



CONTENIDO

Información del taller	2
1.- Conocimiento local de la red:	3
2.- Reconocimiento DNS:	4
3.- Conocer tu sistema operativo y el dominio:	7
4.- Port Scanning	10
5.- Identificación y validación de vulnerabilidades:	11
6.- Gestión de IOCs (Indicators of Compromise):	13
7.- Análisis de malware estático:	15

Información del taller

Fecha:

- 18 de setiembre 2022

Objetivo:

- Mostrar el funcionamiento de herramientas que se podrían usar para comprender cómo prevenir y defender frente a un ciberataque.

Dirigido:

- Analistas de ciberseguridad, networking, sistemas.
- Responsables de Seguridad de la Información
- Estudiantes de Sistemas, Redes, Ciberseguridad.

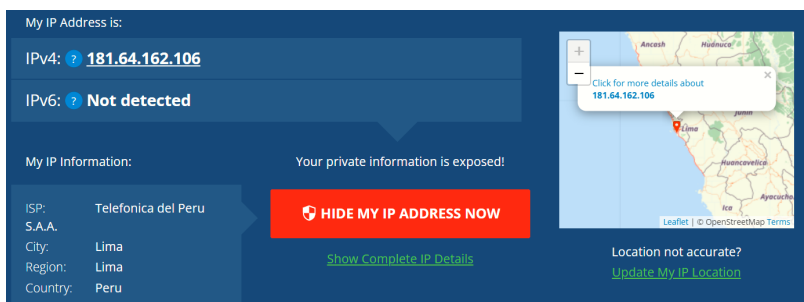
Requerimientos:

- Máquina 1 y 2 : Física o virtual
- Máquina 1: gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor*
- Máquina 2: gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
- RAM: 4 GB como mínimo
- Máquina 1, Podría ser Kali Linux,
<https://www.kali.org/get-kali/#kali-virtual-machines>
- Máquina 2, Podría ser tu host principal bajo Windows en cualquier versión.
- Acceso a Internet libre.
- Permisos de Administrador para la instalación de programas y utilidades.

1.- Conocimiento local de la red:

Herramientas que permitan conocer la dirección IP pública, proveedor de Internet, AS Sistema Autónomo:

- Who is my ip address, Dirección IP, ISP, City.
 - <https://whatismyipaddress.com/>



My IP Address is:

IPv4: **181.64.162.106**

IPv6: **Not detected**

My IP Information: Your private information is exposed!

ISP: Telefonica del Peru

S.A.A. **HIDE MY IP ADDRESS NOW**

City: Lima

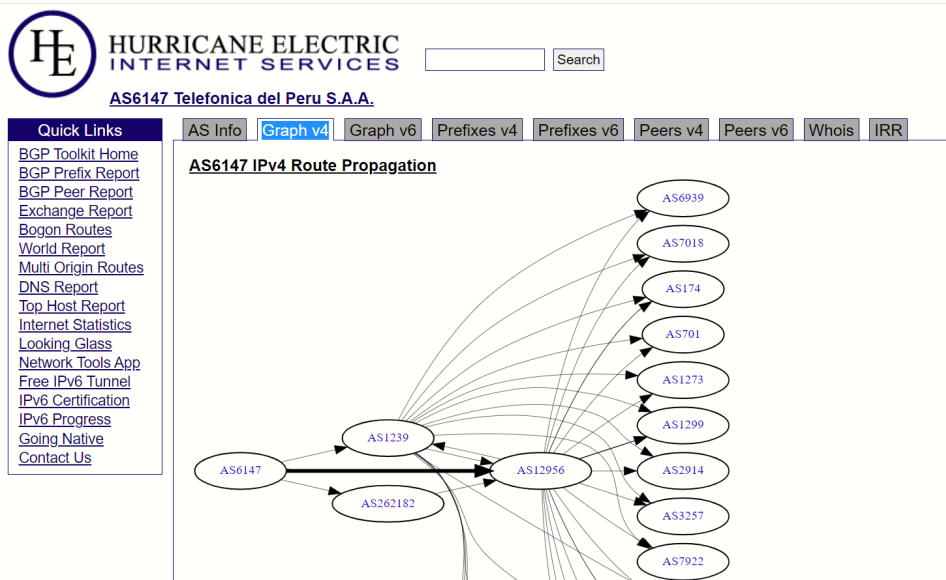
Region: Lima

Country: Peru

Location not accurate? [Update My IP Location](#)

