Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "Careful where you step in"



Index

- DNS: --> readME <--
- DNSSEC: --> readME <--
- **DNS**: --> readME <--
- DNSSEC: --> readME <--

Deployment

Requisits:

Virtualització

- 1 SOA
- 1 Forwarder
- 2 Kali
- 3 Clients en Xarxa Interna

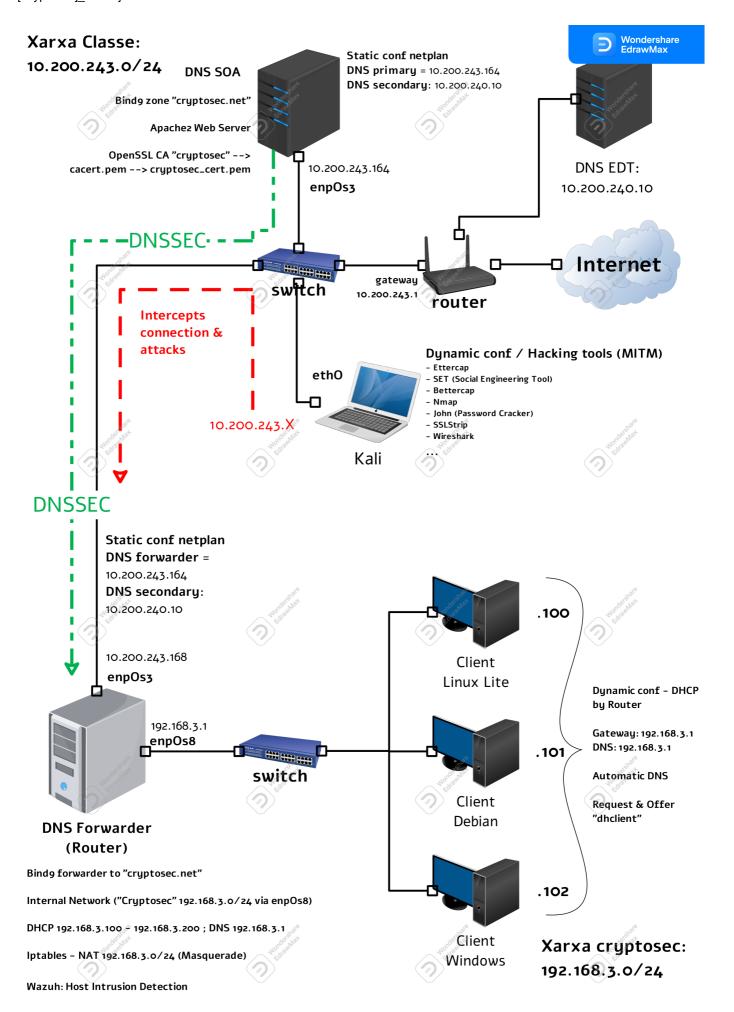
Programari CryptoSEC

- NETPLAN --> Configuración Network Manager dels Servidors Ubuntu Server.
- NMAP --> Verificació d'arp, ports... etc.
- BIND9 --> Forwarder i SOA han de poder resoldre peticions DNS als clients.
- DHCP --> Xarxa Interna --> Configuració automàtica IP i DNS.
- IPTABLES --> Xarxa Interna --> NAT a l'exterior.
- APACHE2 --> https://cryptosec.net
- TEAMVIEWER --> GUI remot
- SSH --> Accés remot
- OPENVAS --> Verificació de vulnerabilitats
- WIRESHARK --> Analitzador de paquets del sistema
- ARP -A --> Veure taula CACHE
- HOST --> Resolver
- NSLOOKUP --> Resolver
- DIG --> Resolver
- JOURNALCTL --> Veure possibles errors
- SYSTEMCTL --> Reiniciar o reload dels serveis
- SSL --> Certificats per Apache2
- ROUTING --> Per poder entrar a 192.168.3.0/24 desde la classe.
- TRACEROUTE --> Observar el traçat del paquet.
- PING --> Observar la conectivitat entre dispositius.
- CERTBOT LET'S ENCRYPT --> Generar certificats per dominis reals (*Tried*).
- WAZUH --> Detectar vulnerabilitats del sistema i de la xarxa (*Tried*).

