Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

Index

  - **OpenSSL**: –> readME <–
  - **DNS + DNSSEC (Asymmetric Cryptography)**: –> readME <–
  - **Vulnerabilitats**: –> readME <–
  - **COM PROTEGIR-SE?**: –> readME <–
- **Bibliografia**: –> readME <–

Objectius "Projecte ASIX - Ciberseguretat: *"Careful where you step in"*

L'objectiu principal d'aquest projecte de Ciberseguretat, és la creació d'una empresa de **"Ciberseguretat"** anomenamada *"CryptoSEC"*. Aquesta empresa implementarà una serie de serveis de **seguretat** i **prevenció** davant d'atacs maliciosos que tindràn la finalitat de *comprometre* la empresa i obtenir informació delicada i confidencial. Aaron i Cristian, son els caps d'aquesta empresa i portaràn a terme aquest magnífic repte de protegir-se davant de *hackers* com les de la Organització **"Anonymous"**, **" The Shadow Brokers", "Elliott Gunton"**... entre altres.

La empresa de ciberseguretat en tot moment s'hi faràn auditoríes per detectar intrusos (**Wazuh**) en la xarxa de **"CryptoSEC"**, entre altres eines de prevenció i detecció.

Arquitectura CryptoSEC

CryptoSEC.NET és una xarxa interna local en algun lloc remot del planeta on hi treballen els millors tècnics en **ciberseguretat**, però hi hà un **"intrús"** que tindrà un *host maliciós* que intentarà fer la vida impossible als altres clients.

Aquest host maliciós serà un **Kali Linux** on hi dispondrà d'eines de seguretat, de *"hackeig"* o *"crackeig"*, de *pentesting*, *accés a la xarxa*... entre altres. Aquest host maliciós farà atacs com el *"DNS Caché Poisoning - DNS Spoofing"*, juntament amb l'"*ARP Cache Poisoning - Spoofing* " (enverinament de la caché dels servidors de *DNS SOA* i *DNS Forwarder* de CryptoSEC, amb posteriori suplantació i redirecció a una pàgina web *"fake"* que serà reenviada com a resposta a la petició dels clients). També farà un atac de **Brute Force** on *crackejarà* contrasenyes amb encriptació SHA512 (UNIX) per poder entrar al servidor *router*: **ForwardSEC**.

Aquest host maliciós interferirà en la connexió entra el DNS autoritari SOA i el DNS Recursor que es qui farà de *resolver/forwarder* dels **clients DNS** que hi pertenèixen a la xarxa interna **"CryptoSEC"**. Serà un **DNS Forwarder (ForwardSEC)** més.

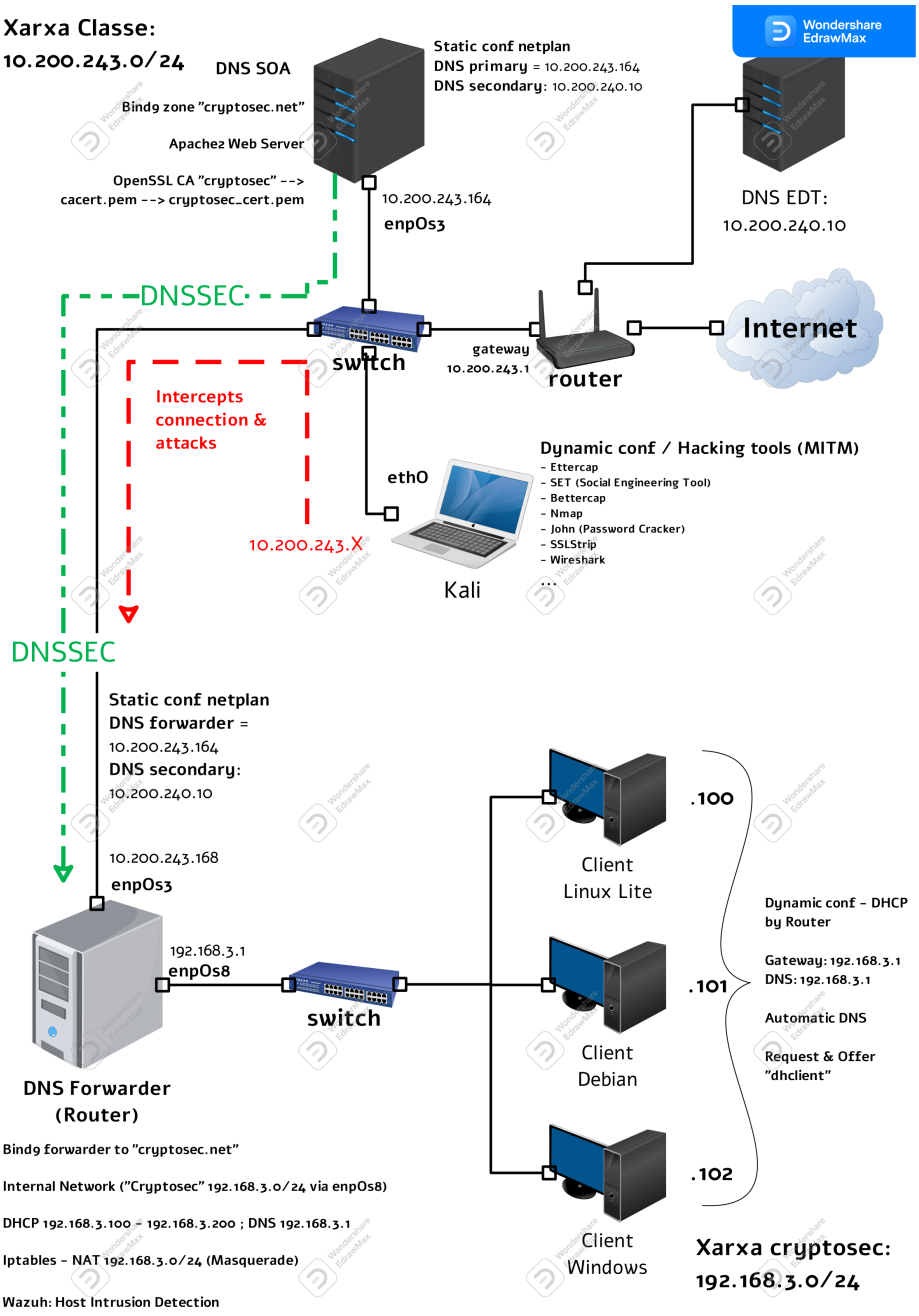
A **CryptoSEC** implementarà, serveis com un DNS autoritari amb una zona anomenada **"cryptosec.net"** que tindrà DNSSEC per assegurar les consultes DNS que hi facin els clients de la seva *"zona"* o *"domini"*.