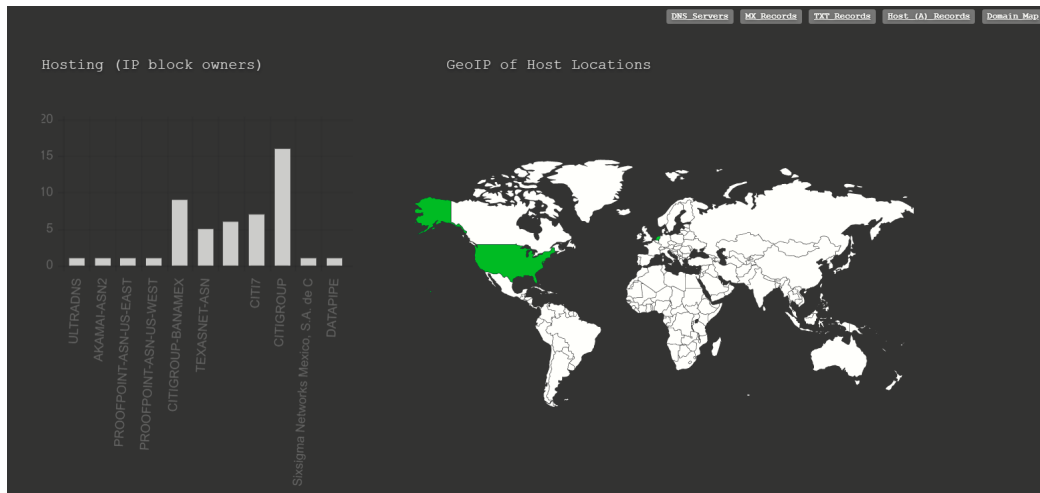
[Show Complete IP Details](#)

- Como salgo a Internet, sobre mi proveedor de Internet
 - <https://bgp.he.net/>
 - https://bgp.he.net/AS6147#_graph4



2.- Reconocimiento DNS:

- Reconocimiento DNS, búsqueda e identificación de registros DNS, MX, A:
- <https://dnsdumpster.com/>
- Ejemplo: tuempresa.com, banamex.com, cemex.com
- Geo IP of host locations



- DNS Server:

DNS Servers		
ns1.cemex.com. 🌐 🔄 🛡️ 👁️ 🟢	200.23.29.245	CEMEX Central, S.A. de C.V. Mexico
ns3.cemex.com. 🌐 🔄 🛡️ 👁️ 🟢	65.246.74.146	UUNET United States
ns2.cemex.com. 🌐 🔄 🛡️ 👁️ 🟢	200.23.29.246	CEMEX Central, S.A. de C.V. Mexico

DNS Servers		
ns1.nsroot1.com. 🌐 🔄 🛡️ 👁️ 🟢	156.154.64.172 pdns172.ultradns.com	ULTRADNS United States
ns2.nsroot2.com. 🌐 🔄 🛡️ 👁️ 🟢	193.108.91.190 ns1-190.akam.net	AKAMAI-ASN2 Netherlands
MX Records ** This is where email for the domain goes...		
5 mx-b.mail.citi.com. 🏠 🔄 👁️ 🟢	67.231.153.94 mx-b.mail.citi.com	PROOFPOINT-ASN-US-EAST United States
5 mx-a.mail.citi.com. 🏠 🔄 👁️ 🟢	67.231.145.106 mx-a.mail.citi.com	PROOFPOINT-ASN-US-WEST United States

