritenuto pericoloso, comportamento comune per gli antivirus dedicati a Windows, un falso positivo potrebbe in realtà essere un file fondamentale per il funzionamento del sistema operativo che, se rimosso, potrebbe renderlo inutilizzabile.[101] Bisogna inoltre tenere a mente che gli antivirus sono pensati per essere utilizzati in contemporanea con i firewall, dato che i primi si occupano di tenere sotto controllo i file mentre gli ultimi si preoccupano invece della sicurezza del traffico internet, ma non supportano la rimozione di file infetti. Una buona prassi per qualunque utente di dispositivi IoT è assicurarsi che questi ultimi siano sempre aggiornati alla loro ultima versione e che tutte le patch, se disponibili, siano installate. Le patch sono aggiornamenti del software e del sistema operativo che risolvono le vulnerabilità di sicurezza di un programma o di un prodotto.[18] Di norma questo tipo particolare di aggiornamento viene rilasciato direttamente dal fornitore del prodotto o software, e viene trattato come un comune aggiornamento. Abbiamo visto nei capitoli precedenti come grosse falle di sicurezza (si pensi alla recente Log4shell) siano state quasi immediatamente risolte tramite patch ed aggiornamenti di sicurezza ed è quindi semplice capire come dei piccoli comuni aggiornamenti possano in realtà essere molto importanti.

Stando sempre alle buone pratiche da seguire per la sicurezza dei propri dispositivi, è importante sapere come anche come comportarsi quando questi vengono utilizzati. Ignorare lo spam e non cadere in tranelli è fondamentale, ma questo può avvenire solamente se l'utente è consapevole di quali sono i rischi e come comportarsi a riguardo. Evitare di cliccare su link ricevuti da sconosciuti e non fidarsi di quasi nessuno diventa quindi imperativo. Molto importante è anche tenere dei backup dei file che si ritengono importanti o dell'intero disco rigido del computer, in caso questo venga corrotto o bloccato tramite ransomware da un hacker. Un'ultima prassi che può risultare complicata per alcuni utenti non troppo esperti, ma molto utile, è la virtualizzazione. Non tutti hanno bisogno di seguire questa strada, ma si visitano spesso siti web poco raccomandabili, bisogna aspettarsi di essere bombardati da spyware e malware. Sebbene il modo migliore per evitare le intrusioni derivate da browser sia quello di tenersi alla larga dai siti non sicuri, la virtualizzazione consente di eseguire il browser in un ambiente virtuale, come Parallels o VMware Fusion, che ignora il sistema operativo per mantenerlo più sicuro.[39] Con questo ulteriore strato di sicurezza, chiamato spesso "sandbox", qualsiasi cosa accada al sistema interno alla macchina virtuale è di poco spessore, perché si può sempre spegnere e cancellare, senza preoccuparsi di molto dato che non dovrebbe contenere nessun dato sensibile o

importante, tenuto invece sul vero e proprio sistema operativo della nostra macchina.

4.2 Misure preventive per enterprise

Quando si parla di imprese, siano queste di piccola o grande dimensione, si utilizzano diversi sistemi per impedire ad eventuali hacker l'accesso alla rete o alle macchine aziendali. In questo caso è importante notare che le macchine, la rete ed anche i singoli individui dipendenti dell'azienda, sono vulnerabili. E' quindi fondamentale riuscire a tutelare tutte queste cose insieme. Per farlo le imprese adottano normalmente quelle che vengono chiamate Information Security Policies, un set di linee guida che aiutano un business a proteggere i dati dei loro clienti e dipendenti contemporaneamente. Queste politiche servono anche a garantire che l'azienda non violi alcuna norma legale o etica. Inoltre, forniscono un quadro di riferimento per l'azienda per assicurarsi di essere pronta ad affrontare eventuali violazioni della sicurezza.[19] Mantenere la sicurezza delle informazioni è un compito difficile. Richiede una vigilanza e un'attenzione costanti e può essere impegnativo tenersi al passo con gli ultimi sviluppi del settore. Esistono molti modi diversi per mantenere la sicurezza delle informazioni e tutte le aziende dovrebbero adottare misure per proteggere i propri dati.

Uno dei primi che vediamo è lo stesso visto in precedenza per i privati, ma con addirittura maggior attenzione: il cambio regolare delle password. Abbiamo già sottolineato come le password predefinite dovrebbero sempre essere personalizzate per ogni singolo utente. Tuttavia, la forza delle password in termini di numeri e caratteri speciali è solo la prima linea di difesa. I nomi utente e le password sono la porta d'accesso più semplice per hacker ai dispositivi e le reti interne delle aziende, di conseguenza queste ultime tendono ad avere politiche per cui le password di ogni utente devono essere cambiate almeno una volta al mese.[53] Un altro fattore importante che invece viene di solito ignorato nell'ambito privato è la scelta del corretto ISP (Internet Service Provider). Un castello è forte quanto le sue mura e lo stesso vale per l'ISP delle aziende. Potrebbe non essere scontato, ma non tutti i fornitori di servizi Internet sono costruiti ne funzionano allo stesso modo. Quando si sceglie un provider di Internet, non ci si deve limitare a velocità e prezzo. Esiste una pletora di fornitori di servizi sul mercato, quindi è saggio scegliere un pacchetto Internet che abbia funzioni di sicurezza integrate. Dopo aver valutato la sicurezza online di un ISP, si passa alla sua convenienza e alla velocità di connessione.[47] La cosa migliore è trovarne uno che soddisfi tutti e tre i criteri.

Torniamo ad analizzare anche il discorso firewall, ma in modo più approfondito. Nel caso di un business vengono spesso implementati diversi tipi di firewall, e si utilizzano anche diversi switch e dispositivi hardware dedicati unicamente al controllo e filtro di pacchetti. Normalmente un'impresa non utilizza un solo tipo di firewall, ma di diversi tipi: il primo tipo che vediamo sono i classici "packet filtering firewalls", il tipo più basico ed usato da privati. Operano a livello di network e controllano gli indirizzi IP di fonti e destinazioni, protocolli, porte e porte di destinazione di connessioni basandosi su regole definite a priori. Passando alla seconda categoria abbiamo firewall che operano a livello di sessione e vengono detti "circuit-level gateways". Questi verificano le connessioni TCP (Transmission Control Protocol) stabilite e tengono traccia delle sessioni attive. Sono abbastanza simili ai firewall di filtraggio dei pacchetti in quanto eseguono un unico controllo e utilizzano risorse minime, ma funzionano a un livello superiore del modello OSI (Open Systems Interconnection). In primo luogo, determinano la sicurezza di una connessione stabilita: quando un dispositivo interno avvia una connessione con un host remoto, i circuit-level gateways stabiliscono una connessione virtuale per conto del dispositivo interno per mantenere nascosti l'identità e l'indirizzo IP dell'utente interno. Sono efficienti dal punto di vista dei costi, semplicistici e hanno un impatto minimo sulle prestazioni della rete.

Passando poi al terzo tipo di firewall denominato "stateful inspection firewalls", abbiamo un firewall che opera ad un'ulteriore passo avanti rispetto al precedente. Gli stateful inspection firewalls verificano e tengono traccia delle connessioni stabilite ed eseguono l'ispezione dei pacchetti per fornire una sicurezza migliore e più completa. Funzionano creando una tabella di stato con IP di origine, IP di destinazione, porta di origine e porta di destinazione una volta stabilita una connessione. Creano dinamicamente le proprie regole per consentire il traffico di rete in entrata previsto, invece di affidarsi a un insieme di regole codificate in base a queste informazioni. Eliminano velocemente i pacchetti di dati che non appartengono a una connessione attiva verificata. Esiste poi un quarto ed ultimo tipo di firewall, chiamato "application-level gateway" o anche più comunemente proxy firewalls. Sono implementati a livello di applicazione tramite un dispositivo proxy. Invece di accedere direttamente alla rete interna, la connessione viene stabilita attraverso il firewall proxy. Il client esterno invia una richiesta al firewall proxy. Dopo aver verificato l'autenticità della richiesta, il firewall proxy la inoltra a uno dei dispositivi o server interni per conto del client. In alternativa, un dispositivo interno può richiedere l'accesso a una pagina web e il dispositivo proxy inoltra la richiesta nascondendo l'identità e la posizione dei dispositivi e della rete.[12]

Questo discorso di politiche, credenziali sicure e firewall va integrato anche con altre ottime pratiche che tutte le aziende dovrebbero seguire. Per esempio, tutti i dati personali e finanziari dei clienti di un'azienda devono essere cifrati. Se poi si vuole raggiungere un ulteriore livello di sicurezza, questo vale per qualsiasi tipo di dato sensibile che venga ospitato all'interno dei database o dei sistemi dell'azienda. Un'altro modo per assicurarsi che i dipendenti rimangano al sicuro da alcuni vettori d'attacco, tra cui principalmente vediamo i tipi relativi al social engineering, è quello di limitare l'accesso ad internet e bloccare siti non necessari. Limitare l'accesso a determinate informazioni online riduce le possibilità di violazione della sicurezza, quindi è buona norma assicurarsi che solo gli utenti necessari abbiano accesso a determinati dati. Allo stesso modo, bloccando la visualizzazione di alcuni siti si riduce la possibilità che siti portatori di virus e spyware vengano aperti all'interno della rete aziendale.[81] Infine, non possiamo nuovamente non citare la sezione riguardante patch e updates. E' imperativo che i sistemi IT di un'impresa siano sempre aggiornati all'ultima versione, onde evitare lo sfruttamento di possibili falle di vecchie versioni. Per concludere vogliamo anche menzionare nuovamente che la mancata consapevolezza di potenziali pericoli da parte dei dipendenti rimane uno dei maggiori rischi di intrusioni di sicurezza. Gli utenti ed i dipendenti devono essere consapevoli dei rischi e delle minacce che incombono sui sistemi e sulle informazioni che utilizzano. È necessario formare gli utenti su come riconoscere i tentativi di accesso ad informazioni sensibili tramite e-mail, telefonate o altri mezzi.[78]

4.3 Il processo di Information Security

Qualsiasi organizzazione che si affida alle reti informatiche ed Internet deve dare priorità alla Information Security, ovvero Sicurezza delle Informazioni. Questo termine si riferisce semplicemente alle strategie, ai prodotti e alle procedure implementate dagli esperti di sicurezza per prevenire l'accesso non autorizzato o le minacce interne alle informazioni sensibili, siano queste memorizzate nel cloud o su dispositivi di archiviazione fisici. L'esperto di sicurezza informatica è responsabile di garantire che questi dati non vengano alterati o modificati in alcun modo.[96] La Information Security è quindi un processo che si muove per fasi, costruendosi e rafforzandosi lungo il percorso. Sebbene questo processo preveda molte strategie ed attività, queste possono essere raggruppate in tre fasi distinte: prevenzione, rilevamento e risposta. Ognuna di queste fasi richiede strategie ed attività che fanno passare il processo alla fase successiva. La crescita dinamica delle nuove minacce e vulnerabilità richiede un adeguamento estremamente veloce delle metodo-

logie del ciclo di prevenzione, rilevamente e risposta, ed un cambiamento in una fase si ripercuote in qualche modo sulle fasi successive e quindi sull'intero processo. Per una gestione efficace di quest'ultimo ogni fase deve essere progettata con grande capacità adeguate ed una supervisione che ne garantisca la maturità Il goal ultimo del processo di Information Security è quello di proteggere tre attributi unici delle informazioni:[25]

Confidenzialità: le informazioni sensibili dovrebbero essere viste solamente da quelle persone autorizzate a visualizzarle. Le informazioni possono essere riservate perché si tratta di informazioni proprietarie dell'organizzazione, oppure possono essere informazioni personali dei clienti che devono essere mantenute riservate a causa di responsabilità legali.

Integrità: le informazioni non devono essere corrotte, degradate o modificare. Devono essere adottate misure per isolare le informazioni da modifiche accidentali o intenzionali.

Disponibilità: le informazioni devono essere sempre disponibili per la visione dal personale autorizzato quando necessario.

Gli attacchi hacker compromettono i sistemi in vie che influenzano uno o tutti questi attributi, e questo deve essere evitato. Un'organizzazione riesce a proteggere questi attributi grazie a una pianificazione adeguata, cosa che può inoltre ridurre notevolmente i rischi di un attacco ed aumentare fortemente le capacità di rilevamento e risposta in caso un attacco abbia luogo.[111] Vediamo ora in dettaglio i processi.

4.3.1 Prevenzione

La prevenzione delle minacce si riferisce generalmente a strumenti che eseguono azioni di rilevamento e prevenzione delle minacce, come il rilevamento e la risposta degli endpoint, o a politiche e strategie di sicurezza informatica che danno priorità alle tecniche di prevenzione. Durante la fase di prevenzione, è quindi necessario progettare e implementare politiche, controlli e processi di sicurezza. Tutte queste cose sono interconnesse fra loro e devono essere sviluppate fin dalle prime fasi. La politica di sicurezza delle informazioni è la pietra angolare su cui si basa tutto il resto. Il primo passo è quindi creare delle politiche di sicurezza che determinano cosa deve essere protetto e come. Il tutto viene seguito dai programmi di sensibilizzazione che educano gli impiegati sull'importanza della sicurezza, l'utilizzo di tali misure e le loro responsabilità legate all'argomento. Ultimo passo è poi quello dell'implementazione del controllo all'accesso. Non tutti gli utenti dovrebbero

avere accesso al sistema e le informazioni contenute all'interno. L'accesso deve essere ristretto e garantito su diversi livelli a chi lo necessità. Per farlo di solito vengono emessi identificatori e metodi di verifica che i dipendenti possono utilizzare per accedere a quello di cui hanno bisogno.[108]

4.3.2 Rilevamento

Il rilevamento delle minacce è la pratica dell' analizzare l'intero ecosistema di sicurezza per identificare qualsiasi attività dannosa che potrebbe compromettere la rete. Se viene rilevata una minaccia, è necessario adottare misure di mitigazione per neutralizzarla prima che possa sfruttare le vulnerabilità presenti. Quando si tratta di rilevare e mitigare le minacce, la velocità è fondamentale. I programmi di sicurezza devono essere in grado di rilevare le minacce in modo rapido ed efficiente. I programmi di difesa di un'azienda sono idealmente in grado di bloccare la maggior parte delle minacce, perché spesso sono già state viste in passato e vengono quindi considerate "note". Tuttavia, esistono altre minacce "sconosciute" che un'organizzazione mira a rilevare. Ciò significa che l'organizzazione non le ha mai incontrate prima, magari perché l'aggressore utilizza metodi o tecnologie nuove. Per cercare di rilevare qualsiasi minaccia, ignorandone il tipo, vengono usate diverse tecniche e programmi: la threat intelligence è un modo di esaminare i dati delle firme di attacchi già visti e di confrontarli con i dati aziendali per identificare le minacce. E' particolarmente efficace nel rilevare le minacce note, ma non quelle sconosciute.