Al **DNS Forwarder (ForwardSEC)** tindrà serveis com **DHCP** que brindarà una configuració automàtica de IPs i DNS als seus clients. Serà com un **router**. Tindrà politiques per defecte ACCEPT, i també permetrà que els seus clients tinguin NAT a l'exterior, és a dir, que puguin navegar per Internet. Tot amb **iptables**.

El **servidor principal autoritari** anomenat com a hostname **"SOACryptosec"** que serà un **Ubuntu Server 20.04**, tindrà només el *BIND9* amb la zona **"cryptosec.NET"**, estarà ubicada en la xarxa de la classe *10.200.243.164/24*.

Tindrà un **servidor secundari forwarder** anomenat com a hostname **"ForwardSEC"** que serà també un **Ubuntu Server 20.04** que tindrà el paper fonamental de fer de *resolver* als clients DNS ja que ell mateix serà un forwarder i reenviarà les peticions de DNS a **"SOACryptosec"** per a que resolgui peticions de DNS tant de **"cryptosec.net"** com d'Internet, si no el sap el preguntarà als **ROOT SERVERS**, *a.k.a.* **Internet**. També tindrà aplicacions per monitoritzar la xarxa i detectar intrusos que intentin sacsejar la nostra xarxa **"cryptosec.net"**.

Com hi haviem comentat, a **CryptoSEC** hi englobem diferents serveis en funcionament, com **detecció d'intrusions (OpenVAS)** o algunes de **prevenció d'atacs**, tot explicant breument cada cascuna dels diferents serveis que hi componen la nostra organització: **"CryptoSEC"**.



Durant aquest projecte, ens trobarem diferents *reptes* tant en l'àmbit *tècnic* com en l'àmbit *sistemàtic*. Haurem de ser capaços de resoldre aquests reptes amb l'ajuda bé de diferents companys de classe, o de la informació investigada per Internet.

En la recerca d'informació de tota la documentació, independentment de les seves funcionalitats, les bateries de proves, el control de versions fins a arribar a l'últim "*stage*" del projecte. Es farà un seguiment de tot el que es fa, es farà i el que s'està fent en hores de projecte.

Conceptes i aspectes generals *"mindset"* del projecte

Tenim una idea clara, *primer* la recerca d'informació i recapitulació de tots els *serveis* que utilitzarem, *segon* un petit exemple de funcionament del servei en qüestió i finalment, l'assemblació al cos del projecte.

Tot això després de verificar que compleixen aspectes tant de la informàtica o concretament a la **ciberseguretat** que un **auditor o defensor de ciberseguretat** ha de conèixer:

- La **identificació**:
  - És necessari identificar els **processos** i **actius** crítics d'alguna.
  - S'ha de mantenir **actualizat** l'**inventari** tant de **hardware** o **software**.
  - Conèixer les **característiques**, ja que amb freqüència son punts d'entrada de programes i aplicatius **maliciosos**.
  - Cal identificar **amenaçes**, **vulnerabilitats** i **riscos** per als actius.

  - Cal assegurar-se que s'estableixin i administrin processos de gestió de **riscos** per garantir que **s'identifiquin**, avaluïn i administrin les amenaces internes i externes, cosa que s'ha de documentar degudament en registres de riscos.