- MX Records:

```
MX Records ** This is where email for the domain goes...
5 cemex-com.mail.protection.outlook.com.      104.47.73.138      MICROSOFT-CORP-MSN-AS-BLOCK
📧 📧 📧 📧 mail-mw2nam080138.inbound.protection.outlook.com United States
```

```
MX Records ** This is where email for the domain goes...
5 mx-b.mail.citi.com.                        67.231.153.94      PROOFPOINT-ASN-US-EAST
📧 📧 📧 📧 mx-b.mail.citi.com United States
5 mx-a.mail.citi.com.                        67.231.145.106     PROOFPOINT-ASN-US-WEST
📧 📧 📧 📧 mx-a.mail.citi.com United States
```

- TXT Records:

```
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations
"h7r4108zgs01khq7d9d76rb9xtt8wyql"
"globalsign-domain-verification=9fb5cddb28c5c5d61feb9768f9f81c4"
"Dynatrace-site-verification=lbdfa2c0-7ccc-42b3-b0a8-b46bbcc9132c_ndh4inn9nf551mjn7i7vkv709g"
"6e6d266675aa499d85eced6b44e8cc78"
"2qtlhrsp6dfk190cnbg5hm101"
"MS=ms96021265"
"smartsheet-site-validation=Mjd-2asVhDieXnL56zwn14T2PGcuRY51"
"v=spf1 ip4:200.23.29.132 ip4:200.23.29.133 ip4:200.23.29.139 ip4:200.23.29.188 ip4:200.23.29.189 ip4:200.23.29.190 ip4:189.205.121.190 ip4:12.129.117.140 ip4:12.129.117.141 ip4:12.129.117.143 include:spf.protection.outlook.com -all"
"3v1lplosalv5hbk22non2esb5j"
"5mkpc5d8kqtnpbpxws9y287s3wwvlrzn"
"status-page-domain-verification=vcfdwqx4g443"
"_globalsign-domain-verification=G2PlFzVkvHAWYhihDKEBZ1CrjgKUOJTvpjeM1149h5"
```

```
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations
"MS=ms91144615"
"MS=C18C7B831E36CCE04AE8E63A5CDE7197BD34D267"
"v=spf1 a:1._spf.citigroup.com a:2._spf.citigroup.com a:mailir.citi.com include:spf-00123c01.pphosted.com include:spf.mittum.com redirect=extl._spf.citigroup.com"
```



- A, Host Records:

ermlogin.cemex.com Microsoft-HTTPAPI/2.0 Microsoft-HTTPAPI/2.0	52.237.251.10	MICROSOFT-CORP-MSN-AS-BLOCK United States
mx2.cemex.com mx1.cemex.com	200.23.29.115	CEMEX Central, S.A. de C.V. Mexico
b2bcpo.cemex.com server: SAP NetWeaver Application Server 7.53 / AS Java 7.50 server: SAP NetWeaver Application Server 7.53 / AS Java 7.50	189.205.121.182 bb-mvs-189-205-121- 182.mexdf.static.axtel.net	CEMEX Central, S.A. de C.V. Mexico
mycemexqa2.cemex.com BigIP Apache/2.4.25 (Win64) OpenSSL/1.0.2a Apache/2.4.25	189.205.121.187 bb-mvs-189-205-121- 187.mexdf.static.axtel.net	CEMEX Central, S.A. de C.V. Mexico
meet.vc.cemex.com Microsoft-IIS/10.0 Microsoft-IIS/10.0 IIS/10.0 IIS/10.0	57.77.35.33	ORANGE-BUSINESS-SERVICES-IPSN-ASN Ireland
s360qa.cemex.com Microsoft-IIS/8.5 IIS/8.5	189.205.121.171 bb-mvs-189-205-121- 171.mexdf.static.axtel.net	CEMEX Central, S.A. de C.V. Mexico