L'intelligence delle minacce è spesso utilizzata con grande efficacia nelle tecnologie SIEM (Security Information and Event Management) di cui parleremo ampiamente più avanti, antivirus, IDS (Intrusion Detection System) e web proxy. Vengono utilizzati in congiunzione con i SIEM gli UEBA (Users and Entity Behaviour Analytics), grazie ai quali un'organizzazione è in grado di capire quale sia il comportamento normale di un dipendente: a che tipo di dati accede, a che ora si connette e dove si trova fisicamente, ad esempio. Un comportamento imprevisto farà scattare un campanello d'allarme, che aprirà una investigazione sull'evento per determinarne le ragioni. Un ultimo metodo di rilevamento, che deriva fortemente dalla prevenzione, è quello della creazione di trappole, i cosiddetti "honeypot". Alcuni obiettivi sono troppo allettanti per un aggressore. I team di sicurezza lo sanno, quindi preparano trappole nella speranza che l'aggressore abbocchi. Quando un aggressore punta a questa esca, scatta un allarme per far sapere al team di sicurezza che c'è un'attività sospetta nella rete che deve essere indagata.[107]

4.3.3 Risposta

La risposta agli incidenti (detta Incident Response o IR) si riferisce ai processi e alle tecnologie di un'organizzazione per rilevare e rispondere a minacce informatiche, violazioni della sicurezza o attacchi informatici. L'obiettivo della risposta agli incidenti è prevenire gli attacchi informatici prima che si verifichino e ridurre al minimo i costi e le interruzioni dell'attività derivanti da eventuali attacchi informatici non prevenuti.[61] Idealmente, un'organizzazione definisce i processi e le tecnologie di risposta agli incidenti in un piano formale di risposta agli incidenti (detto IRP) che specifica esattamente come i diversi tipi di attacchi devono essere identificati, contenuti e risolti. Un piano di risposta agli incidenti efficace può aiutare i team di cybersecurity a individuare e contenere le minacce informatiche e a ripristinare più rapidamente i sistemi colpiti, riducendo i mancati introiti, le sanzioni normative e gli altri costi associati a queste minacce. I due framework per l'Incident Response più noti sono stati sviluppati da NIST e SANS per fornire ai team IT una base su cui costruire i loro piani di risposta agli incidenti. Di seguito sono riportate le fasi del framework di SANS,[21] su cui ci focalizziamo in quanto più dettagliato.

1. *Preparation*: Nessuna organizzazione è in grado di organizzare una risposta efficace agli incidenti con un solo preavviso. È necessario disporre di un piano per prevenire e rispondere agli eventi. Questo comporta che le organizzazioni facciano un inventario completo della loro infrastruttura IT, comprese reti, server ed endpoint, e ne valutino l'importanza. Per valutare l'importanza, le organizzazioni devono stabilire quali asset IT contengono informazioni critiche o sensibili. Inoltre, devono creare una linea di base per le attività normali attraverso il monitoraggio. Come parte della preparazione, i team di sicurezza devono anche creare una guida su come gestire i tipi comuni di incidenti e identificare quali tipi di incidenti richiedono un'indagine approfondita.[106]

2. *Identification*: L'individuazione comporta la raccolta di dati dai sistemi IT, dagli strumenti di sicurezza, dalle informazioni disponibili pubblicamente e dalle persone all'interno e all'esterno dell'organizzazione, e l'identificazione di segnali che indicano che un incidente potrebbe verificarsi in futuro (precursori) e di dati che mostrano che un attacco è avvenuto o sta avvenendo ora (indicatori). L'analisi prevede l'identificazione di una linea di base o di un'attività normale per i sistemi interessati, la correlazione di eventi correlati e la verifica di eventuali deviazioni dal comportamento normale.[22]

3. *Containment*: Se viene identificato un incidente, la fase successiva è il contenimento: i team di sicurezza devono lavorare per isolare l'attacco e impedirne la diffusione. Ciò può comportare la segmentazione della rete sotto attacco come parte del contenimento a breve termine. Una volta adottate le misure a breve termine, i team di sicurezza possono concentrarsi sulle soluzioni a lungo termine, che possono comportare la ricostruzione di interi sistemi.[23]

4. *Eradication*: Per eradicazione si intende la rimozione effettiva del malware o di altri artefatti introdotti dagli attacchi e il ripristino completo di tutti i sistemi colpiti. Il processo di eradicazione SANS prevede per prima cosa il re-imaging, ovvero una pulizia completa dei dischi rigidi del sistema interessato per garantire la rimozione di qualsiasi contenuto dannoso. Si cerca poi di capire cosa ha causato l'incidente per evitare compromissioni future. Dopo di che si applicano le migliori pratiche di sicurezza di base, ad esempio aggiornare le vecchie versioni del software e disattivare i servizi inutilizzati. Infine, si utilizza un software antimalware o un antivirus di nuova generazione per scansionare i sistemi interessati e garantire la rimozione di tutti i contenuti dannosi.[89]

5. *Recovery*: Questa fase prevede il ripristino dei sistemi interessati che sono stati disattivati durante il periodo dell'incidente. I team di sicurezza devono testare e monitorare i sistemi interessati per garantire che gli attacchi non si ripetano e che si raggiunga la normale funzionalità.[44]

6. *Lesson Learned*: Poco dopo l'attacco, i team devono guardare indietro e valutare come è stato gestito l'incidente e analizzare come migliorare il processo di risposta agli incidenti per gli incidenti futuri. Questo significa scrivere una documentazione completa riguardo un incidente, pubblicare i report dello stesso e identificare come migliorare le performance del team di sicurezza. Si conduce poi un meeting con i membri del gruppo per discutere l'incidente e cementare le lezioni che si possono imparare ed applicare immediatamente.[24]

Questo conclude il processo di risposta ad una minaccia informatica. Abbiamo visto come il processo di Information Security, nonostante la sua corposità, sia fondamentale per la corretta protezione di un sistema informatico di una organizzazione. Parleremo fra poco più in dettaglio degli applicativi che vengono adoperati.

Capitolo 5

I SIEM come misura di sicurezza

Una misura di sicurezza usata dalle organizzazioni in tutto il mondo, in congiunzione con altri strumenti, è quella dell'utilizzo dei SIEM. Nel campo dell'information security i SIEM sono una abbreviazione per "security information and event management", e si tratta di un sottocampo particolare dove prodotti e servizi quali "security information management" (SIM) e "security event management" (SEM) sono combinati, dando quindi vita ai sistemi SIEM.[133] In questo capitolo vogliamo introdurre questi sistemi e spiegare cosa sono, come funzionano, quali sono le loro capacità ed in generale fornire una base di conoscenza sufficiente per addentrarsi alla loro progettazione, installazione, configurazione e manutenzione che verrà raccontata nel prossimo capitolo.

5.1 Cosa sono i SIEM e come sono nati

Come abbiamo appena detto, combinando la gestione delle informazioni di sicurezza (SIM) e la gestione degli eventi di sicurezza (SEM), otteniamo la gestione delle informazioni e degli eventi di sicurezza (SIEM). Questa offre il monitoraggio e l'analisi in tempo reale degli eventi, nonché il tracciamento e la registrazione dei dati di sicurezza a fini di conformità o di audit. In parole povere, il SIEM è una soluzione di sicurezza informatica che aiuta le organizzazioni a riconoscere le potenziali minacce e vulnerabilità alla sicurezza prima che abbiano la possibilità di interrompere le operazioni aziendali.[82] Il SIEM rileva le anomalie del comportamento degli utenti e utilizza l'intelligenza artificiale per automatizzare molti dei processi manuali associati al rilevamento delle minacce e alla risposta agli incidenti, diventando un punto

fermo dei moderni centri operativi di sicurezza (SOC) per i casi d'uso della gestione della sicurezza e della conformità. Nel corso degli anni, il SIEM è maturato fino a diventare qualcosa di più dei semplici strumenti di gestione dei log che lo hanno preceduto. Oggi il SIEM offre analisi avanzate del comportamento di utenti ed entità (UEBA) grazie alla potenza dell'intelligenza artificiale e dell'apprendimento automatico.[14] Abbiamo quindi davanti agli occhi un sistema di orchestrazione dei dati altamente efficiente per la gestione di minacce in continua evoluzione, nonché per la conformità normativa e la reportistica.[57]

Per capire a dove siamo arrivati oggi con l'utilizzo dei SIEM è prima importante capire come si è arrivati a questo punto. Come la maggior parte dei sistemi moderni di security per le tecnologie, la storia dei SIEM non è molto lunga. Il primo prodotto SIEM commerciale risale infatti a meno di vent'anni fa, all'inizio del nuovo millennio. L'arrivo della prima generazione di piattaforme SIEM ha inaugurato una nuova alba nel settore della sicurezza dei dati, combinando per la prima volta la gestione degli eventi di sicurezza con la gestione delle informazioni di sicurezza, qualcosa che ancora non si era visto prima. Tuttavia, queste piattaforme SIEM 1.0 avevano il problema enorme di scalare solo verticalmente, cosa che ne ha limitato fortemente la crescita. Essendo richiesto un hardware sempre più grande per gestire i carichi di dati, arrivare ad un limite di gestione di I/O diventa inevitabile, e a quel punto la scalabilità si interrompe.

La seconda generazione di SIEM, rilasciata circa nel 2011, arriva giusto in tempo e non sorprende che la principale differenza rispetto al SIEM 1.0 sia la scalabilità, abbandonando il database centralizzato e utilizzando invece i big data per consentire una scalabilità orizzontale. Il SIEM 2.0 ha inoltre permesso di migliorare la reportistica e i cruscotti, nonché di interrogare per la prima volta i dati storici. Tuttavia, se la scalabilità era la più grande forza del SIEM 2.0, alla fine è diventata anche la sua maledizione. Non perché non funzionasse, ma perché semplicemente spostava il problema più in basso nella pipeline operativa. Prima del SIEM, i professionisti della sicurezza erano essenzialmente ciechi, incapaci di vedere a livello di dati ciò che accadeva nei loro ambienti IT. La prima generazione di SIEM ha dato loro la vista, ma la seconda generazione l'ha tolta di nuovo presentando più dati di quanti ne potessero gestire. Inoltre, non è riuscita a innovare gli aspetti di allerta del SIEM, lasciando i team a dipendere da avvisi preconfigurati che, nel migliore dei casi, si correlavano solo con alcuni elementi. Nella sua nuova e più recente versione introdotta circa nel 2015, il SIEM 3.0, viene aggiunta per la prima volta l'analisi, attraverso l'applicazione del machine learning. Ciò che rende diverso il SIEM 3.0 dalle versioni precedenti, e per la prima volta realmente

viabile, è il passaggio dagli avvisi preconfigurati a un approccio basato sul rischio. Gli avvisi rimangono preziosi quando si cercano fatti semplici e noti, ma nella moderna gestione della sicurezza è altrettanto probabile che i team si trovino di fronte a minacce zero-day sconosciute. Il monitoraggio della sicurezza basato sugli analytics applica tecniche statistiche a quantità enormi di dati per costruire modelli operativi, che sono linee di base per ogni singolo utente ed entità dell'ambiente. Questa tecnica è nota come "user and entity behaviour analytics" (UEBA).[76] [45] [40]

5.1.1 Cosa sono i UEBA

Data la loro importanza e forte impiego all'interno dei sistemi, è importante spiegare di cosa si tratta quando si parla di sistemi UEBA. UEBA è l'acronimo di User and Entity Behavior Analytics (analisi del comportamento degli utenti e delle entità) e in precedenza era noto come user behavior analytics (UBA). L'UEBA utilizza grandi insiemi di dati per modellare i comportamenti tipici e atipici di persone e macchine all'interno di una rete. Definendo tali linee di base, è in grado di identificare comportamenti sospetti, potenziali minacce e attacchi che gli antivirus tradizionali potrebbero non rilevare. Ciò significa che i sistemi UEBA sono in grado di rilevare attacchi non basati su malware perché analizzano vari modelli comportamentali. UEBA utilizza inoltre questi modelli per valutare il livello di minaccia, creando un punteggio di rischio che può aiutare a guidare la risposta appropriata. Sempre più spesso, UEBA utilizza l'apprendimento automatico per identificare i comportamenti normali e segnalare le deviazioni rischiose che suggeriscono minacce interne, movimenti laterali, account compromessi e attacchi.[119] Tornando al discorso dei SIEM, oltre a notare i comportamenti di rete sospetti, i SIEM si sono evoluti fino a includere l'analisi del comportamento di utenti ed entità ed integrando quindi al loro interno i sistemi UEBA. [88]

5.2 Come funzionano i SIEM e quali sono le loro capacità

Al livello più basico, tutte le soluzioni SIEM eseguono un certo livello di funzioni di aggregazione, consolidamento e smistamento dei dati per identificare le minacce e rispettare i requisiti di conformità dei dati. Anche se alcune soluzioni variano in termini di capacità, la maggior parte offre lo stesso set di funzionalità di base:

Log management: Il SIEM acquisisce i dati degli eventi da un'ampia gamma di fonti nell'intera rete di un'organizzazione. I log e i dati di flus-

so provenienti da utenti, applicazioni, risorse, ambienti cloud e reti vengono raccolti, archiviati e analizzati in tempo reale, offrendo ai team IT e di sicurezza la possibilità di gestire automaticamente i log degli eventi e i dati di flusso della rete in un'unica posizione centralizzata. Alcune soluzioni SIEM si integrano anche con feed di threat intelligence di terze parti per correlare i dati di sicurezza interni con le firme e i profili delle minacce precedentemente riconosciuti. L'integrazione con i feed delle minacce in tempo reale consente ai team di bloccare o rilevare nuovi tipi di firme di attacco non precedentemente conosciuti.

Event correlation and analytics: La correlazione degli eventi è una parte essenziale di qualsiasi soluzione SIEM. Utilizzando analisi avanzate per identificare e comprendere modelli di dati intricati, la correlazione degli eventi fornisce approfondimenti per individuare e ridurre rapidamente le potenziali minacce alla sicurezza aziendale. Le soluzioni SIEM migliorano significativamente il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR) per i team di sicurezza IT, scaricando i flussi di lavoro manuali associati all'analisi approfondita degli eventi di sicurezza.

Incident monitoring and security alerts: Poiché consentono la gestione centralizzata dell'infrastruttura on-premise e basata su cloud, le soluzioni SIEM sono in grado di identificare tutte le entità dell'ambiente IT. Ciò consente alla tecnologia SIEM di monitorare gli incidenti di sicurezza tra tutti gli utenti, i dispositivi e le applicazioni connesse, classificando i comportamenti anomali non appena vengono rilevati nella rete. Utilizzando regole di correlazione predefinite e personalizzabili, gli amministratori possono essere avvisati immediatamente e intraprendere le azioni appropriate per mitigare il problema prima che si concretizzi in problemi di sicurezza più significativi.