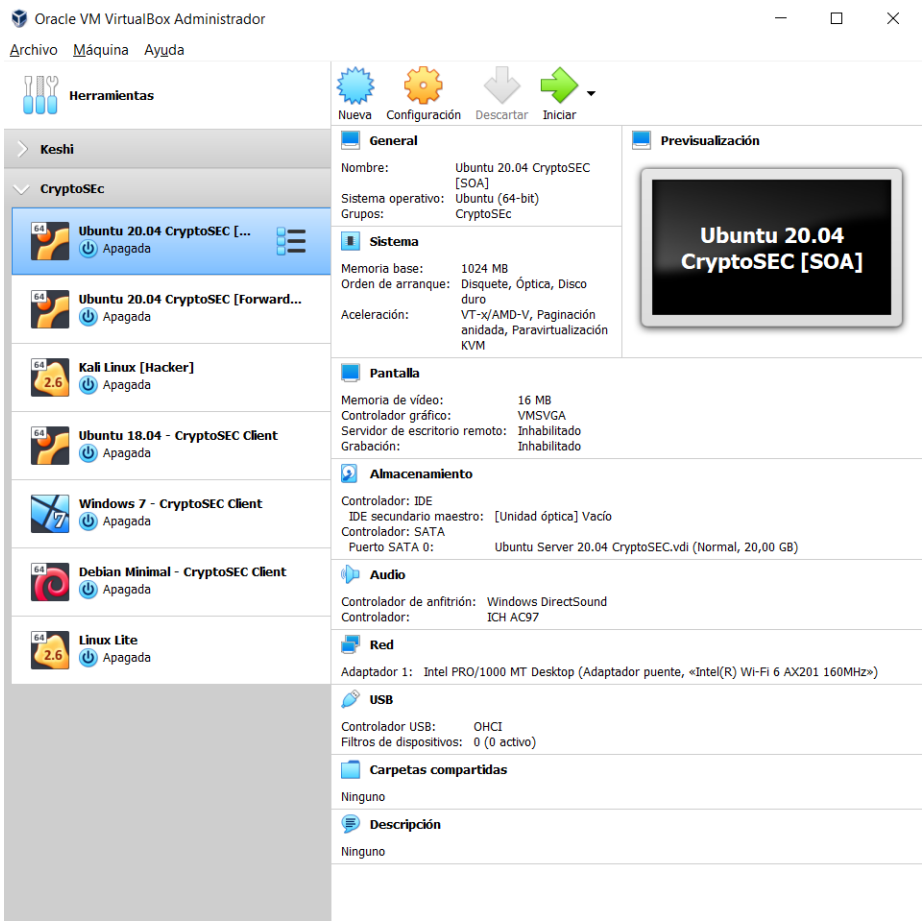
- La **protecció**:
  - Convé **administrar** l'accés als **actius** i la **informació**.
  - La companyia ha de crear comptes únics per a cada empleat i assegurar-se que els usuaris només tinguin accés a la informació, els ordinadors i les aplicacions que necessiten per als seus treballs.
  - Cal **administrar** i **rastrejar** estrictament l'accés **físic** als dispositius.
  - Realitzar **còpies de seguretat** periòdiques és útil. Una bona pràctica és mantenir un conjunt de dades de còpia de seguretat freqüent fora de línia per protegir contra el ransomware.
  - S'han d'implementar **polítiques formals** per a l'eliminació segura de fitxers electrònics i dispositius en desús.
- Els **backups**: És important assegurar la informació abans i després de que s'hagin provocat *"desastres informàtics"*. Una bona recuperació o *cleaning* d'avant d'aquest escenari és clau per retomar una activitat d'una empresa.
- La **detecció**:
  - És important desenvolupar i provar processos i procediments per detectar accions no autoritzades a les xarxes ia l'entorn físic, inclosa l'activitat del personal.
  - Cal comprendre l'impacte dels esdeveniments de ciberseguretat. Cal treballar ràpidament i exhaustivament per comprendre l'amplitud i la profunditat de l'impacte. Així com comunicar informació sobre l'esdeveniment amb les parts interessades apropiades.
  - Cal monitoritzar els ordinadors per controlar si es detecta accés de personal no autoritzat als ordinadors, dispositius (suports demmagatzematge de dades de tipus USB) i programari. Heu de revisar la xarxa per controlar si es detecten usuaris o connexions no autoritzats.
- La **resposta**:
  - Els plans de **resposta** s'han de provar per assegurar-se que cadascú conegui les seves **responsabilitats** en la seva execució.
  - Coordinar amb les parts interessades internes i externes és vital davant el desastre.
  - Cal assegurar-se que els plans de resposta i les actualitzacions incloguin totes les parts interessades clau i proveïdors de serveis externs. Poden contribuir a millores en la planificació i execució.