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

banamex.com citibanamex.com	192.193.206.22	CITIGROUP-BANAMEX United States
sndr001.banamex.com	207.207.2.250	TEXASNET-ASN United States
nmxjar-edns01.banamex.com nmxjar-edns01.banamex.com	192.193.204.74	CITIGROUP-BANAMEX United States
nmxmtty-edns01.banamex.com nmxmtty-edns01.banamex.com	192.193.207.41	United States
mailcpx01.banamex.com mailcpx01.banamex.com	192.193.206.152	CITIGROUP-BANAMEX United States
ns1.banamex.com ns1.banamex.com	192.193.204.42	CITIGROUP-BANAMEX United States
dev.banamexsoaproxy1.banamex.com	200.52.96.43	CIT17 Mexico
sandbox.banamexsoaproxy1.banamex.com	192.193.104.97	CITIGROUP United States
mailcpx02.banamex.com mailcpx02.banamex.com	192.193.206.154	CITIGROUP-BANAMEX United States

3.- Conocer tu sistema operativo y el dominio:

- Se necesita conocer las aplicaciones, procesos, conexiones de red para validar comportamientos correctos o maliciosos.
- Versión:
 - #winver
 - #systeminfo:

```
C:\Users\USUARIO>systeminfo

Nombre de host:                DESKTOP-MI [REDACTED]
Nombre del sistema operativo:  Microsoft Windows 10 Home Single Language
Versión del sistema operativo: 10.0.19044 N/D Compilación 19044
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de:                  USUARIO
Organización registrada:
Id. del producto:              00327-60000-00000-AA666
Fecha de instalación original:  24/04/2021, 11:16:42
Tiempo de arranque del sistema: 18/09/2022, 00:21:43
Fabricante del sistema:        HP
Modelo del sistema:            OMEN by HP Laptop
Tipo de sistema:                x64-based PC
Procesador(es):                 1 Procesadores instalados.
                                [01]: Intel64 Family 6 Model 158 Stepping 9 GenuineIntel ~2496 Mhz
Versión del BIOS:                Insyde F.35, 23/01/2017
Directorio de Windows:          C:\Windows
Directorio de sistema:          C:\Windows\system32
Dispositivo de arranque:        \Device\HarddiskVolume1
Configuración regional del sistema: es-mx;Español (México)
Idioma de entrada:              es-mx;Español (México)
Zona horaria:                    (UTC-05:00) Bogotá, Lima, Quito, Rio Branco
Cantidad total de memoria física: 16,236 MB
Memoria física disponible:       7,513 MB
Memoria virtual: tamaño máximo: 18,668 MB
Memoria virtual: disponible:     5,713 MB
Memoria virtual: en uso:         12,955 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio:                          WORKGROUP
Servidor de inicio de sesión:    \\DESKTOP-MI [REDACTED]
Revisión(es):                    19 revisión(es) instaladas.
                                [01]: KB5017022
                                [02]: KB4562830
                                [03]: KB4570334
                                [04]: KB4577586
                                [05]: KB4580325
                                [06]: KB4586864
```

FIGURA 12

- Windows:
 - TCPView, Sysinternals.
 - Proceso, ID, local address, local port, remote address, remote port, etc
 - <https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview>