HACKING Kali

- SET --> Setoolkit --> Software d'atacs d'Enginyeria Social
- BETTERCAP --> Framework/Sniffer per poder fer atacs de Man in the Middle.
- ZPHISHING --> Framework per simular *Phishing* real.
- ETTERCAP --> Framework/Sniffer per poder fer atacs de man in the Middle.
- JOHN --> Brute Force Attack tool --> Cracker password
- SSLSTRIP --> Strips HTTPS to HTTP (Tried)
- SLOWHTTP --> A type of DOS to take down cryptosec.net (Tried)

Practica:



Plantejament a VIRTUALBOX:

Portàtil d'en Keshi:

- Kali Linux: BRIDGE (DHCP eth0)
 - X11 Forwarding SSH o Teamviewer
 - Static Routing to 192.168.3.0/24: ip route add 192.168.3.0/24 via 10.200.243.168 dev eno1
 - Setoolkit
 - Ettercap
 - Bettercap
 - John (Brute Force Crack)
 - Wireshark
 - Nmap
 - Traceroute

Portàtil d'en Cristian:

- KALI White Hacker
- Ub 20.04 SOA "SOACryptosec": BRIDGE (DHCP enp0s3) 10.200.243.164/24
 - APACHE2: Pag www.cryptosec.net o 10.200.243.164/cryptosec/index.html
 - /var/www/html/cryptosec/index.html
 - Perquè funcioni el HTTPS cal importar el CACERT.PEM al FIREFOX.
 - DNS AUTORITARI (cryptosec.net)
 - DNS
 - DNSSEC

PC Aaron i11:

- Ub 20.04 Forwarder "ForwarderCryptosec":
 - BRIDGE (DHCP enp0s3) 10.200.243.168/24
 - Internal Network (cryptosec enp0s8 192.168.3.0/24) 192.168.3.1/24
 - IPTABLES
 - DHCP
 - DNS FORWARDING
 - Cryptosec Clients:
 - Internal Network (cryptosec enp0s3 192.168.3.0/24) 192.168.3.100/24 192.168.3.200/24

Kali (Keshi-Hacker)

- 1. Verificació de les IPS i conectivitat amb Internet.
- 2. Rebre la IP per DHCP de la classe.
- 3. Activar services.sh.
- 4. Activar Teamviewer o cctivar X11 Forwarding SSH a l'ordinador del Professor:

Extra

X11 FORWARDING (Permetre Obrir Apps mode Gràfic):

- ssh -X anonymous@ip
- xauth list \$DISPLAY --> COPIAR1
- fet \$DISPLAY --> COPIAR2
- sudo bash
- xauth add [ENGANXAR COPIAR1]
- export DISPLAY=[ENGANXAR COPIAR2]
- 5. Verificar conectivitat des de l'ordinador del PROFE i veure què es pot obrir OK.

SOA

- 1. Verificació de les IPS i conectivitat amb Internet.
- 2. Modificar NETPLAN.
 - o netplan try + netplan apply
 - IMPORTANT! Verificar *PING* i *RESOLV* cryptosec.net amb la IP adequada!
- 3. Modificar BIND9 (Primer en **DNS normal** i després **DNSSEC**).
- 4. Verificar **APACHE2**: 10.200.243.164 i 10.200.243.164/cryptosec/index.html
 - Verificar els fitxers de "cryptosec.net" a Apache2
 - Són a /etc/apache2/sites-available/cryptosec.net.conf
 - Comandes per verificar Apache2:
 - **a2ensite cryptosec.net.conf** --> Habilita els virtualHost.
 - apache2ctl configtest --> Verifica apache2
 - openssl x509 --noout --text -in cacert.pem
 - openssl x509 --noout --text -in cryptosec_cert.pem
 - **ufw allow "Apache Full"** --> Permet firewall Apache2
- 5. Verificar que **DNSSEC** funciona:
 - dnssec-keygen --> GENERAR
 - \$INCLUDE a db.cryptosec.net --> Signatura manual
 - o dnssec-signzone --> Signar autom .signed
 - dig cryptosec.net +dnssec +multiline
 - dnssec-verify -o cryptosec.net db.cryptosec.net [-v level]
 - host cryptosec.net
 - nslookup cryptosec.net
- 6. Verificar claus de **DNSSEC** i engegada davant **spoofing** de la zona.

FORWARD

- 1. Verificació de les **IPS** i conectivitat amb Internet.
- 2. Modificar NETPLAN.
 - netplan try + netplan apply.
 - IMPORTANT! Verificar PING i RESOLV cryptosec.net amb la IP adequada!
 - Verificar que el DNS nameserver sigui FORWARDER a 10.200.243.164.
- 3. Activar IPTABLES: cryptonat.sh
 - Verificar ip estàtica de la classe 10.200.243.168.
- 4. Activar FORWARDING de DNS.
 - Verificar named.conf.default-zones
 - Ver named.conf.options
 - Reiniciar i verificar que facin PING I RESOLV. Sinó Journal.
- 5. Activar **DHCP** per a 192.168.3.0/24 a la interfície **enp0s8**.
 - Reiniciar DHCP i verificar.
 - Fitxers /etc/dhcp/dhcpd.conf i /etc/default/isc-dhc-server
 - Verificar amb CLIENTS que rebin la IP i facin resoldre a cryptosec.net.