- La **recuperació**:
  - Cal comunicar-se amb usuaris afectats, tant de dins con de fora davant d'aquests desastres, per fer un plà de recuperació.
  - La comunicació és clau per protegir-se.
  - Cal assegurar-se que els plans de recuperació estiguin **actualitzats**.
  - S'han de reparar i restaurar els equips i les parts de la xarxa que van resultar afectats.

La proposta final

El deployment

Hem decidit utilitzar **VirtualBox** per al *deployment* d'aquest projecte simplement amb la facilitat d'utilització, la compatibilitat tant de **Linux**, **Windows** o **MAC** i la versatilitat alhora de clonar, encendre, interactuar amb la virtualització de les màquines virtuals.



A més de que tenim un control avançat alhora de *"toquetejar"* l'emulador de VirtualBox tant a nivell de **hardware** com a nivell de **software**.

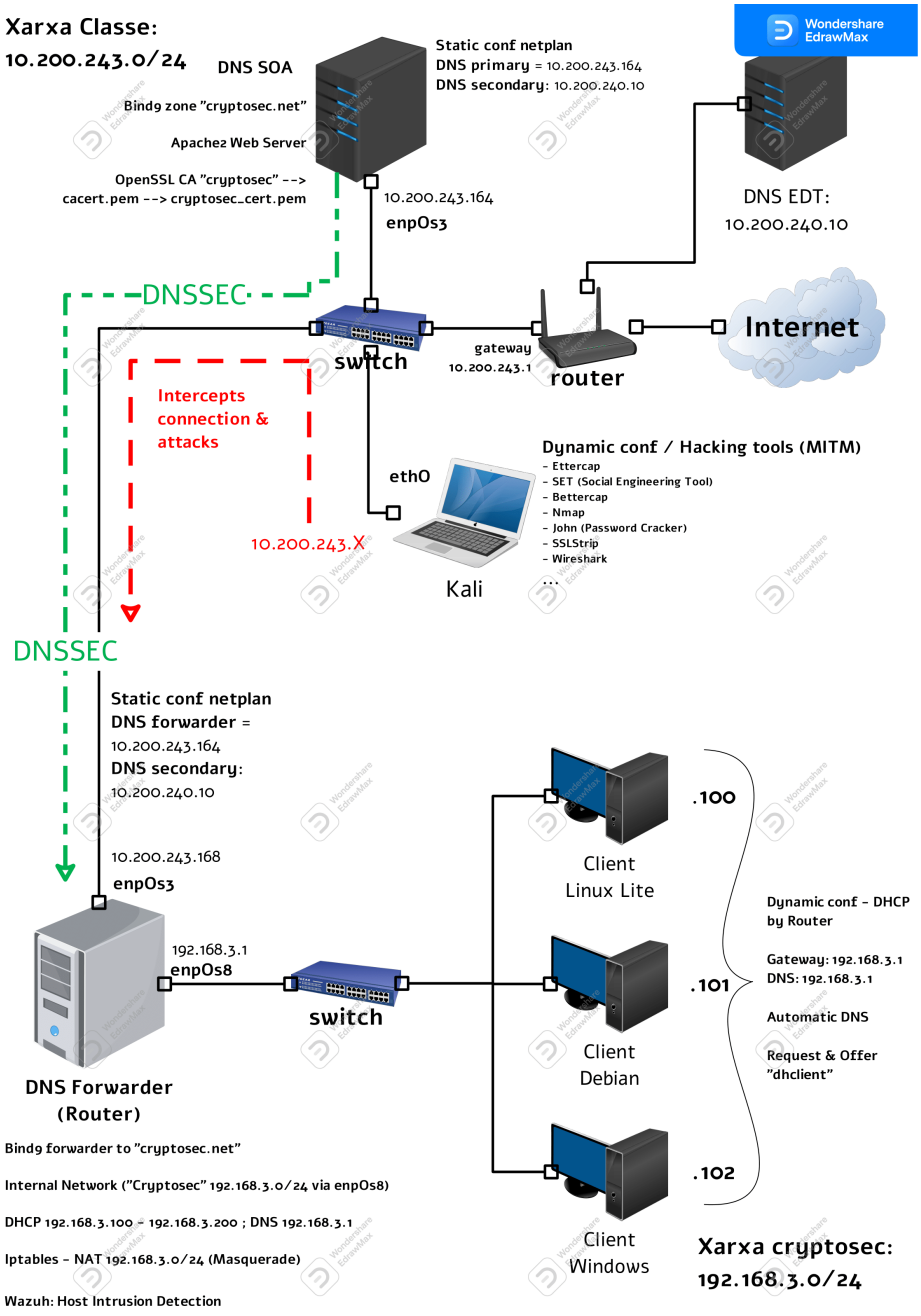
El servidor **"ForwardSEC"** farà de router on hi tindrà 2 interfícies (**enp0s3**) i (**enp0s8**), la primera serà un **"bridge"** amb configuració *netplan* estàtica **10.200.243.168/24** i en la segona serà una **xarxa interna** que tindrà la ip **192.168.3.1/24**. Aquesta tindrà la xarxa interna **"cryptosec.net"** *192.168.3.0/24*.