Compliance management and reporting: Le soluzioni SIEM sono una scelta popolare per le organizzazioni soggette a diverse forme di conformità normativa. Grazie alla raccolta e all'analisi automatizzata dei dati che fornisce, il SIEM è uno strumento prezioso per raccogliere e verificare i dati di conformità nell'intera infrastruttura aziendale. Le soluzioni SIEM possono generare in tempo reale rapporti di conformità per PCI-DSS, GDPR, HIPPA, SOX e altri standard di conformità, riducendo l'onere della gestione della sicurezza e rilevando tempestivamente potenziali violazioni per poterle affrontare. Molte soluzioni SIEM sono dotate di componenti aggiuntivi precostituiti e pronti all'uso, in grado di generare report automatici progettati per soddisfare i requisiti di conformità. [58] [42] [20] [13]

5.3 I benefici dell'utilizzo dei SIEM

Indipendentemente da quali siano le dimensioni di una data organizzazione, adottare misure proattive per monitorare e ridurre i rischi di sicurezza informatica è essenziale. Le soluzioni SIEM offrono alle aziende diversi vantaggi e sono diventate ad oggi una componente fondamentale per semplificare i flussi di lavoro della sicurezza. Tra i vari benefici dati dal loro utilizzo, vediamo subito l'importanza di un riconoscimento avanzato delle minacce in tempo reale. Le soluzioni di monitoraggio su tutta l'infrastruttura riducono in modo significativo il tempo necessario per identificare e reagire a potenziali minacce e vulnerabilità della rete, contribuendo a rafforzare la postura di sicurezza man mano che l'organizzazione si espande. Vediamo inoltre un ottimo controllo della conformità normativa. Le soluzioni SIEM consentono di centralizzare le verifiche di conformità ed i report su un'intera infrastruttura aziendale. L'automazione avanzata semplifica la raccolta e l'analisi dei log di sistema e degli eventi di sicurezza, riducendo l'utilizzo delle risorse interne e rispettando i rigorosi standard di reporting sulla conformità. Rivedendo il discorso del machine learning, vediamo quindi una automazione guidata dall'intelligenza artificiale. Le soluzioni SIEM di nuova generazione si integrano con potenti funzionalità di orchestrazione, automazione e risposta alla sicurezza (SOAR), che consentono ai team IT di risparmiare tempo e risorse nella gestione della sicurezza aziendale.

La conseguenza di tutto quello che abbiamo visto finora è quindi un miglioramento dell'efficienza organizzativa. Grazie alla migliore visibilità degli ambienti IT che offre, il SIEM può essere un fattore essenziale per migliorare l'efficienza interdipartimentale. Con una visione unica e unificata dei dati di sistema e un SOAR integrato, i team possono comunicare e collaborare in modo efficiente quando rispondono agli eventi percepiti e agli incidenti di sicurezza. Considerando la rapidità con cui cambia il panorama della cybersecurity, le organizzazioni devono poter contare su soluzioni in grado di rilevare e rispondere alle minacce alla sicurezza sia note che sconosciute. Utilizzando i feed integrati di threat intelligence e la tecnologia AI, le soluzioni SIEM possono mitigare con successo le violazioni della sicurezza dei giorni nostri, come ad esempio gli attacchi classici del social engineering, tra cui ritorna sempre il phishing, ma anche iniezioni SQL, attacchi DDoS ed esfiltrazioni di dati. Un altro vantaggio enorme dato dall'utilizzo delle soluzioni SIEM è la possibilità di condurre indagini forensi digitali una volta che si verifica un incidente di sicurezza. E' quindi semplice per le organizzazioni raccogliere e analizzare in modo efficiente i dati di log di tutte le risorse digitali in un unico luogo. In questo modo possono ricreare incidenti passati o analizzarne di nuovi per indagare su attività sospette e implementare processi

di sicurezza più efficaci. Abbiamo quindi visto come l'impiego delle soluzioni SIEM offra diversi vantaggi, soprattutto incentrati sul rendere più semplici attività che prima risultavano tediose e dispendiose sia a livello di risorse che di tempistica. [56][114][112][87][11]

5.4 Terminologia e componenti

Per dare delle definizioni corrette e complete è necessario avere ben chiara la terminologia che viene usata per descrivere i SIEM, le capacità che offrono ed i componenti che integrano. Oltre a chiarire diversi termini spiegati in precedenza che potrebbero essere semplici da confondere, introdurremo nuovi termini utili a capire l'infrastruttura dei sistemi SIEM ad un livello di dettaglio maggiore. Oltre alla terminologia vogliamo anche analizzare quali sono le componenti che possono fare parte di un sistema SIEM. Iniziamo quindi con una carrellata di termini a cui attribuire un significato ed una funzione chiara.

- Quando parliamo di *dispositivo*, o device, usiamo questo termine generico per descrivere server, firewall, switch, postazioni di lavoro etc. Il termine dispositivo di rete, o network device, va più in dettaglio e si riferisce a tutti e soli quei dispositivi che interconnettono la rete come firewall, routers, switch, ma esclude invece i server e le postazioni di lavoro. Il termine CMDB sta per configuration management database. Il CMDB lista tutti i dispositivi che stanno inviando dei log al SIEM. Ogni dispositivo nella CMDB mostra il proprio stato di salute oltre al numero corrente di eventi per secondo (EPS).

- Un *data collector*, o collettore di dati, è un dispositivo o server che colleziona diversi tipi di dati fra cui log, eventi, flussi di rete etc. Il collettore di dati procede poi ad inviare i suddetti verso il sistema SIEM. Il Syslog è un protocollo di logging standard che permette ad un dispositivo di inviare dei log ad un server in ascolto. Il server in ascolto può essere un server di log che poi fa forwarding verso il SIEM, oppure può trattarsi direttamente l'host del sistema SIEM. I log inviati contengono un codice che ne specifica la natura ed un livello di gravità. Esistono diversi tipi di Syslog tra cui syslog-ng, rsyslog o syslogd. Un evento è una voce specifica nel file di log che rappresenta un evento particolare, tipo una connessione bloccata o un fallimento di login.

- E' importante anche definire una forte differenza fra *eventi* (e quindi log) ed i *flow*, o flussi, che rappresentano l'attività di rete normalizzando

gli indirizzi IP, le porte, il conteggio dei byte e dei pacchetti e altri dati in record di flusso, che di fatto sono registrazioni di sessioni di rete tra due host. I flow sono specifici del SEIM QRadar, che prendiamo in esempio più avanti.

- *Regola* - Il SIEM analizza gli attributi degli eventi e correla i log con altri dispositivi del SIEM. I registri vengono confrontati con le regole, che cercano uno schema di eventi che corrisponde a criteri specifici. Quando viene individuato uno schema, viene attivato un incidente.

- Un *incidente* è un'istanza unica di una regola. Gli incidenti forniscono la definizione della regola e gli eventi che l'hanno innescata.

- Un *falso positivo* si ha quando si attiva una regola che non rappresenta un vero incidente di sicurezza. Per uno sguardo più approfondito sui falsi positivi, consultate la sezione "Falsi positivi".

- Un'*eccezione* aggiunge una condizione a una regola per evitare che si attivi quando sono soddisfatte condizioni specifiche. Ad esempio, uno scanner di vulnerabilità che viene eseguito regolarmente genererebbe una quantità eccessiva di ticket anche se il traffico è legittimo. Un'eccezione verrebbe aggiunta per ridurre il tasso di falsi positivi creati dallo scanner di vulnerabilità.

- *EPS*, ovvero eventi al secondo che un dispositivo invia al SIEM. Le variazioni di EPS possono indicare che un dispositivo deve essere controllato per problemi di configurazione o di sicurezza.

[9][90][134]

Parliamo ora delle componenti di un sistema SIEM. Le architetture di questi sistemi possono variare a seconda del fornitore, ma generalmente le componenti essenziali che compongono un SIEM sono sempre le stesse. Bisogna tenere a mente che un sistema SIEM è una collezione di elementi distinti fra loro che costruiscono e creano un sistema, piuttosto che una singola applicazione. Queste componenti, che abbiamo anche visto e spiegato in precedenza, sono:

- *Gestione dei registri*: questo componente tratta la raccolta, la gestione e la conservazione dei dati ricevuti. Il SIEM acquisisce sia i dati degli eventi che i dati contestuali. L'architettura SIEM raccoglie fondamentalmente dati di eventi da sistemi organizzati come dispositivi installati, protocolli di rete, protocolli di archiviazione e protocolli di streaming.

- *Normalizzazione dei log*: Il SIEM riceve in ingresso i dati relativi agli eventi e al contesto, ma questi dati non sono ancora illeggibili perché troppo corposi. La normalizzazione è un processo necessario che tratta la trasformazione dei dati degli eventi in informazioni utili per la sicurezza. Questa procedura comprende la rimozione dei dati irrilevanti dai dati ricevuti mediante una procedura di filtraggio. L'aspetto più importante è che solo i dati rilevanti vengono conservati per un esame futuro.

- *Fonti di log*: I dispositivi di cui parlavamo prima, sia di network che non, generano tutti dei log. Questa procedura riguarda essenzialmente il modo in cui le organizzazioni alimentano i registri nel SIEM per la sicurezza.

- *Correlazione dei dati*: I dati devono essere presentati in modo pertinente e organizzato perché vengono acquisiti da dispositivi diversi. La funzione di correlazione aiuta a presentare un quadro più ampio dei dati raccolti da più punti.

- *Monitoraggio in tempo reale*: Gli utenti ricevono informazioni in tempo reale su qualsiasi tipo di violazione della sicurezza. Di conseguenza, la minaccia può essere rintracciata ed eliminata in modo tempestivo ed efficace.

- *Automazione*: Qualsiasi evento può essere reagito automaticamente grazie a SOAR (Security, Orchestration, Automation, and Response), che elimina la necessità di analisti della sicurezza.

- *Dashboards*: I cruscotti SIEM semplificano la comprensione dei cambiamenti nei modelli di dati da parte degli analisti della sicurezza. Di conseguenza, un analista di sicurezza può notare rapidamente e prontamente qualsiasi irregolarità nella rete.

- *Reporting*: Altri amministratori possono utilizzare lo strumento di reporting del SIEM per generare vari report, riducendo l'incertezza sulle loro attività di reporting. Il SIEM genera report rapidamente grazie alla memorizzazione di tutti i dati di log in tabelle di database.

[36][77][138]

5.5 Casi d'uso dei SIEM

Abbiamo già discusso le capacità, la terminologia e le componenti dei sistemi SIEM. Andiamo ora a vedere i casi d'uso di implementazione di questi sistemi. Il ricercatore di sicurezza Chris Kubecka, esperto di cyberwarfrare, ha identificato i seguenti casi d'uso presentandoli alla conferenza di hacking 28C3 (Chaos Communication Congress):[129]

- La visibilità ed il rilevamento di anomalie dei sistemi SIEM può aiutare a prevenire diversi tipi di vulnerabilità di tipo zero-days o codice polimorfico. Questo deriva soprattutto a causa dei bassi tassi di rilevamento degli antivirus contro questo tipo di malware in rapida evoluzione.

- L'analisi, la normalizzazione e la categorizzazione dei log possono avvenire automaticamente, indipendentemente dal tipo di computer o dispositivo di rete, purché sia in grado di inviare un log. Questa è un'altra caratteristica importante dei sistemi SIEM perché gli permette di ingerire quantità enormi di dati che sarebbero, come lo erano nelle prime versioni di questi sistemi, troppo grandi da gestire per i team di sicurezza.

- La visualizzazione di dati con un SIEM utilizzando gli eventi di sicurezza e le anomalie dei registri può aiutare a rilevare dei modelli. Questi modelli possono poi essere raffinati ed utilizzati dagli stessi team di sicurezza per migliorarsi sia in termini di efficacia che di velocità, soprattutto nel rilevare anomalie di sicurezza.

- Le anomalie di protocollo, che possono indicare una configurazione errata o un problema di sicurezza, possono essere identificate con un SIEM utilizzando il rilevamento di pattern, gli avvisi, la baseline e le dashboard. Ciò permette ad un sistema di SIEM di rilevare potenziali configurazioni errate di dispositivi, che potrebbero poi portare a grandi falle di sicurezza all'interno di una organizzazione.

- I sistemi SIEM sono in grado di rilevare comunicazioni occulte e dannose e canali criptati. Questa capacità si rivela molto utile, soprattutto nel caso di pericoli di insider threats, che possono così essere sventati velocemente e senza danni per l'azienda.

- I SIEM possono addirittura rilevare con precisione le guerre informatiche, individuando sia gli aggressori che le vittime. Diversi paesi nel mondo hanno interessi in questo tipo di attività e già diverse guerre

informatiche sono attive in questo momento. I SIEM si rivelano quindi uno strumento essenziale anche per entità governative, siano o meno queste coinvolte in questo tipo di attività.

[135] [75] [35]

Capitolo 6

Progettazione, installazione, configurazione e manutenzione di un sistema SIEM

In questo capitolo procederemo con una dimostrazione di progettazione, installazione, configurazione e manutenzione di un sistema SIEM. Il sistema scelto, come parte del tirocinio svolto con il team di sicurezza dell'Università degli studi di Parma, è QRadar SIEM Community Edition fornito da IBM. Questa edizione particolare di QRadar è una versione gratuita e completa, a bassa memoria e basso EPS, che include una licenza perpetua. Questa versione è limitata a 50 eventi al secondo e a 5.000 flussi di rete al minuto, supporta le app, ma si basa su un'impronta più piccola per un uso non aziendale. Nonostante queste limitazioni fornisce comunque una base solida su cui lavorare ed il workflow relativo alla progettazione ed i passi successivi rimane lo stesso dell'edizione completa.

6.1 L'architettura di IBM QRadar

Prima di tutto vediamo come è strutturata l'architettura del SIEM: QRadar raccoglie, elabora, aggrega e archivia i dati di rete in tempo reale. Utilizza poi questi dati per gestire la sicurezza della rete fornendo informazioni e monitoraggio in tempo reale, avvisi e offese e risposte alle minacce di rete. Si tratta di un'architettura modulare che fornisce visibilità in tempo reale dell'infrastruttura IT, utilizzabile per il rilevamento delle minacce e la definizione delle priorità. È possibile scalare QRadar per soddisfare le esigenze di raccolta e analisi di log e flussi ed è anche possibile aggiungere moduli integrati alla piattaforma, come QRadar Risk Manager, QRadar Vulnera-

bility Manager e QRadar Incident Forensics, disponibili però nella versione completa del prodotto.

Il funzionamento della piattaforma di intelligence di sicurezza QRadar è costituito da tre livelli e si applica a qualsiasi struttura di implementazione QRadar, indipendentemente dalle sue dimensioni e dalla sua complessità. Il diagramma seguente mostra i livelli che compongono l'architettura di QRadar.