CLIENTS

- 1. Obrir i verificar que rebin IP i DNS.
 - o Sinó reiniciar networking o dhclient -r (release) i dhclient -v (verbose).
 - Al FIREFOX introduir el cacert.pem --> Importar al navegador i provar https://cryptosec.net
 - LINUX: systemd-resolve --flush-cache --> Neteja la cahcé DNS
 - Windows: ipconfig /flushdns

Comander per verificar la conectivitat:

- systemd-resolved --status --> Verifica DNS actual
- nmap -sP 10.200.243.0/24 --> Escaneig de la Xarxa
- resolvectl query cryptosec.net --> Resol cryptosec.net

- host cryptosec.net --> Resol cryptosec.net
- dig cryptosec.net +dnssec +multiline --> Resol cryptosec.net segur DNSSEC.

• EXTRES:

- Ordinador PROFE fer ROUTING a 192.168.3.0/24
 - Han de tenir NAT a l'exterior (Forwarder ha d'activar Iptables)
 - ip route add 192.168.3.0/24 via 10.200.243.168 dev eno1
 - Provar PING
 - Provar SSH -X usuariClientCryptosec@192.168.3.x

X11 FORWARDING (Permetre Obrir Apps mode Gràfic):

- ssh -X anonymous@ip
- xauth list \$DISPLAY --> COPIAR1
- fet \$DISPLAY --> COPIAR2
- sudo bash
- xauth add [ENGANXAR COPIAR1]
- export DISPLAY=[ENGANXAR]

Atacs del hacker

- Brute Force Attack Cracking Password with John: El hacker ha aconseguit una copia dels fitxers /etc/passwd i /etc/shadow i les ha anomenat mini-passwd.txt i mini-shadow.txt. John és un tool de Kali que permetrà desxifrar els *hashes* de les contrasenyes. Quant més difícil més temps trigarà. Posarem contrasenyes sencilletes. Podrem veure com les desxifra. Utilitzarà un diccionari rockyou.txt. Aprofitant també que l'usuari ha
- ARP Poisoning / Spoofing (2 parts) (BETTERCAP): Envenenament de les taules ARP de les víctimes implicades i reenviament de paquets al hacker. Amb el Wireshark - ARP - Nmap, veurem com fa el duplicat de MAC.
 - MITM Eavesdropping (Sniffing) (BETTERCAP): Amb l'ARP Spoof d'abans activarem un sniffer i estarem escoltant la màquina afectada i veient les pàgines on visita. Podem captar credencials de pàgines HTTP.

- DNS Poisoning / Spoofing) (BETTERCAP): Amb l'ARP Spoof d'abans activarem un dnsspoof i injectarem un registre de DNS fals on ens redirigirà a la nostra màquina on hi tindrem una fake page: m0odle.escoladeltreball.org (Moodle EDT) i l'enviarem per correu utilitzant SET dient que "URGENT! L'Eduard ha posat les notes de M06, entra urgentment i mira la nota que tens!!!" llavors l'usuari entrarà i no se n'adonarà i li robarem les credencials mostrades al SET.
- Spoofing CryptoSEC.NET + DOS SlowHTTP (take down cryptosec.net) (BETTERCAP): Ídem que l'anterior però els targets son el SOA i el Forwarding, els clients interns de CryptoSEC quan hagin d'anar a la pàgina web cryptosec.net, entraràn a cryptos3c.net ja que el hacker ha avisat que hi hà una urgència a la pàgina principal i han d'entrar a la pàgina web dada pel hacker i les seves credencials seràn robades sense que se'n adoni! Abans de tot, el hacker utilitzarà una eina per que la pàgina de cryptosec.net vagi més lent durant uns minuts. Durant aquest minuts aprofitarà per donar un comunicat oficial a l'empresa CryptoSEC dient que la pàgina ha sigut tumbada i han d'anar a un altra anomenada cryptos3c.net.
- **ZPHISHING: Phishing with a real "fake" HTTPS website**: Exemple real de **Phishing** automatitzat i desplegat a **Cloudflare** per un programa anomenat **Zphishing**. Genera servidor temporal a Internet amb una plantilla a escollir de l'usuari. Enmascarar el enllaç amb un *url shortner* i enviar-ho a alguna víctima mitjançant **SET** que enviarà el correu automàticament amb un compte de **Gmail**. L'usuari entrarà però no veurà l'enllaç perquè és una emergència i posarà les seves credencials. D'aquesta manera recollirem l'usuari i la contrasenya de l'usuari (*Credential Harvester*).

Credentials

aaroncryptosec@gmail.com:acryptosec22

cristiancryptosec@gmail.com:acryptosec22

Victima: cryptocorp03@gmail.com:CryptoCorp03\$