El servidor **"SOACryptosec"** serà un servidor autoritari on hi tindrà la zona **"cryptosec.net"** hi tindrà 1 interfícies (**enp0s3**) i (**enp0s8**), serà un només un **"bridge"** que tindrà una configuració *netplan* estàtica **10.200.243.164/24**.

Tots els clients de la xarxa de **"cryptosec"** han de passar per el router per poder navegar a l'exterior o fer peticions *DNS* (En aquest cas han de preguntar al **resolver ForwardSEC**).

El servidor **"SOACryptosec"** farà de router emetrà IPs automàticament gràcies

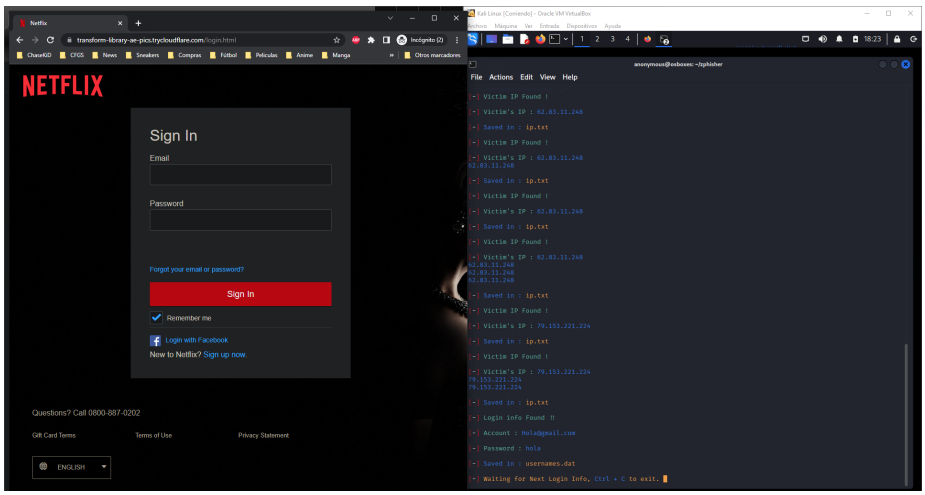
a DHCP i donarà els nameservers adequats a les seves xarxes internes per a que puguin navegar a Internet. També s'hi farà NAT a l'exterior on hi navegaràn *enmascarats*.



Ciberseguretat a CryptoSEC

- L'**aïllament en la xarxa interna**: Mecanisme de seguretat que permetrà separar els programes en execució, per tal de mitigar errors del sistema o vulnerabilitats de software. Gracies a la nostra xarxa interna **"cryptosec"**.
- **Xifratge de dades**: Comunicació xifrada en tot moment a CryptoSEC. Els clients podràn fer resolucions al seu *resolver* de forma segura utilitzant "**criptografía asimétrica**". D'aquesta forma l'atacant hacker no podrà dur a terme el seu atac **man in the middle** amb **spoofing**. L'accés a la pàgina de **cryptosec.net** estarà xifrada en tot moment gràcies als certificats generats i signats per **Veritat Absoluta**. Permeten que actui el SSL, així no podràn interceptar-nos.
- **Protegirse davant la vulnerabilitat**: Davant d'un atac maliciós, d'una denegació de servei DOS, d'un metaexploit, d'un phishing, d' un spoofing... etc. Hem de saber com actuar davant d'aquests escenaris. Millor prevenir que lamentar-nos!
- **Detecció i actuació davant el desastre**: Verificació amb eines com **Nmap**, **Arp**, **Wireshark**...
- Durant l'assemblatge final, es faràn diversos atacs a l'empresa **CryptoSEC**, i l'empresa es protegirà davant d'aquestes amenaçes on es posaràn en perill la integritat de l'empresa.
- L'atacant farà els atacs des d'un Kali Linux.

  Exemple d'atac d'Enginyeria Social: "*Phishing + Credential Harvester*"



Els objectius dels serveis de CryptoSEC

DHCP

- S'hi brindarà una configuració automàtica al seus clients de la xarxa interna **CryptoSEC.net**

Iptables

- Els usuaris podràn fer NAT a l'exterior, enmascarats.

OpenVAS (Host Intrusion Detect)

- **Detectar** i **monitoritzar** la infraestructura, les amenaçes i l'intent d'intrusió.
- També detectarà anomalies del sistema o aplicacions mal configurades o accions d'usuari no autoritzats.

OpenSSL

- Asseguració de la connexió mitjançant la **criptografía**. Utilitzant TLS com a protocol de *transport* i *SSL*.
- Ens servirà per un certificat a la nostra zona "cryptosec.net", on hi tindrem un Apache2.
- Amb el parell de claus privades - publiques, la nostra conexió estarà xifrada. Ja que Apache2 utilitzarà la *keys* i el *cert* de **CryptoSEC**, aquest certificat ha sigut firmat per **Veritat Absoluta**.