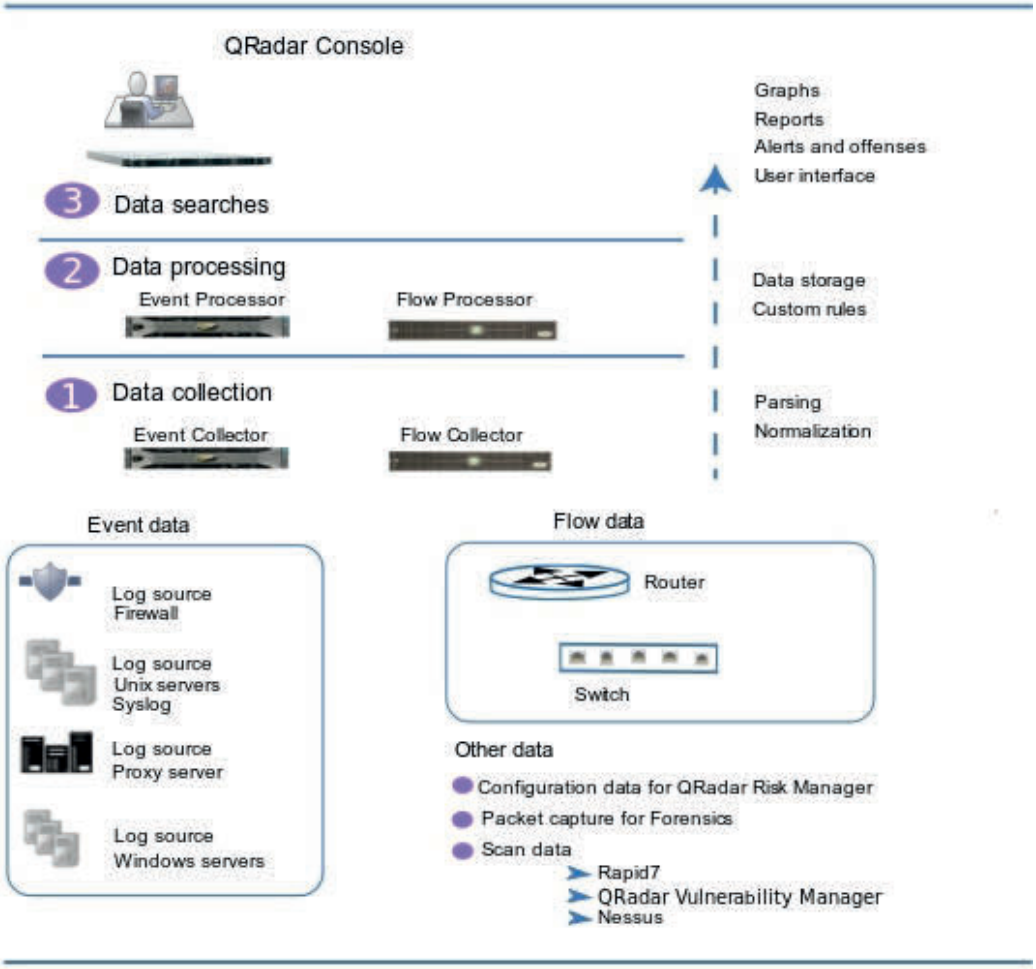


Figura 6.1: I livelli architetturali di QRadar

I tre livelli visti rappresentano le funzionalità principali di qualsiasi sistema QRadar.

6.1.1 Data collection:

La raccolta dei dati è il primo livello, in cui vengono raccolti dati come eventi o flussi dalla rete. L'appliance All-in-One può essere utilizzata per raccogliere i dati direttamente dalla rete oppure si possono utilizzare collettori come QRadar Event Collectors o QRadar QFlow Collectors per raccogliere i dati di eventi o flussi. I dati vengono analizzati e normalizzati prima di passare al livello di elaborazione. Quando i dati grezzi vengono analizzati, vengono normalizzati per presentarli in un formato strutturato e utilizzabile.

La funzionalità principale di QRadar si concentra principalmente sulla raccolta dei dati degli eventi e sulla raccolta dei flussi, detti anche flows ed events. E' necessario delineare una distinzione fra le due cose: i dati degli eventi rappresentano gli eventi che si verificano in un determinato momento nell'ambiente dell'utente, come ad esempio i login degli utenti, le e-mail, le connessioni VPN, i dinieghi dei firewall, le connessioni proxy e qualsiasi altro evento che si desidera registrare nei registri dei dispositivi. I dati di flusso sono invece informazioni sulle attività di rete o sulle sessioni tra due host di una rete, che QRadar traduce in record di flusso. QRadar traduce o normalizza i dati grezzi in indirizzi IP, porte, conteggi di byte e pacchetti e altre informazioni in record di flusso, che rappresentano effettivamente una sessione tra due host.

6.1.2 Data processing:

Dopo la raccolta dei dati, il secondo livello o livello di elaborazione dei dati è quello in cui i dati degli eventi e i dati di flusso vengono fatti passare attraverso il Custom Rules Engine (CRE), che genera infrazioni e avvisi, e quindi i dati vengono scritti nell'archivio.

I dati degli eventi e i dati di flusso possono essere elaborati da un dispositivo All-in-One senza la necessità di aggiungere processori di eventi o processori di flusso. Se la capacità di elaborazione dell'appliance All-in-One viene superata, potrebbe essere necessario aggiungere processori di eventi, processori di flusso o qualsiasi altra appliance di elaborazione per gestire i requisiti aggiuntivi. Potrebbe anche essere necessaria una maggiore capacità di archiviazione, che può essere gestita aggiungendo Data Nodes.

6.1.3 Data searches:

Nel terzo livello, o livello superiore, i dati raccolti ed elaborati da QRadar sono a disposizione degli utenti per ricerche, analisi, reportistica, avvisi o indagini sui reati. Gli utenti possono effettuare ricerche e gestire le attività

di amministrazione della sicurezza per la propria rete dall'interfaccia utente della QRadar Console. In un sistema All-in-One, tutti i dati vengono raccolti, elaborati e archiviati sull'appliance All-in-One. Negli ambienti distribuiti, la QRadar Console non esegue l'elaborazione degli eventi e dei flussi, né l'archiviazione. Al contrario, la QRadar Console viene utilizzata principalmente come interfaccia utente e gli utenti possono utilizzarla per ricerche, report, avvisi e indagini.[59]

6.2 Scelta della distribuzione

Quando si vuole installare un sistema SIEM in una organizzazione occorre prima di tutto iniziare con la distribuzione del sistema stesso. L'architettura di IBM QRadar supporta implementazioni di varie dimensioni e topologie, da un'implementazione a host singolo, in cui tutti i componenti software vengono eseguiti su un unico sistema, a host multipli, in cui le appliance come Event Collector e Flow Collector, i Data Nodes, App Host, Event Processors e Flow Processors, hanno ruoli specifici e si trovano su macchine diverse. Prima di pianificare l'implementazione, considerate le seguenti domande: In che modo l'azienda utilizza Internet? Si utilizza l'upload tanto quanto il download? Quanti eventi al secondo (EPS) e flussi al minuto (FPM) è necessario monitorare? Quante informazioni è necessario memorizzare e per quanto tempo?[59]

La tipologia più utilizzata di distribuzione per una organizzazione di media dimensione, sulla quale ci focalizziamo, è quella dell' All-in-One. Un'appliance All-in-One include le funzionalità di raccolta, elaborazione, archiviazione, monitoraggio, ricerca, reporting e gestione delle infrazioni, tutte sulla stessa macchina. Il seguente diagramma mostra i componenti di QRadar che possono essere utilizzati per raccogliere, elaborare e archiviare i dati degli eventi e dei flussi nell'implementazione di QRadar.[55]

L'Event Collector raccoglie i dati degli eventi dalle fonti di log della rete e li invia all'Event Processor. Il Flow Collector raccoglie i dati di flusso dai dispositivi di rete, come una porta SPAN dello switch, e li invia al Flow Processor. Entrambi i processori forniscono i dati ai collettori e alla QRadar Console. Le appliance del processore possono memorizzare i dati, ma possono anche utilizzare i Data Nodes per memorizzarli. L'appliance QRadar Console viene utilizzata per il monitoraggio, la ricerca dei dati, la creazione di report, la gestione delle infrazioni e l'amministrazione dell'implementazione QRadar.[59]

Nel nostro caso, all'interno dell'Ateneo, si è deciso di scegliere la distribuzione di un appliance All-in-One all'interno della facoltà di matematica, che

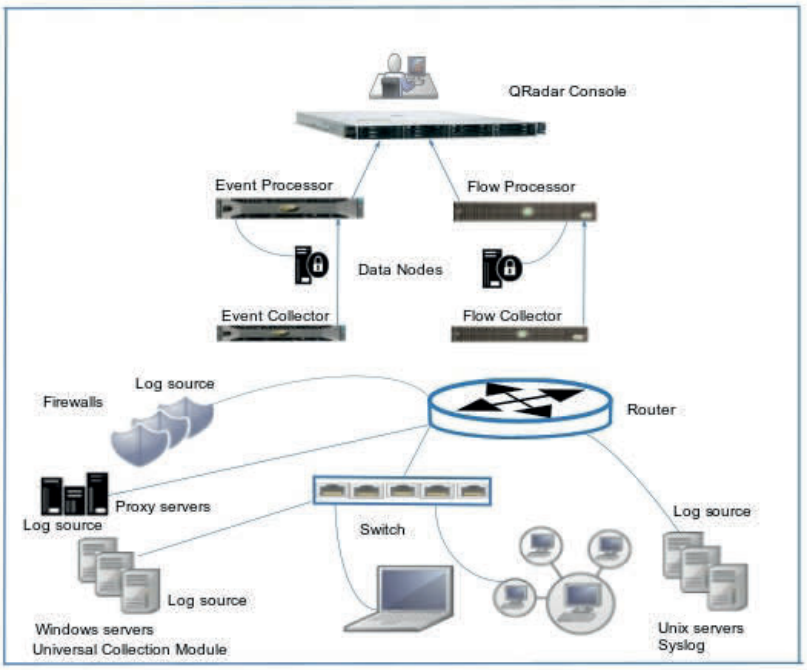


Figura 6.2: Le componenti di QRadar

dispone di diverse macchine potenti per il calcolo e per la ricerca. Una macchina è stata quindi dedicata interamente all'appliance di QRadar. Si è deciso anche di creare su una macchina differente un honeypot, utilizzando Artillery, da collegare successivamente a QRadar. Lo scopo di Artillery è quello di fornire una combinazione di honeypot, monitoraggio del file-system, rafforzamento del sistema, raccoglimento di informazioni sulle minacce in tempo reale e strumento di salute e monitoraggio del server; per creare un modo completo di proteggere un sistema. Il progetto Artillery è stato scritto per essere un'aggiunta alla sicurezza di un server e rendere molto difficile per gli aggressori penetrare in un sistema. Questa scelta è stata fatta perché non essendo possibile configurare decine di macchine e workstation per inviare log verso il SIEM, si può ovviare il problema avendo una singola macchina che attiri l'attenzione dalle altre e comunichi con il SIEM per la gestione della sicurezza dell'intero network. In un caso più realistico, tutte le macchine collegate alla rete dovrebbero inviare i log verso il SIEM, ma qui trattiamo un caso semplificato. Si è ottenuta quindi una progettazione dove la macchina honeypot funge da flow ed event collector, dove QRadar è invece il flow ed event processor, per poi poter visualizzare i dati normalizzati sulla dashboard.

6.3 Installazione

L'installazione del sistema menzionato sopra comincia quindi con l'installazione dell'appliance di QRadar su una macchina apposita, che utilizza come sistema operativo una distribuzione recente di Ubuntu Desktop. La Community Edition (CE) di QRadar viene fornita sotto forma di file .ova, utilizzabile da applicazioni di virtualizzazione come VMware Workstation o Oracle VirtualBox. Si procede quindi con la creazione di una macchina virtuale, importando il file .ova precedentemente scaricato, tramite VirtualBox a riga di comando dando per scontato di essere collegati alla macchina in questione tramite SSH.

```
$ vboxmanage import QRadar.ova
0\%...10\%...20\%...30\%...40\%...50\%...60\%...70\%...80\%...90\%...100\%
Interpreting /home/user/Downloads/QRadar.ova...
OK.
Disks:
   vmdisk1       250     4362338304     http://www.vmware.com/interfaces/specifications/vmdk.html#streamOptimized
         QCE-jan22-disk1.vmdk     3441993728     -1

Virtual system 0:
 0: Suggested OS type: "RedHat_64"
    (change with "--vsys 0 --ostype <type>"; use "list ostypes" to list all possible values)
 1: Suggested VM name "vm 1"
    (change with "--vsys 0 --vmname <name>")
 2: Suggested VM group "/"
    (change with "--vsys 0 --group <group>")
 [...]
12: Hard disk image: source image=QCE-jan22-disk1.vmdk, target path=QCE-jan22-disk1.vmdk, controller=10;port=0
    (change target path with "--vsys 0 --unit 12 --disk path";
     change controller with "--vsys 0 --unit 12 --controller <index>";
     change controller port with "--vsys 0 --unit 12 --port <n>";
     disable with "--vsys 0 --unit 12 --ignore")
0\%...10\%...20\%...30\%...40\%...50\%...60\%...70\%...80\%...90\%...100\%
```

```
22 Successfully imported the appliance.
```

Tramite il comando `vboxmanage list vms` ora possiamo vedere la macchina virtuale creata: `"vm" {e860195d-1c0e-44dc-99a3-0fa6105ec828}`

Non è importante il nome della macchina assegnata, quindi lo si può lasciare invariato. A questo punto è necessario, se si utilizza una macchina virtuale ospitata localmente con un indirizzo IP locale, inoltrare la porta 8444 alla porta 443 per accedere a QRadar nel browser web ed inoltrare la porta 2222 alla porta 22 per utilizzare ssh per connettersi alla macchina di QRadar. Questo passaggio però non è necessario nel caso si dovesse utilizzare una impostazione di networking della macchina virtuale di tipo bridged, come nel nostro caso. Con la rete di tipo bridged la macchina virtuale è accessibile dalla rete ed è sufficiente assegnarle un IP statico tramite DHCP, di modo che ad ogni riavvio l'indirizzo IP rimanga sempre lo stesso. Se la rete è di tipo NAT, invece, condivide la connessione di rete dell'host assegnando alle macchine virtuali un indirizzo IP da una rete privata e traduce le richieste di rete del guest. In questo modo l'host appare come un unico sistema alla rete. L'installazione procede poi avviando la macchina virtuale tramite:

`vboxmanage startvm vm`

Collegandosi a quest'ultima, eseguendo il login come root, impostando una password ed infine inserendo poi il comando `./setup` . Una volta completato questo passaggio basta accettare i termini e condizioni e l'installazione inizierà il suo corso. Terminata l'installazione la macchina avvierà i servizi necessari e la dashboard tramite interfaccia web sarà disponibile all'indirizzo IP della macchina host.

Figura 6.3: La schermata di login di QRadar

Una volta effettuato l'accesso, tramite un account admin e non più quello di root che rimarrà inutilizzato per motivi di sicurezza, vediamo una presentazione dell'interfaccia web di QRadar. Possiamo notare subito due tab importanti da cui visualizzeremo i dati che ci interessano: log activity e network activity. Queste due sezioni sono dedicate rispettivamente agli eventi, quelli ottenuti dai log delle macchine esterne che inviano informazioni ed interni a QRadar, e ai flussi di rete, ottenuti invece da routers, switch, TAP nella rete, ma anche macchine configurate per inviare questo tipo di informazioni.

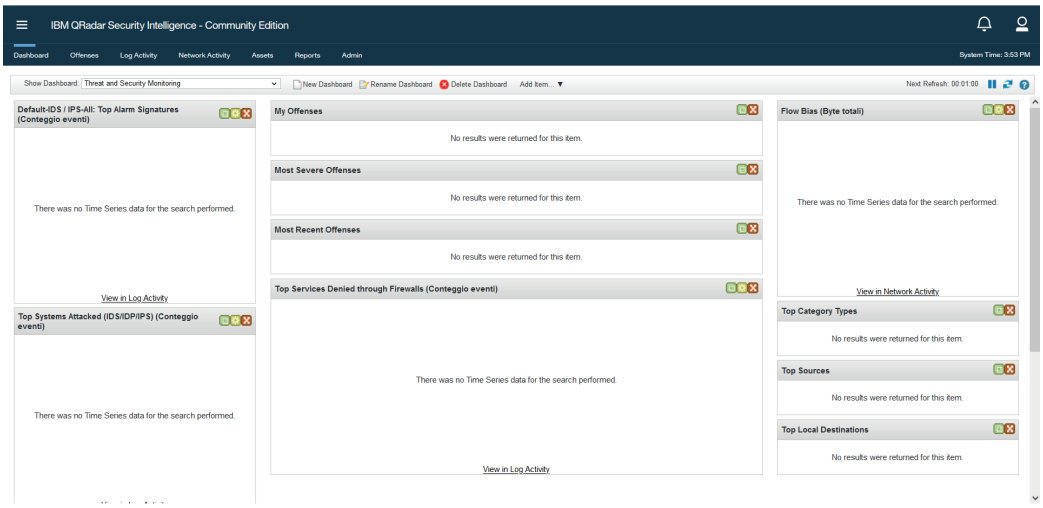


Figura 6.4: La dashboard di QRadar

Passiamo ora all'installazione del honeypot: come detto in precedenza si utilizza Artillery e la sua installazione è molto semplice. Partendo dalla macchina su cui si vuole installare l'applicazione, usiamo git per clonare la repository:

```
sudo git clone https://github.com/BinaryDefense/artillery
```

Successivamente, entriamo nella directory creata (cd artillery) e proseguiamo scrivendo `./setup`. In questo modo Artillery verrà installato in `/var/artillery` e tutte le sue funzionalità possono essere modificate dal file di configurazione di nome "config" presente nella directory di installazione. Il risultato delle nostre installazioni porta ad una mappa topografica della rete del tipo visibile nella figura seguente.

Per una organizzazione generica di dimensioni medie il processo di installazione risulta lo stesso in termini di installazione dell'appliance di QRadar SIEM. Riguardo alle altre componenti, come firewall, switch, server, honeypot ed in generale qualunque macchina il cui compito specifico sia di comunicare con il SIEM per un motivo o per l'altro, avranno la propria installazione

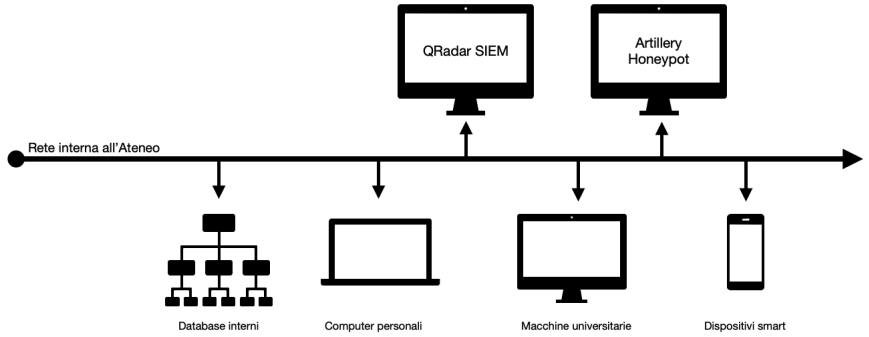


Figura 6.5: Esempio topografia rete di Ateneo

da seguire. Genericamente ogni workstation è impostata per inviare eventi a QRadar mentre switch e router sono configurati per inviare i flussi di rete.

6.4 Configurazione

La configurazione del sistema di QRadar, quella necessaria per il suo funzionamento, avviene in automatico. Di base, per avere accesso a QRadar SIEM e la sua interfaccia web, non ci sono passi specifici di configurazione da seguire, oltre al setup iniziale dell'appliance. In questo caso però intendiamo la parte di configurazione come i passi necessari a configurare la comunicazione fra le varie macchine. Prima di procedere però occorre menzionare un problema che affligge la versione corrente di QRadar SIEM Community Edition ed altre versioni complete dell'appliance: delle modifiche apportate a QRadar il 31 dicembre 2020 possono avere (e di fatto lo hanno) un impatto sulla funzionalità del prodotto.[60] Il risultato è che anche dopo aver configurato correttamente la comunicazione fra le macchine da cui si vogliono estrapolare dati e QRadar stesso, l'interfaccia web non mostrerà nessun dato. Una patch è stata rilasciata da IBM che permette la risoluzione del problema. E' sufficiente essere collegati alla macchina host di QRadar tramite SSH ed eseguire uno dei seguenti comandi, dipendenti dalla versione che si utilizza. Una volta fatto ciò, un semplice riavvio dell'interfaccia web risolverà il problema.

Vediamo la versione per QRadar Community Edition:

```
1 \if [ -f /opt/qradar/ecs/license.txt ] ; then echo -n "
    QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc
    :12/31/20" > /opt/qradar/ecs/license.txt ; fi ; if [ -f
    /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/
```

```
license.txt ] ; then echo -n "QRadar:Q1 Labs Inc
.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/
ibm/si/services/ecs-ec-ingress/current/eventgnosis/
license.txt ; fi ; if [ -f /opt/ibm/si/services/ecs-ep/
current/eventgnosis/license.txt ] ; then echo -n "QRadar
:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc
:12/31/20" > /opt/ibm/si/services/ecs-ep/current/
eventgnosis/license.txt ; fi ; if [ -f /opt/ibm/si/
services/ecs-ec/current/eventgnosis/license.txt ] ; then
 echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:
WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/ibm/si/services/
ecs-ec/current/eventgnosis/license.txt ; fi ; if [ -f /
usr/eventgnosis/ecs/license.txt ] ; then echo -n "QRadar
:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc
:12/31/20" > /usr/eventgnosis/ecs/license.txt ; fi ; if
[ -f /opt/qradar/conf/templates/ecs_license.txt ] ; then
 echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:
WnT9X7BDFOgB1WaXwokODc:12/31/20" > /opt/qradar/conf/
templates/ecs_license.txt ; fi
```

E' possibile ora continuare con la configurazione delle macchine di modo da stabilire una connessione fra loro. Questo significa configurare QRadar di modo da poter ricevere eventi e flussi dalle altre macchine, o nel nostro caso Artillery, e le altre macchine di modo da poter inviare gli stessi eventi e flussi verso l'appliance di QRadar.

6.4.1 Configurazione di QRadar e Artillery per eventi

Per configurare le due applicazioni di modo da comunicare fra loro sono necessari due passaggi, uno per ognuna delle due appliance. Prima di tutto bisogna abilitare QRadar alla ricezione dei suddetti eventi, e per farlo, bisogna aggiungere una fonte per questi dati ovvero un log source. Questo significa dirigersi nel pannello admin, poi data sources, log sources e cliccare add per aggiungere una nuova fonte di log.

Dobbiamo innanzi a tutto fornire un nome per la fonte, poi fornire l'indirizzo IP dalla quale ci si aspetta di ricevere il contenuto. Bisogna anche selezionare il tipo di fonte, che in questo caso utilizza il protocollo syslog (RSyslog per la precisione), e sarà quindi di tipo Linux OS. Una volta completato questo passo, di nuovo nella tab Admin, ci basta cliccare su deploy changes ed aspettare che le modifiche abbiano effetto. QRadar è ora correttamente configurato alla ricezione di eventi (o log). E' importante notare che

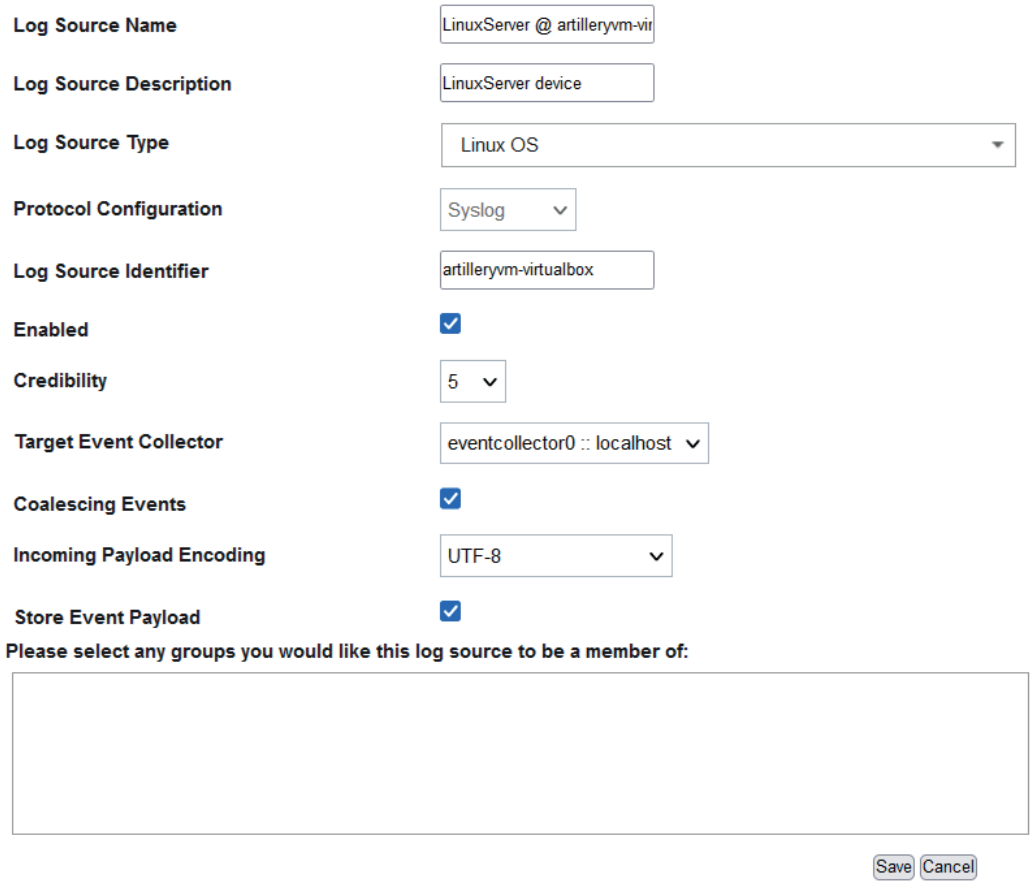


Figura 6.6: Aggiunta di una fonte di log

questo procedimento è da ripetersi per ogni diversa fonte di log che si vuole configurare.

Riguardo alla configurazione del Syslog e Artillery per l'invio dei file di log, vogliamo che la macchina inoltri sia i log di Artillery che quelli della macchina stessa verso QRadar. Per farlo, avremo i log di Artillery mandati in pipe verso i log di sistema, che a loro volta saranno inoltrati al SIEM tramite il protocollo RSyslog. Bisogna quindi collegarsi tramite SSH alla macchina host dell'applicazione e poi controllare che RSyslog, il protocollo di comunicazione scelto, sia presente sul sistema. Per farlo possiamo digitare:

```
$ systemctl status rsyslog
```

```
1 rsyslog.service - LSB: enhanced syslogd
2      Loaded: loaded (/etc/init.d/rsyslog; generated)
3      Active: active (exited) since Tue 2023-02-14 11:00:35
   CET; 26min ago
```

```
4          Docs: man:systemd-sysv-generator(8)
5       Process: 1785 ExecStart=/etc/init.d/rsyslog start (code
    =exited, status=0/SUCCESS)
6
7 Feb 14 11:00:35 ***** systemd[1]: Starting LSB: enhanced
    syslogd...
8 Feb 14 11:00:35 ***** systemd[1]: Started LSB: enhanced
    syslogd.
```

Una volta verificata la presenza del protocollo, dobbiamo modificare il file contenente la configurazione del syslog, usando:

`sudo nano /etc/rsyslog.conf`

aggiungiamo le seguenti righe sul fondo del file di testo:

```
1 #####QRADAR CONNECTION#####
2 module(load="imtcp")
3 input(type="imtcp" port="514")
4 #module(load="imudp")
5 #input(type="imdup" port="514")
6 *.*@@192.168.50.252:514 #Connessione di tipo TCP
7 #*.*@192.168.50.252:514  #COnnessione di tipo UDP
```

Questa modifica nel file di configurazione del protocollo di configurazione farà di modo che i log di sistema vengano reindirizzati all'appliance di QRadar, che è stata configurata per ricevere i suddetti eventi sulla porta 514. E' necessario infine accedere al file di configurazione di Artillery (presente in /var/artillery) per poter reindirizzare in pipe i log dell'applicazione in direzione localhost di modo che questi vengano poi inviati al SIEM. Ultimo passo è quello di eseguire un restart del protocollo di comunicazione syslog tramite console, systemctl restart rsyslog, e di avviare il servizio di Artillery tramite ./restart-server. Per controllare la corretta funzionalità del honeypot possiamo digitare

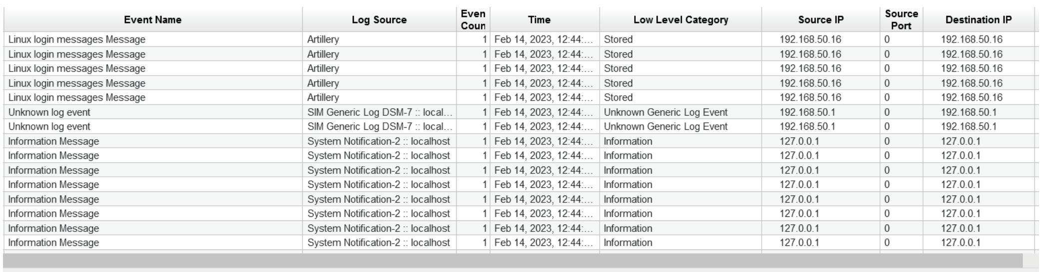
```
$ sudo netstat -nlp | grep python
```

e dovremmo vedere che diversi processi Python sono in ascolto su diverse porte:

```
1     tcp   0   0   0.0.0.0:5900     0.0.0.0:*   LISTEN   9020/
    python3
2     tcp   0   0   0.0.0.0:110      0.0.0.0:*   LISTEN   9020/
    python3
```

```
  tcp  0  0  0.0.0.0:10000  0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:8080   0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:21     0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:1433   0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:1337   0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:25     0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:44443  0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:1723   0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:445    0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:3389   0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:135    0.0.0.0:*  LISTEN  9020/
python3
  tcp  0  0  0.0.0.0:5800   0.0.0.0:*  LISTEN  9020/
python3
```

Se tutto è andato a buon fine, accedendo ora all'interfaccia web di QRadar e cliccando sulla tab "Log Activity", dovrebbero ora apparire una serie di eventi sia interni alla macchina, sia da parte della macchina host di Artillery.



Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP
Linux login messages Message	Artillery	1	Feb 14, 2023, 12:44:...	Stored	192.168.50.16	0	192.168.50.16
Linux login messages Message	Artillery	1	Feb 14, 2023, 12:44:...	Stored	192.168.50.16	0	192.168.50.16
Linux login messages Message	Artillery	1	Feb 14, 2023, 12:44:...	Stored	192.168.50.16	0	192.168.50.16
Linux login messages Message	Artillery	1	Feb 14, 2023, 12:44:...	Stored	192.168.50.16	0	192.168.50.16
Linux login messages Message	Artillery	1	Feb 14, 2023, 12:44:...	Stored	192.168.50.16	0	192.168.50.16
Unknown log event	SIM Generic Log DSM-7 :: local...	1	Feb 14, 2023, 12:44:...	Unknown Generic Log Event	192.168.50.1	0	192.168.50.1
Unknown log event	SIM Generic Log DSM-7 :: local...	1	Feb 14, 2023, 12:44:...	Unknown Generic Log Event	192.168.50.1	0	192.168.50.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1
Information Message	System Notification-2 :: localhost	1	Feb 14, 2023, 12:44:...	Information	127.0.0.1	0	127.0.0.1

Figura 6.7: Scheda log activity

Un'ulteriore modo di testare che le due macchine comunichino è utilizzare il comando logger, per generare log che saranno poi spediti da RSyslog verso

la macchina QRadar. Bisogna prima però mettere in ascolto la macchina di QRadar, da console, usando tcpdump. I comandi saranno quindi:

Sulla macchina host di QRadar:

```
sudo tcpdump -i enp0s17 host 192.168.50.16
```

Sulla macchina artillery:

```
logger -n 192.168.50.252 -P 514 Test
```

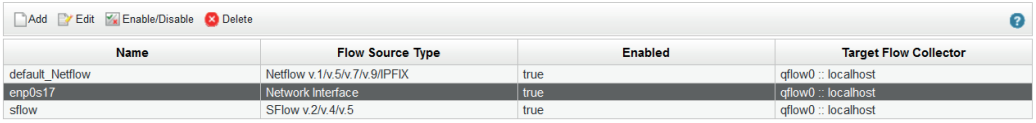
In output dalla console di QRadar, quando lanciamo il comando diverse volte, vediamo che i messaggi vengono ricevuti e questo ci conferma che le due macchine stanno comunicando.

```
1 E... ..@.@.FS..2 ...2..... ...<13>1 2023-02-15T12
    :02:10.640449+01:00 ********** - - [timeQuality
    tzKnown="1" isSynced="1" syncAccuracy="421500"] Test
2 12:02:09.578836 IP (tos 0x0, ttl 64, id 19298, offset 0,
    flags [DF], proto UDP (17), length 163)
3     ********.54669 > localhost.localdomain.514: SYSLOG,
    length: 135
4         Facility user (1), Severity notice (5)
5         Msg: 1 2023-02-15T12:02:10.961475+01:00 ******** **
    **- - [timeQuality tzKnown="1" isSynced="1" syncAccuracy
    ="421500"] Test
6 E...Kb@.@.....2 ...2....../<13>1 2023-02-15T12
    :02:10.961475+01:00 ********** - - [timeQuality
    tzKnown="1" isSynced="1" syncAccuracy="421500"] Test
```

6.4.2 Configurazione dei flussi di rete

Oltre alla configurazione degli eventi sappiamo che è inoltre possibile configurare i flussi di rete così che le connessioni vengano monitorate da QRadar e appaiano nella sezione "Network Activity". Come visto in precedenza ci sono diversi metodi per raccogliere questo tipo di flussi, dalla possibilità di utilizzare protocolli come SFlow o JFlow, a poter monitorare le connessioni direttamente dalla scheda di rete utilizzata dall'appliance. Vediamo come popolare la network activity usando la scheda di rete: bisogna per prima cosa nuovamente dirigersi nel pannello Admin e cliccare su Flows, e poi Flows Sources. Una scheda nuova si aprirà dove sarà possibile configurare la fonte per i flussi di rete.

Una volta completato questo passaggio è sufficiente, come già fatto prima, utilizzare il comando di deploy per effettuare le modifiche e, una volta completate, possiamo dirigerci sulla pagina di network activity che sarà ora



Name	Flow Source Type	Enabled	Target Flow Collector
default_Netflow	Netflow v.1/v.5/v.7/v.9/IPFIX	true	qflow0 :: localhost
enp0s17	Network Interface	true	qflow0 :: localhost
sflow	SFlow v.2/v.4/v.5	true	qflow0 :: localhost

Figura 6.8: Aggiunta di una fonte di flow

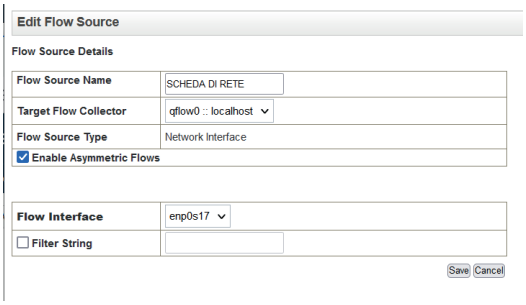


Figura 6.9: Utilizzo della scheda di rete per il monitoring

popolata da tutte le informazioni che la nostra scheda di rete rileva. E' possibile aggiungere diverse fonti, soprattutto se è presente la necessità di monitorare diverse sottoreti, ma per evitare ridondanza abbiamo evitato questa strada.

Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source
	Feb 14, 20...	192.168.50.252	39414	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	38278	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	34207	192.168.50.1	53	udp_ip	Misc.domain	90 (C)	140 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	55945	192.168.50.1	53	udp_ip	Misc.domain	85 (C)	162 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.1	N/A	224.0.0.1	N/A	igmp	Other	192 (C)	0	3	0	N/A	localhost
	Feb 14, 20...	192.168.50.252	59376	192.168.50.1	53	udp_ip	Misc.domain	85 (C)	162 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.16	60926	192.168.50.252	514	udp_ip	Misc.Syslog	115 (C)	0	1	0	N/A	localhost
	Feb 14, 20...	192.168.50.252	54375	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	41290	192.168.50.1	53	udp_ip	Misc.domain	85 (C)	162 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.16	45263	192.168.50.252	514	udp_ip	Misc.Syslog	106 (C)	0	1	0	N/A	localhost
	Feb 14, 20...	192.168.50.252	54022	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	40498	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	38649	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.16	48337	192.168.50.252	514	udp_ip	Misc.Syslog	132 (C)	0	1	0	N/A	localhost
	Feb 14, 20...	192.168.50.252	41906	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	42255	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	56223	192.168.50.1	53	udp_ip	Misc.domain	136 (C)	159 (C)	1	1	N/A	localhost
	Feb 14, 20...	192.168.50.252	41745	192.168.50.1	53	udp_ip	Misc.domain	85 (C)	162 (C)	1	1	N/A	localhost

Figura 6.10: Scheda network activity

6.5 Manutenzione

Vediamo ora la parte di responsabilità per la manutenzione e le attività di amministrazione comuni. La maggior parte degli scenari di manutenzione o amministrazione personalizzata è definita come un'attività che può essere eseguita nell'interfaccia utente o qualsiasi personalizzazione che non rientra

nella Documentazione IBM per QRadar. Se è necessario eseguire una configurazione o un processo che non è descritto nella documentazione, si tratta probabilmente di una configurazione personalizzata e non di un problema del prodotto, come l'aggiunta di cron job o la modifica di file. La maggior parte dei lavori di manutenzione relativi a QRadar si limitano però a riprendere le configurazioni che abbiamo visto in precedenza ed applicarle per diversi servizi. Questo avviene principalmente nel caso si volesse espandere la propria rete aziendale e quindi aggiungere macchine, routers, dispositivi TAP o altro, di modo che anch'essi siano in grado di comunicare con QRadar e fornire informazioni utili agli analisti.

Vediamo una lista di lavori di manutenzione che si possono presentare in diverse occasioni quando si sta mantenendo un SIEM complesso come QRadar:

- Rimozione di dati di eventi o flussi diversi da quelli configurati nei bucket di conservazione.
- Amministratori che chiedono al Supporto QRadar di aprire porte, aggiornare iptables o aggiungere cron job alle appliance.
- Richieste di casi per la modifica di file o l'implementazione di workaround per funzionalità non incluse nella Documentazione IBM.
- Modifica dell'interfaccia utente.
- Creazione di script personalizzati per l'esecuzione di attività per gli amministratori.
- Richieste di aggiornamento o gestione dell'implementazione di QRadar, come ad esempio:
- Pulizia delle fonti di log inutilizzate.
- Aggiunta e configurazione di host gestiti per gli amministratori quando non vengono segnalati errori.
- Revisione, pulizia o manutenzione dei dati dei set di riferimento.
- Richieste di monitoraggio dello spazio su disco, eliminazione di dati o spostamento di dati tra le appliance QRadar.
- Esecuzione di aggiornamenti della gerarchia di rete per gli amministratori.

- Richieste di testare le fonti di log funzionanti per scopi di audit o di convalida dei dati.
- Creare percorsi statici.
- Mantenere o aggiornare gli indirizzi IP o completare le modifiche DNS per gli amministratori.
- Manutenzione delle regole.
- Aggiornamenti o manutenzione delle Proprietà evento personalizzate (CEP)
- Pianificazione, modifica dei report o aggiornamento del layout dei report per gli amministratori.
- Rimozione degli agenti WinCollect o aggiornamento dei parametri di configurazione di WinCollect nell'interfaccia utente.
- Risoluzione di problemi implementati da fornitori terzi o implementati dai Security Experts Labs.

Un esempio di manutenzione che abbiamo visto in sede di tirocinio in Ateneo è stato quello della creazione di una regola che attribuisce l'output di un determinato log di Artillery, in particolare dove viene scritto in output che un attacco ad un range di porte è stato rilevato, ad una offense, ovvero un rischio di compromissione per il sistema.

6.6 Sperimentazione ed attacchi

Per la parte di sperimentazione, dopo aver eseguito tutti i passi visti in precedenza, si è scelto di monitorare la rete per controllarne la situazione di normalità e sicurezza. Il risultato è stato soddisfacente in quanto la rete di ateneo è risultata sicura e priva di qualsiasi tipo di attacco in un periodo di qualche mese. Per questo motivo, si è scelto di simulare diversi attacchi al honeypot installato e di vedere come si può rilevare la presenza del suddetto tramite QRadar per poi agire di conseguenza e mitigare l'attacco. Questi attacchi sono volti a simulare le tre fasi fondamentali che un hacker seguirebbe nel caso di un reale attacco:

- Ricognizione
- Penetrazione della macchina

- Modifica dei file interni al sistema

L'idea è stata di prendere una macchina interna alla rete e quindi priva di sospetti, per poi eseguire da essa uno scan completo (host, porte, servizi) del honeypot. Questo procedimento è volto a simulare la fase di ricognizione che un attaccante svolgerebbe in preparazione ad un possibile attacco all'infrastruttura dell'ateneo. E' stato scelto di utilizzare una macchina interna alla rete di ateneo per via della protezione di quest'ultima da parte di una VPN. Per eseguire l'attacco si è scelto uno strumento comunemente usato dagli hacker per la ricognizione chiamato NMAP, che vediamo fra poco nel dettaglio.

Un secondo tipo di attacco che si è voluto testare nei confronti del honeypot è quello di una connessione tramite SSH dalla macchina "infetta". Dopo aver applicato la buona pratica di cambiare la porta del servizio SSH del honeypot dalla classica porta 22 a qualcosa di più sicuro, tipo 22117, si è tentata una connessione sulla porta monitorata: Artillery monitora diverse porte e tipi di connessione, compresa le porte 22 e 21 per le connessioni SSH. Questo secondo tipo di attacco è volto a vedere e comprendere la reazione del sistema in caso un potenziale hacker, dopo aver svolto la ricognizione e visto che la macchina accetta le connessioni SSH, provi a connettersi magari sperando che la password sia semplice e per tentare un potenziale brute-force, che potrebbe garantirgli l'accesso.

Il terzo tipo di attacco che abbiamo voluto testare è la modifica di file interni alla macchina honeypot in caso questa venga penetrata. Questo corrisponde alla fase di manomissione dei file interni al sistema una volta avvenuta la penetrazione, come per esempio l'aggiunta di una backdoor dentro alla macchina. Artillery monitora determinate directory interne, che possono essere modificate a piacere, di modo da poter notificare l'analista in caso che delle modifiche non consentite avvengano. Vediamo successivamente gli attacchi nel dettaglio.

6.6.1 NMAP

Nmap («Network Mapper») è uno strumento open-source per la network exploration e l'auditing. È stato progettato per scansionare rapidamente reti di grandi dimensioni, ma è indicato anche per l'utilizzo verso singoli host. Nmap usa pacchetti IP "raw" (grezzi, non formattati) in varie modalità per determinare quali host sono disponibili su una rete, che servizi (nome dell'applicazione e versione) vengono offerti da questi host, che sistema operativo (e che versione del sistema operativo) è in esecuzione, che tipo di firewall e packet filters sono usati, e molte altre caratteristiche. Nonostante Nmap sia

comunemente usato per audits di sicurezza, molti sistemisti e amministratori di rete lo trovano utile per tutte le attività giornaliere come ad esempio l'inventario delle macchine presenti in rete, per gestire gli aggiornamenti programmati dei servizi e per monitorare gli host o il loro uptime. In aggiunta ad una tabella delle porte interessanti, Nmap può fornire ulteriori informazioni sugli obiettivi come ad esempio i nomi DNS risolti (reverse DNS names), il probabile sistema operativo in uso, il tipo di device e l'indirizzo fisico (MAC address).[92] [91]

6.6.2 I risultati, la rilevazione, le contromisure

Il primo tipo di attacco che vogliamo testare è quello che abbiamo associato alla fase di ricognizione. In questa fase un attaccante svolge diversi scan per cercare di capire quali possono essere determinate vulnerabilità di una determinata macchina. Uno strumento usato comunemente è quello che abbiamo visto sopra, ovvero NMAP. La scansione tramite NMAP si svolge in maniera semplice. Una volta installato il tool, basta lanciare il comando con i parametri che si vogliono utilizzare. In questo caso:

`sudo apt-get install NMAP  sudo NMAP -sU -V 192.168.50.251`

Il risultato dello scan ci appare subito dopo:

```
1 Completed SYN Stealth Scan at 15:22, 0.11s elapsed (1000
    total ports)
2 Nmap scan report for artilleryvm-virtualbox
    (192.168.50.251)
3 Host is up (0.00062s latency).
4 Not shown: 986 closed ports
5 PORT      STATE SERVICE
6 21/tcp    open  ftp
7 22/tcp    open  ssh
8 25/tcp    open  smtp
9 110/tcp   open  pop3
10 1433/tcp  open  ms-sql-s
11 1723/tcp  open  pptp
12 5060/tcp  open  sip
13 5061/tcp  open  sip-tls
14 5800/tcp  open  vnc-http
15 5900/tcp  open  vnc
16 8080/tcp  open  http-proxy
17 10000/tcp open  snet-sensor-mgmt
18 16993/tcp open  amt-soap-https
19 44443/tcp open  coldfusion-auth
20 MAC Address: ************ (Oracle VirtualBox virtual NIC)
```

```
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001
   (40.084KB)
```

Oltre al risultato però, sulla console di QRadar ci appare subito un evento sospetto, che vediamo essere inviato dalla macchina host di Artillery.