DNS + DNSSEC (Asymmetric Cryptography)

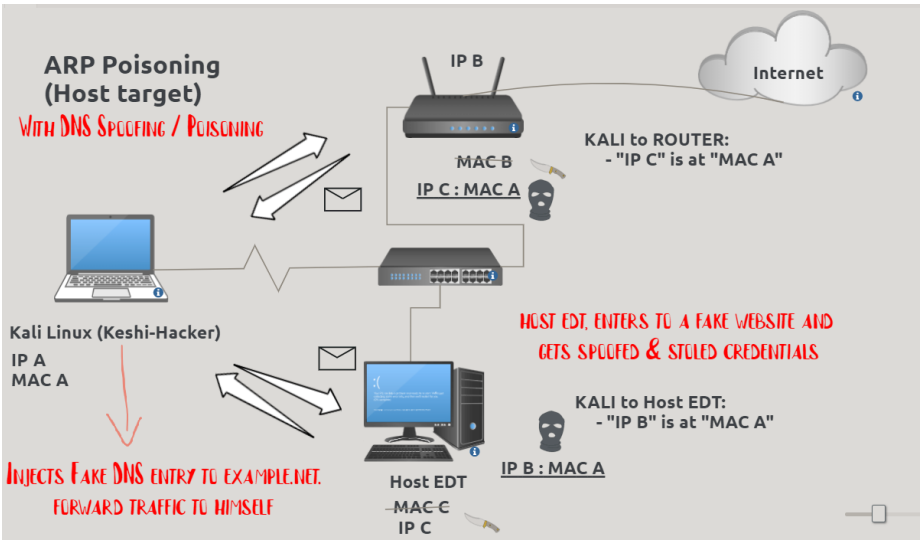
- Implementació de BIND9.
- Entendre conceptes de DNS, zones i registre de recursos.
- Entendre DNSSEC:
  - Claus firmades,
  - DNSKEY, RRSIG, NSEC, NSEC3...
- Creació i administració de claus per a la zona "CryptoSEC".
- Resoldre problemes de servidor de noms autoritzats que atén zones segures com DNSSEC de "CryptoSEC".
- Configuració BIND com un servidor recursiu que realitza la validació DNSSEC en nom dels seus clients.
- TSIG per a una comunicació segura amb BIND.

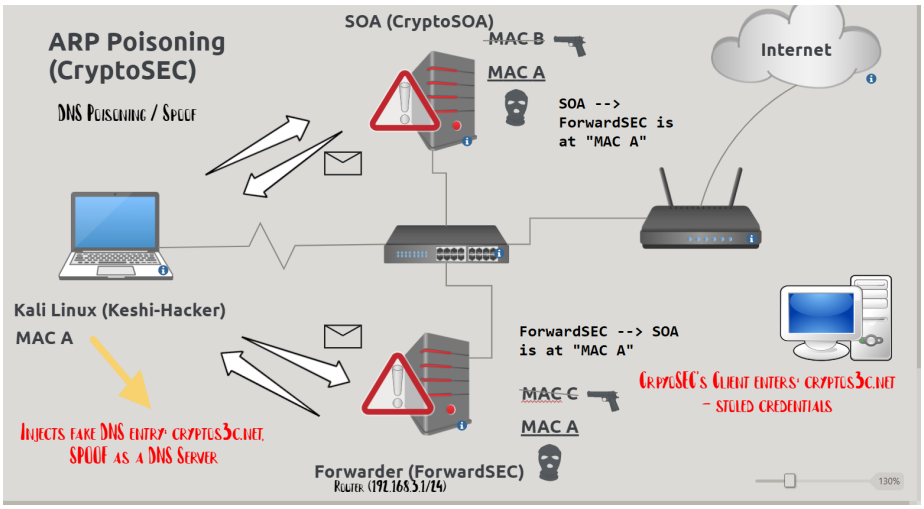
Vulnerabilitats

Alguns exemples de:

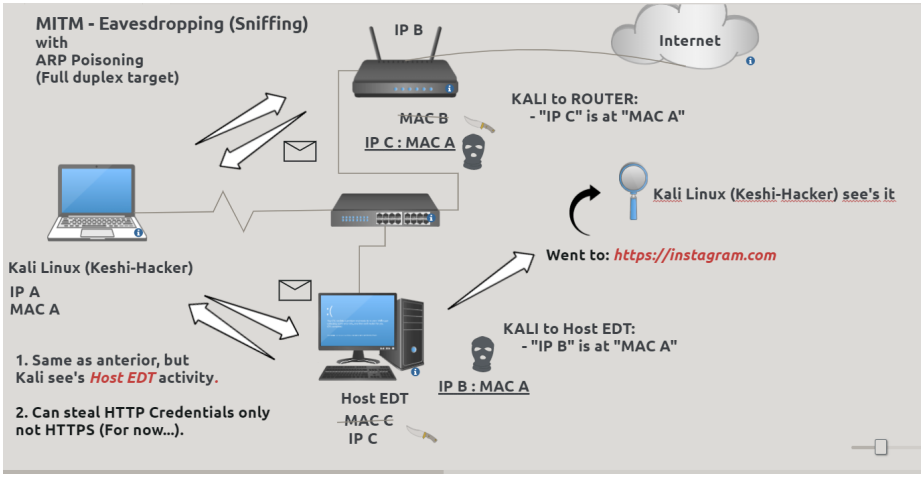
Les que veurem:

- **Brute Force - Password Cracker**: Els atacs de força bruta desxifren dades en provar totes les combinacions possibles, com quan un lladre intenta obrir una caixa forta en intentar tots els números al pany.
- **MITM - ARP Cache Poisoning / Spoofing**: Injecta registres o enverina a la taula ARP dels dispositius implicats i fa una redirecció a l'atacant, suplantant la MAC dels dispositius implicats.
- **MITM - DNS Cache Poisoning / Spoofing + Phishing**: Injecta registres o enverina el registre DNS d'un servidor DNS o varis implicats. L'atacant fa una redirecció a la víctima a una web falsa, suplanta un registre DNS fent-lo creure que està anant al lloc adequat.

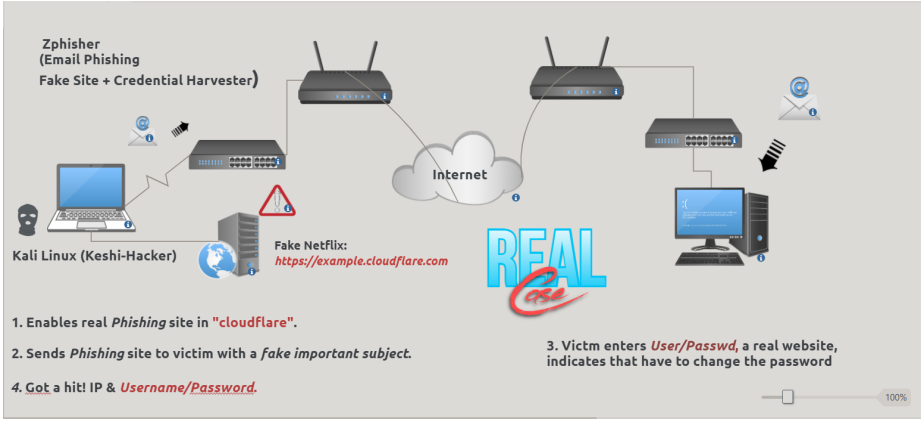




- **MITM - Eavesdropping (SNIFFER)**: Permet veure l'activitat de la victima d'incògnits. Com veure a quines pàgines està entrant. O agafar-li les credencials (HTTP).



- **Social Engineering: Fake Page + Mail Phishing**: Enviament de correu amb una suplantació de DNS, aquest correu s'enviarà desde una eina de Kali a una víctima perque accedeixi al enllaç.



Altres:

- Keylogger
- Rootkits
- Rogue Access Points
- Phishing
- Metaexploits

. . . entre altres

COM PROTEGIR-SE?

- **DNSSEC**: Firma i assegura una zona. Afegeix una capa de seguretat addicional al protocol DNS que permet comprovar la integritat i autenticitat de les dades
- **VPN**: Mitjançant una connexió xifrada a través d'ún túnel amb criptografía asimètrica (Claus híbrids).
- **IPSEC**: Establir comunicacions segures, amb autenticació i xifratge de dades.
- **HTTPS**: HTTP utilitza criptografía TLS/SSL per poder establir i protegir la integritat i la confidencialitat de les dades dels usuaris entre els vostres ordinadors i el lloc.
- **S/MIME**: Activar l'encriptació d'extrem a extrem del correu electrònic corporatiu signant digitalment amb un certificat de correu electrònic.
- **OPENSSL**: Secure Socket Layer (SSL) i Transport Layer Security (TLS) per a l'autenticació web.
- **Vigilància correus Phishing**: No obrir correus de remitents desconeguts.

- **Mantenir sistemes actualitzats, antivirus... etc**: Actualitzar el programari i el maquinari per a no tenir vulnerabilitats quan hi hàgin amenaçes.

Bibliografia

CIBERSECURITY

- https://www.lpi.org/our-certifications/exam-303-objectives
- https://nordvpn.com/es/blog/protocolo-ipsec/ - IPSEC
- https://www.auditool.org/blog/auditoria-de-ti/8200-5-aspectos-de-ciberseguridad-que-todo-auditor-debe-conocer-para-evaluar-y-recomendar
- https://www.rosario3.com/ecos365/noticias/Cuales-son-los-aspectos-clave-en-ciberseguridad-20190722-0011.html

BETTERCAP

- https://www.bettercap.org/installation/ - BETTERCAP
- https://www.youtube.com/watch?v=7Bvdprvzvko - BETTERCAP
- https://www.youtube.com/watch?v=AoUB2MAnMJA - BETTERCAP
- https://hackpuntes.com/obtener-credenciales-https-con-bettercap-y-sslstrip/ - BETTERCAP SSLSTRIP
- https://jaymonsecurity.com/mitm-credenciales-sslstrip-mitmf-delorean/ - BETTERCAP SSLSTRIP

WAZUH

- https://documentation.wazuh.com/current/user-manual/overview.html - WAZUH

SSLSTRIP

- https://www.youtube.com/watch?v=F5m9cXVJZ18 - SSLSTRIP
- https://www.youtube.com/watch?v=jFWd_nN0DXU - BREAK HTTPS USING KALI
- https://www.youtube.com/watch?v=OtO92bL6pYE&list=LL&index=4 - SSLSTRIP ON KALI LINUX

ETTERCAP

- https://programmerclick.com/article/2815493326/ - ETTERCAP
- https://esgeeks.com/tutorial-ettercap-ejemplos/ - ETTERCAP EXEMPLES
- https://esgeeks.com/tutorial-ettercap-ejemplos/ - ETTERCAP EXEMPLES

ARP CACHE POISONING / ARP SPOOF

- https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/ - ARP POISONING
- https://es.acervolima.com/ataque-mitm-man-in-the-middle-usando-arp-poisoning/ - ARP POISONING

DNS CACHE POISONING / DNS SPOOF

- https://www.varonis.com/blog/dns-cache-poisoning - DNSSPOOF
- https://programmerclick.com/article/2815493326/ - DNSSPOOF
- https://www.boomernix.com/2018/03/realizando-un-dns-spoofing.html - DNSSPOOF
- https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/ - DNSSPOOFING
- https://www.varonis.com/blog/dns-cache-poisoning - CACHE POISON
- https://www.cloudflare.com/learning/dns/dns-cache-poisoning/ - DNSSPOOF
- https://www.okta.com/identity-101/dns-poisoning/ - DNSCACHE POISON
- https://www.youtube.com/watch?v=uQrmKhW35mQ&t=765s - DNSSPOOFING ETTERCAP BACKBOX
- https://www.varonis.com/blog/dns-cache-poisoning - SPOOF DNS CACHE POISONING
- https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/#:~:text=DNS%20poisoning%2C%20also%20known%20as,web%20servers%20and%20phishing%2
  cache-poisoning - CACHE POISONING
- https://www.imperva.com/learn/application-security/dns-spoofing/ - DNSSPOOFING
- https://www.amirootyet.com/post/how-to-spoof-dns-in-kali-linux/ - DNSSPOOFING
- https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/#:~:text=DNS%20poisoning%2C%20also%20known%20as,web%20servers%20and%20phishing%2
  - DNSSPOOFING

SOCIAL ENGINEERING TOOL

- https://www.youtube.com/watch?v=Jjulz-xHwEo&t=2s - SITE CLONER
- https://www.youtube.com/watch?v=GC4wtfMr3t8 - SITE CLONER
- https://www.youtube.com/watch?v=sP_PDnXTX7A&t=9s - SET TOOLKIT
- https://www.youtube.com/watch?v=1TsCybFNrM0&t=315s - SITE CLONER
- https://www.youtube.com/watch?v=jXy9ewmDVBE - SITE CLONER
- https://www.youtube.com/watch?v=u9dBGWVwMMA - PHISHING ATTACKS SCARY

MITM

- https://www.youtube.com/watch?v=LEPEk5pFffw - MITM ETTERCAP
- https://www.youtube.com/watch?v=bEMwES6TQUw - MITM SSLSTRIP
- https://www.youtube.com/watch?v=GkexkyUbUd4 - MITM
- https://www.youtube.com/watch?v=-AMd5mxgpX8&t=443s - INTERCEPT SSL TRAFFIC USING MTM SSL STRIP
- https://www.youtube.com/watch?v=-rSqbgI7oZM - SNIFF NETWORK TRAFFIC MITM ATTACK
- https://es.acervolima.com/ataque-mitm-man-in-the-middle-usando-arp-poisoning/ - MITM

OTHER

- https://www.youtube.com/watch?v=sqaie9YNtpQ - PHISHING
- https://www.youtube.com/watch?v=rhd-bqE91bY - DRIFTNET
- https://www.youtube.com/watch?v=rhd-bqE91bY - DRIFTNET
- https://www.youtube.com/watch?v=Jitm4DtT2_8&t=670s - PHISHING
- https://www.youtube.com/watch?v=wsXMicWMlQI - PHISHING
- https://www.youtube.com/watch?v=MkEet3Akvyo – SET CURS OFENSIU
- https://www.youtube.com/watch?v=gKykLr59LW8 - BASIC ATTACK WITH METASPLOIT
- https://www.youtube.com/watch?v=MkEet3Akvyo - SET BASIC HACKING