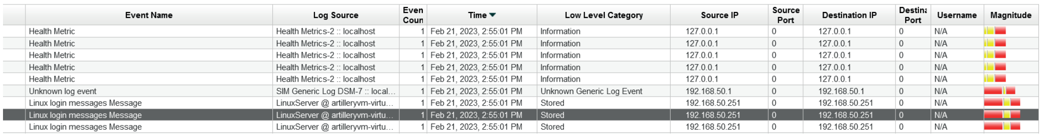


Figura 6.11: Evento sospetto rilevato da Artillery

Evidenziando il messaggio ed aprendo la scheda relativa possiamo notare come viene evidenziato che il honeypot ha rilevato una connessione:

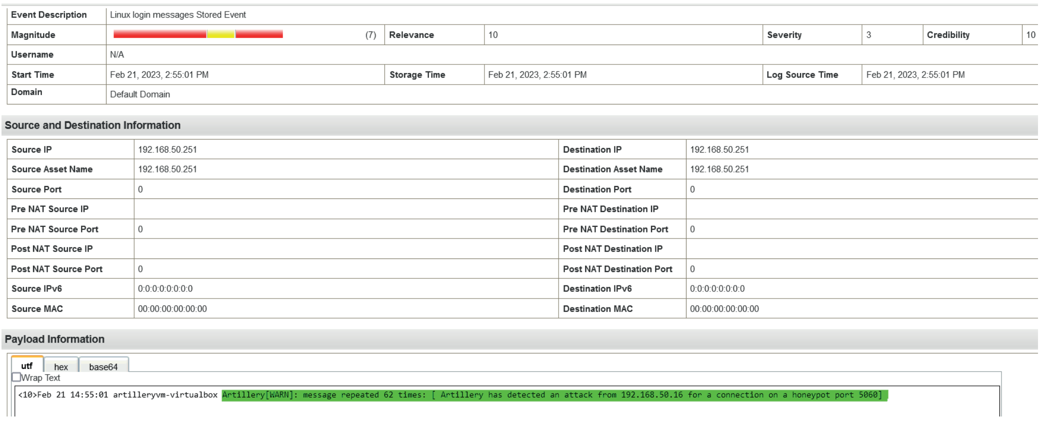


Figura 6.12: Dettagli dell'evento sospetto

E' semplice quindi notare che lo scan, nonostante non si tratti di un vero e proprio tentativo di connessione, è stato rilevato immediatamente dal honeypot che ha poi inviato i log verso QRadar per poter consentire all'analista di visualizzarli. Tutti questi avvisi, volendo, possono essere trasformati tramite regole in offenses (offese) di modo che sia semplice e veloce rilevare i problemi "reali" da tutti i log comuni che si possono ricevere.

Il secondo tipo di attacco di cui abbiamo parlato in precedenza è quello di un tentativo di connessione tramite SSH alla macchina honeypot da parte dell'hacker, che dopo la ricognizione ha notato che la porta 21 e 22 sono

convenevolmente aperte. Inserendo semplicemente l'indirizzo IP e la porta, l'hacker in questione prova quindi a collegarsi alla macchina eseguendo: `sudo ssh 192.168.50.251 -p 21` Ma la connessione viene bloccata:

```
kex_exchange_identification: banner line contains invalid
    characters
```

E' possibile vedere nella sezione Log Activity dell'interfaccia web di QRadar che sono spuntati fuori dei log con magnitudo alto relativi al tentato accesso. Aprendo uno dei log generati otteniamo una descrizione dell'attacco che ci dice come Artillery abbia rilevato un tentativo di connessione all'indirizzo IP e la porta.

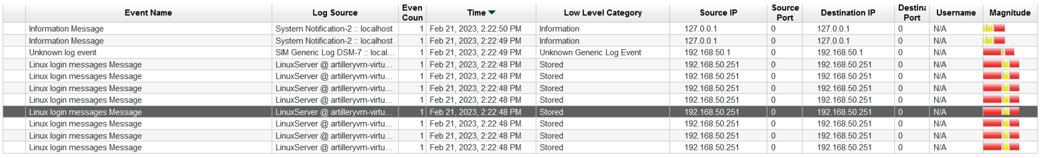


Figura 6.13: Evento per tentativo di connessione

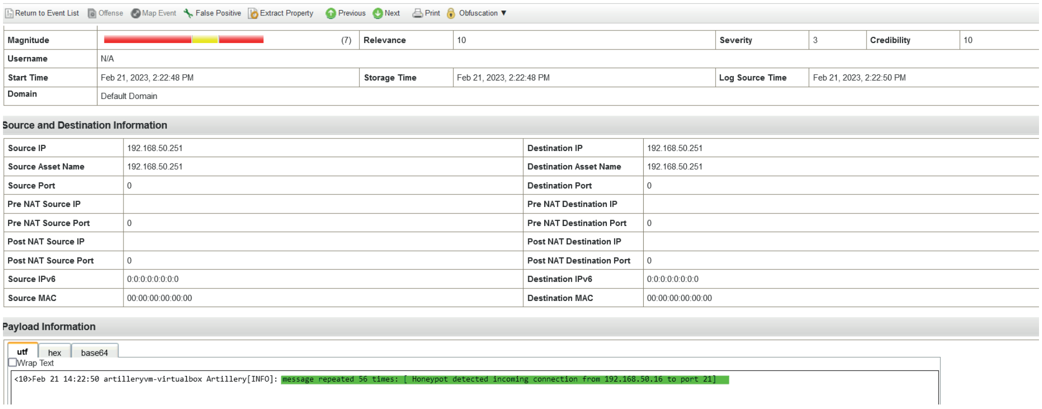


Figura 6.14: Dettagli tentativo di connessione

Il terzo tipo di attacco che abbiamo visto è la modifica di file del sistema. In questo caso si suppone che l'hacker sia riuscito a collegarsi alla macchina tramite SSH e voglia ora installare una backdoor in una qualche directory. Dopo aver impostato Artillery per monitorare la directory /var/www/, per simulare l'attacco si è semplicemente creato un file dentro alla directory utilizzando il comando touch:

`sudo touch bad_file`

Dopo pochi istanti è possibile vedere dall'interfaccia web di QRadar nella sezione Log Activity il problema. Facendo doppio click sull'evento si può vedere nel dettaglio cosa è successo: vediamo come Artillery manda un warning e ci dice che dentro a `/var/www` è stato notato un cambio e ci viene anche specificato il nome del file creato, in questo caso `bad_file`.

	Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username
	Unknown log event	SIM Generic Log DSM-7 :: local…	1	Feb 21, 2023, 1:11:51 PM	Unknown Generic Log Event	192.168.50.1	0	192.168.50.1	0	N/A
	Information Message	System Notification-2 :: localhost	1	Feb 21, 2023, 1:11:50 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
	Unknown log event	SIM Generic Log DSM-7 :: local…	1	Feb 21, 2023, 1:11:48 PM	Unknown Generic Log Event	192.168.50.1	0	192.168.50.1	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Linux login messages Message	LinuxServer @ artilleryvm-virtu…	1	Feb 21, 2023, 1:11:47 PM	Stored	192.168.50.251	0	192.168.50.251	0	N/A
	Unknown log event	SIM Generic Log DSM-7 :: local…	1	Feb 21, 2023, 1:11:43 PM	Unknown Generic Log Event	192.168.50.1	0	192.168.50.1	0	N/A
	Information Message	System Notification-2 :: localhost	1	Feb 21, 2023, 1:11:41 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A
	Information Message	System Notification-2 :: localhost	1	Feb 21, 2023, 1:11:37 PM	Information	127.0.0.1	0	127.0.0.1	0	N/A

Figura 6.15: Evento per modifica directory osservata

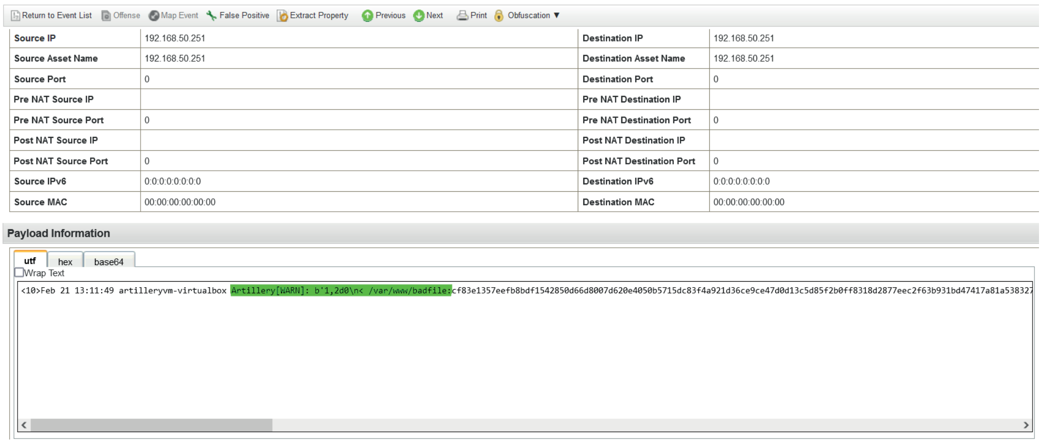


Figura 6.16: Dettagli sulle modifiche apportate

Conclusione

Durante la fase di sperimentazione abbiamo visto come un buon sistema configurato per la difesa di un network sia in grado di rilevare e bloccare un tentativo di intrusione in modo completamente automatico. Nel primo test abbiamo notato subito la ricognizione svolta dal hacker e, volendo, avremmo potuto configurare Artillery di modo da applicare un ban immediato su questo genere di offese. Questo avrebbe reso il sistema ancora più sicuro, ma a scopo simulativo abbiamo deciso di non farlo. Dopo aver ricevuto la notifica le misure di sicurezza che un'analista avrebbe potuto prendere sono diverse: avendo l'hacker effettuato uno scan, si potrebbe fare la stessa cosa per verificare i risultati e fortificare il sistema nei punti deboli trovati, se necessario. Nel secondo test abbiamo invece bloccato una connessione SSH in entrata e notificato il tentativo. Anche qui sarebbe potuto scattare un ban immediato e ci si dovrebbe preoccupare di controllare che tutte le buone pratiche di sicurezza delle connessioni SSH siano in atto. In una rete protetta da altri strati soprastanti di sicurezza (come una VPN) bisognerebbe invece occuparsi di capire da dove venga la connessione e come sia stato possibile per l'hacker tentare la connessione. Proseguendo in stile "backtracking" si cercano le falle e si prosegue nel applicare i fix se necessario. Riguardo al terzo attacco, dove la situazione ricade nell'incident responding, i passi da seguire sono quelli che abbiamo visto nel testo nella sezione dedicata (4.3.3). In generale però, si ha ora una notifica di una intrusione, e grazie ad Artillery, l'autore del fatto può essere bloccato immediatamente.

In questo testo abbiamo visto i malware, il social engineering ed i loro vettori di attacco. Abbiamo parlato ampiamente di information security, del suo processo e di come mantenersi sicuri ma anche come gli hacker sfruttino tutti gli strumenti a loro disposizione per compromettere macchine e reti, siano queste private, aziendali o governative. Risulta estremamente difficile stare al passo con l'evoluzione delle tecnologie e questo ci mostra come sia ancora più difficile rimanere aggiornati e pronti alla protezione di sistemi che sono in continuo aumento e fonte di dati che devono rimanere protetti, lontani dalle mani e dagli occhi di coloro che li sfrutterebbero per scopi

malevoli. Nonostante le misure di sicurezza siano in continua evoluzione, la battaglia per l'attacco e la difesa delle informazioni è destinata a continuare, probabilmente di pari passo, per i decenni a venire. Quello che siamo riusciti a dimostrare durante la nostra fase di sperimentazione è come i SIEM semplificano la gestione della sicurezza per le aziende, filtrando enormi quantità di dati sulla sicurezza e dando priorità agli avvisi di sicurezza generati dal software. Il software SIEM consente alle organizzazioni di rilevare incidenti che altrimenti potrebbero passare inosservati, come dei semplici scan di sistema o tentativi di connessione, come abbiamo visto nel capitolo precedente. Oltre a tutti i sistemi e metodi difensivi che sono stati menzionati in questo testo, è ora chiaro che i sistemi SIEM offrano un qualcosa di cui un team di sicurezza ha assoluto bisogno per processare una enorme quantità di dati e renderla utilizzabile.

Bibliografia

[1] Bhattacharjee, 2011; kshetri, 2013; broadhurst et al., 2014, p. 13. .

[2] Bhattacharjee, 2011; kshetri, 2013; broadhurst et al., 2014, p. 3. .

[3] Heartbleed. https://heartbleed.com.

[4] Sherly et al. Abraham. An overview of social engineering malware: Trends, tactics, and implications. 2010. .

[5] Filipo Sharevski Adam Trowbridge, Jessica Westbrook. Sorry: Ambient tactical deception via malware-based social engineering. https://arxiv.org/ftp/arxiv/papers/1810/1810.11063.pdf.

[6] Muhammad Hashir Ali. Smart home security: Security and vulnerabilities. 2022. https://www.wevolver.com/article/smart-home-security-security-and-vulnerabilities.

[7] Mansi Chaudhary Anshul Kumar and Nagresh Kumar. Social engineering threats and awareness: A survey. 2015. https://ejaet.com/PDF/2-11/EJAET-2-11-15-19.pdf.

[8] 2023 Arcitc Wolf, 2022; ANDRA ANDRIOAIE. The top 5 cyber attack vectors; top 10 attack vectors most exploited by hackers revealed. https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/, https://heimdalsecurity.com/blog/top-10-attack-vectors-most-exploited-by-hackers-revealed/.

[9] Colton Bachman. Siem terms and definitions. 2017. https://www.pratum.com/blog/356-siem-terms-and-definitions.

[10] 2017 Bateman, 2013; Glenny. https://www.unodc.org.

[11] Blumira. What is siem and what are the benefits? https://www.blumira.com/glossary/what-is-siem/.

[12] Giorgio Bonuccelli. What are the basic types of firewalls? 2020. https://www.parallels.com/blogs/ras/types-of-firewalls/.

[13] Chris Brook. What is siem? how it works, best practices for implementation & more. 2022. https://www.digitalguardian.com/blog/what-siem-how-it-works-best-practices-implementation-more.

[14] Ben Canner. Ai in siem: The benefits for enterprises of all sizes. 2019. https://solutionsreview.com/security-information-event-management/ai-in-siem-the-benefits-for-enterprises-of-all-sizes/.

[15] Zach Capers. Social engineering techniques that hack your employees. 2019. https://www.getapp.com/resources/social-engineering/.

[16] UK National Cyber Security Centre. Log4j vulnerability - what everyone needs to know. 2022. https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know.

[17] Checkpoint. What is a firewall? https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/.

[18] CISA. Understanding patches and software updates. https://www.bu.edu/tech/support/information-security/security-for-everyone/understanding-patches-and-software-updates/.

[19] Collaboris. A beginners guide to information security policies. https://www.collaboris.com/information-security-policies-beginners-guide/.

[20] Encryption Consulting. What is siem and how it works? https://www.encryptionconsulting.com/education-center/what-is-siem/.

[21] Crowdstrike. Incident response plan: Frameworks and steps. 2022. https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/.

[22] Cynet. Incident response. 2022. https://www.cynet.com/incident-response/.

[23] Cynet. Incident response sans: The 6 steps in depth. 2022. https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/.

[24] Robin Dickerson. Incident management 101 preparation and initial response (aka identification). 2005. https://www.sans.org/white-papers/1516/.

[25] DNV. The three-pillar approach to cyber security: Data and information protection. https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-16

[26] Security Through Education. Governments. https://www.social-engineer.org/framework/general-discussion/categories-social-engineers/governments/.

[27] Security Through Education. Social engineering tactics used in interrogation. 17/08/2022. https://www.social-engineer.org/social-engineering/social-engineering-tactics-used-in-interrogation/.

[28] CompTIA et al. What is social engineering. 2020. https://www.comptia.org/content/articles/what-is-social-engineering.

[29] Kasperky et al. What is social engineering? https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering.

[30] Kaspersky et al. What is the deep and dark web? https://www.kaspersky.com/resource-center/threats/deep-web.

[31] Kaspersky et al. What is wannacry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

[32] Kaspersky et al. Year 2001. https://encyclopedia.kaspersky.com/knowledge/year-2001/.

[33] Kaspersky et al. A brief history of computer viruses & what the future holds. 2020. https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds.

[34] Claire L. Evans. Searching for susy thunder. 26/01/2022. https://www.theverge.com/c/22889425/susy-thunder-headley-hackers-phone-phreakers-claire-evans.

[35] Exabeam. 10 siem use cases in a modern threat landscape. https://www.exabeam.com/explainers/siem/siem-use-cases/.

[36] Exebeam. What is siem, why is it important and how does it work? https://www.exabeam.com/explainers/siem/what-is-siem/.

[37] Center for Internet Security. Log4j zero-day vulnerability response. 2022. https://www.cisecurity.org/log4j-zero-day-vulnerability-response.

[38] Val Saengphaibul FortiNet. A brief history of the evolution of malware. March 15, 2022. https://www.fortinet.com/blog/threat-research/evolution-of-malware.

[39] Max Freedman. 18 ways to secure your devices from hackers. 2023. https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html.

[40] Stephen Gailey. A brief history of siem. 2020. https://cybersecurity-magazine.com/a-brief-history-of-siem/.

[41] Katlyn Gallo. Log4j vulnerability explained: What it is and how to fix it. 2022. https://builtin.com/cybersecurity/log4j-vulerability-explained.

[42] Kelsey Gast. What is siem? 2021. https://logrhythm.com/blog/what-is-siem.

[43] Gatefy. Social engineering history in the age of computers and the internet. 29/03/2021. https://gatefy.com/blog/social-engineering-history-computers-internet/.

[44] Elisha Girken. Incident response steps and frameworks for sans and nist. 2020. https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide.

[45] Gartner Glossary. Security information and event management (siem). https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem.

[46] Graphus. Artificial intelligence (ai) in cybersecurity. 10/06/2022. https://www.graphus.ai/blog/artificial-intelligence-in-cybersecurity/.

[47] Emily Green. 5 easy ways to protect your business against hackers. https://articles.bplans.com/5-easy-ways-to-protect-your-business-against-hackers/.

[48] Johnatan Greig. Average organization targeted by over 700 social engineering attacks each year: report. 2021. https://www.zdnet.com/article/average-organization-targeted-by-over-700-social-engineering-attacks-each-year

[49] Roger Grimes. 70% to 90% of all malicious breaches are due to social engineering and phishing attacks. 2023. https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-

[50] Darren Guccione. What is the dark web? how to access it and what you'll find. 1/06/2021. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

[51] GWU.edu. Social engineering life cycle. https://blogs.gwu.edu/gwinfosec.

[52] GWU.edu. Social engineering life cycle. https://blogs.gwu.edu/gwinfosec/tag/social-engineering.

[53] Danielle Hoverman. 8 preventative security controls you should consider. 2018. https://blog.totalprosource.com/8-preventative-security-controls-you-should-consider.

[54] Hypr. Eternalblue. https://www.hypr.com/security-encyclopedia/eternalblue.

[55] IBM. All-in-one deployment. https://www.ibm.com/docs/en/qsip/7.4?topic=overview-all-in-one-deployment.

[56] IBM. The benefits of siem. https://www.ibm.com/topics/siem.

[57] IBM. hat is siem? https://www.ibm.com/topics/siem.

[58] IBM. How does siem work? https://www.ibm.com/topics/siem.

[59] IBM. Qradar architecture overview. https://www.ibm.com/docs/en/qsip/7.4?topic=deployment-qradar-architecture-overview.

[60] IBM. A qradar deploy changes on 31 december 2020 can impact product functionality. https://www.ibm.com/support/pages/updated-qradar-deploy-changes-31-december-2020-can-impact-product-functionalit

[61] IBM. What is incident response? https://www.ibm.com/topics/incident-response.

[62] IMDb. Who is kevin mitnick. https://www.imdb.com/name/nm1137342/bio.

[63] Kaspersky. Combining social engineering & malware implementation techniques. https://www.kaspersky.com/resource-center/threats/malware-manipulation.

[64] Securelist et al. Kaspersky. 1980s. https://encyclopedia.kaspersky.com/knowledge/years-1980s/.

[65] Erica Kastner. History of the dark web [timeline]. 07/02/2020. https://www.soscanhelp.com/blog/history-of-the-dark-web.

[66] Swati Khandelwal. Top eight security blunders that prove online security is illusion. 2017. https://www.linkedin.com/pulse/top-eight-security-blunders-prove-online-illusion-swati-khandelwal/.

[67] Baris Kirdemir. Hostile influence and emerging cognitive threats in cyberspace. 2019. .

[68] KnowBe4. Who is kevin mitnick? https://www.knowbe4.com/products/who-is-kevin-mitnick/.

[69] Robert Koch. Hidden in the shadow: The dark web - a growing risk for military operations? 2019. https://ccdcoe.org/uploads/2019/06/Art_15_Hidden-in-the-Shadow.pdf.

[70] Gene J. Koprowski. Instant messaging grew by nearly 20 percent in 2005. 2005. https://www.technewsworld.com/story/instant-messaging-grew-by-nearly-20-percent-in-2005-47270.html.

[71] Neal Levitt. Instant messaging: A new target for hackers. 2005. p.20-23.

[72] Wei Chieh Lim. Apache log4j vulnerability explained. 2022. https://www.swarmnetics.com/blog/apache-log4j-vulnerability-explained/.

[73] Wei Chieh Lim. Apache log4j vulnerability explained. 2022. https://www.swarmnetics.com/blog/apache-log4j-vulnerability-explained.

[74] James Linton. https://www.linkedin.com/in/james-linton-social-engineer-and-hacker.

[75] Logpoint. Top 10 siem use cases to implement. https://www.logpoint.com/en/understand/top-10-use-cases-implement/.

[76] Logsign. Evolution of siem over the years. 2018. https://www.logsign.com/blog/evolution-of-siem-over-the-years/.

[77] ManageEngine. Components of siem architecture. https://www.manageengine.com/log-management/siem/siem-components.html.

[78] Jim Breithaupt Mark S. Merkow. Information security: Principles and practices, 2nd edition. 2014. https://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=9.

[79] Jacques Van Marken. Social engineering. https://www.eoht.info/page/Social%20engineering.

[80] McAfee. What is ransomware? https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html.

[81] Forbes Councils Member. Nine practical ways to protect your company from hackers and phishing attacks. 2021. https://www.forbes.com/sites/theyec/2021/03/16/nine-practical-ways-to-protect-your-company-from-hackers-and-phishing-attacks/

[82] Microsoft. What is siem? https://www.microsoft.com/en-us/security/business/security-101/what-is-siem.

[83] Microsoft. What is antivirus software? 2011. .

[84] Kevin Mitnick. The history of social engineering & how to stay safe today. https://www.mitnicksecurity.com/the-history-of-social-engineering, chapter 2.

[85] Kevin Mitnick. The art of deception. 2016. p.41.

[86] Kevin Mitnick. Tweet. 2019. https://twitter.com/kevinmitnick/status/1093956721494478848, Twitter.

[87] N-able. Top siem benefits. 2020. https://www.n-able.com/blog/top-siem-benefits.

[88] Netsurion. Siem, ueba, soar and your cybersecurity arsenal. https://www.netsurion.com/articles/siem-ueba-soar-and-your-cybersecurity-arsena.

[89] Sam Newton. Understanding incident response frameworks - nist & sans. 2021. https://www.stickmancyber.com/cybersecurity-blog/incident-response-frameworks-nist-sans.

[90] Nist. Glossary definitions. https://csrc.nist.gov/glossary.

[91] NMAP. Description. https://nmap.org/man/it/index.html#man-description.

[92] NMAP. Documentation. https://nmap.org/docs.html.

[93] Norton. What is social engineering? a definition + techniques to watch for. 2021. https://us.norton.com/blog/emerging-threats/what-is-social-engineering.

[94] Reuters OCCRP. 2016. https://www.unodc.org.

[95] Andy O'Donnell. How to enable your wireless router's built-in firewall. 2021. https://www.lifewire.com/how-to-enable-your-wireless-routers-built-in-firewall-2487668.

[96] Ufuoma Ogono. What information security processes does an information security analyst need to know? 2022. https://careerkarma.com/blog/information-security-processes/.

[97] Verizon Paul Gillin. The history of phishing. https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/#:~:text=It%27s%20thought%20that%20the%20first,passwords%20and%20hijack%20their%20accounts.

[98] Pretend Podcast. Ambush interview with frank abagnale, the con artist behind catch me if you can (part 5). 04/09/2022. Podcasttranscript.

[99] proofpoint. Threat report 2022 state of the phish. 2022. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

[100] proofpoint. Threat report 2022 state of the phish. 2022. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

[101] Emil Protalinski. Avg incorrectly flags user32.dll in windows xp sp2/sp3. 2008. .

[102] PurpleSec. Cyber security statistics. https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering.

[103] PurpleSec. Cyber security statistics: The ultimate list of stats data, & trends for 2023. https://purplesec.us/resources/cyber-security-statistics/.

[104] Purplesec. Cyber security statistics, the ultimate list of stats, data & trends. 2021. https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering.

[105] PurpleSec. Cyber security statistics the ultimate list of stats data, & trends for 2023. 2023. https://purplesec.us/resources/cyber-security-statistics/.

[106] Rapid7. Incident response plan: Make a plan now and save time where it counts. https://www.rapid7.com/fundamentals/incident-response-plan/.

[107] Rapid7. Threat detection: Quickly and efficiently detect threats, both known and unknown. https://www.rapid7.com/fundamentals/threat-detection/.

[108] Riversafe. Cyber security: Why prevention is better than recovery. https://riversafe.co.uk/tech-blog/cybersecurity-why-prevention-is-better-than-recovery/.

[109] Sian Roach. What is social engineering? 2021. https://netacea.com/blog/part-1-what-is-social-engineering/#investigation.

[110] Jessica Scarpati Robert Sheldon. Server message block protocol (smb protocol). https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol.

[111] James LaPiedra SANS Institute. The information security process prevention, detection and response. 2002. https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197.

[112] TechTarget Security. A guide to siem platforms, benefits and features. https://www.techtarget.com/searchsecurity/feature/Three-enterprise-benefits-of-SIEM-products.

[113] DANIEL SNYDER. The very first viruses: Creeper, wabbit and brain. May 30, 2010. https://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/.

[114] The Redscan Team. The benefits of siem. 2016. https://www.redscan.com/news/the-benefits-of-siem-as-a-service/.

[115] Security through education. The attack cycle. https://www.social-engineer.org/framework/attack-vectors/attack-cycle.

[116] Security through education. The attack cycle. https://www.social-engineer.org/framework/attack-vectors/attack-cycle.

[117] Security through education. Information gathering. https://www.social-engineer.org/framework/information-gathering/.

[118] Treccani. Definizione. https://www.treccani.it/enciclopedia/malware/.

[119] Trellix. What is ueba? https://www.trellix.com/en-us/security-awareness/operations/what-is-ueba.html.

[120] 2017 TrendMicro. The michelangelo virus, 25 years later. 2017. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-michelangelo-virus-25-years-later.

[121] Abi Tyas Tunggal. What is a cve? common vulnerabilities and exposures explained. 2022. https://www.upguard.com/blog/cve.

[122] Abi Tyas Tunggal. What is an attack vector? 16 common attack vectors in 2023. 2023. https://www.upguard.com/blog/attack-vector.

[123] Aby Tyas Tunggal. 22 types of malware and how to recognize them in 2022. 2021. https://www.upguard.com/blog/types-of-malware.

[124] UNODC. Criminal groups engaging in cyber organized crime. June 2019. https://www.unodc.org.

[125] Verizon. 2022 data breach investigations report. 2022. https://www.verizon.com/business/en-gb/resources/reports/dbir/.

[126] John Walker. The animal episode. 12/08/1996. https://www.fourmilab.ch/documents/univac/animal.html.

[127] Wang and Kshteri Antonopoulos. 2010, 2016. https://www.unodc.org.

[128] the virus encyclopedia Wikidot. Michelangelo. http://virus.wikidot.com/michelangelo.

[129] Wikipedia. Chris kubecka. https://en.wikipedia.org/wiki/Chris_Kubecka.

[130] Wikipedia. Definiton. https://en.wikipedia.org/wiki/Google_hacking.

[131] Wikipedia. Definizione. https://en.wikipedia.org/wiki/Attack_vector.

[132] Wikipedia. Eternal blue. https://en.wikipedia.org/wiki/EternalBlue.

[133] Wikipedia. Security information and event management. https://en.wikipedia.org/wiki/Security_information_and_event_management.

[134] Wikipedia. Security information and event management, terminology. https://en.wikipedia.org/wiki/Security_information_and_event_management#Terminology.

[135] Wikipedia. Security information and event management, use cases. https://en.wikipedia.org/wiki/Security_information_and_event_management.

[136] Wikipedia. Cabir (computer worm). 27/1/2023. https://en.wikipedia.org/wiki/Cabir_(computer_worm).

[137] Wkipedia. Iloveyou. 22/02/2022. https://en.wikipedia.org/wiki/ILOVEYOU.

[138] SIEM XPERT. Siem architecture. https://www.siemxpert.com/blog/siem-architecture/.

[139] Arif Sari Zeynep Busra Kirencigil, Onurhan Yilmaz. Cyber security and open source intelligence. 2016. .