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Addr...	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
[Time Wait]		TCP	Time Wait	DESKTOP-MD...	57476	DESKTOP-MD...	9150						
tor.exe	8068	TCP	Established	DESKTOP-MD...	57457	212-51-141-2...	9002	18/09/2022 22:56:42	tor.exe	25	197	23,730	292,519
[Time Wait]		TCP	Time Wait	DESKTOP-MD...	57447	schulzcom.de	9001						
tor.exe	8068	TCP	Established	DESKTOP-MD...	57447	schulzcom.de	9001	18/09/2022 22:56:33	tor.exe	2	5	1,063	3,188
Teams.exe	9908	TCP	Established	DESKTOP-MD...	57487	52.114.104.172	https	18/09/2022 22:59:24	Teams.exe	8	6	3,033	1,018
svchost.exe	1940	TCP	Established	DESKTOP-MD...	57490	13.68.233.9	https	18/09/2022 22:59:37	CDPUserSvc_1632ea	8	9	10,360	11,939
svchost.exe	4380	TCP	Established	DESKTOP-MD...	59286	207.2.167	https	18/09/2022 21:33:45	WpnService				
chrome.exe	7048	TCP	Established	DESKTOP-MD...	64344	whatsapp-cd...	https	18/09/2022 21:33:56	chrome.exe	43	44	4,847	10,265
chrome.exe	7048	TCP	Established	DESKTOP-MD...	64345	40.102.32.130	https	18/09/2022 21:33:56	chrome.exe	70	73	16,335	17,532
chrome.exe	7048	TCP	Established	DESKTOP-MD...	64346	cf-in-f188.1e1...	https	18/09/2022 21:33:56	chrome.exe	1	1	26	26
chrome.exe	7048	TCP	Established	DESKTOP-MD...	64475	104.244.42.65	https	18/09/2022 22:15:31	chrome.exe	6	4	402	429
chrome.exe	7048	TCP	Established	DESKTOP-MD...	57261	104.244.42.194	https	18/09/2022 22:40:41	chrome.exe	6	4	1,074	309
chrome.exe	7048	TCP	Established	DESKTOP-MD...	64814	cf-in-f121.1e1...	https	18/09/2022 22:29:27	chrome.exe	72	26	12,496	1,817
[Time Wait]		TCP	Time Wait	DESKTOP-MD...	57321	139.148.107.34...	https						
SearchApp.exe	8608	TCP	Close Wait	DESKTOP-MD...	57380	152.199.55.200	https	18/09/2022 22:56:12	SearchApp.exe	5	6	985	1,609
Teams.exe	9908	TCP	Established	DESKTOP-MD...	57403	52.112.120.14	https	18/09/2022 22:56:20	Teams.exe	12	14	7,758	3,269
tor.exe	8068	TCP	Established	DESKTOP-MD...	57452	62diviri.qwta...	https	18/09/2022 22:56:38	tor.exe	244	441	166,250	491,938
Teams.exe	10712	TCP	Established	DESKTOP-MD...	57412	52.114.133.47	https	18/09/2022 22:56:25	Teams.exe	7	7	463	309
[Time Wait]		TCP	Time Wait	DESKTOP-MD...	57474	13.68.233.9	https						
[Time Wait]		TCP	Time Wait	DESKTOP-MD...	57463	lb-140-82-11...	https						
chrome.exe	7048	TCP	Established	DESKTOP-MD...	57485	cb-in-f17.1e1...	https	18/09/2022 22:58:41	chrome.exe	12	12	7,324	5,060
chrome.exe	7048	TCP	Established	DESKTOP-MD...	57284	cdn-185-199-...	https	18/09/2022 22:48:24	chrome.exe	18	144	1,667	203,144
SearchApp.exe	8608	TCP	Close Wait	DESKTOP-MD...	57430	152.199.54.186	https	18/09/2022 22:56:28	SearchApp.exe	5	6	669	1,186
chrome.exe	7048	TCP	Established	DESKTOP-MD...	57486	20.189.173.13	https	18/09/2022 22:56:49	chrome.exe	4	7	3,069	6,735
tor.exe	8068	TCP	Established	DESKTOP-MD...	57445	s91-143-81-2...	http	18/09/2022 22:56:32	tor.exe	402	1,535	282,356	2,607,126
putty.exe	2060	TCP	Established	DESKTOP-MD...	64554	167.172.38.120	ssh	18/09/2022 22:16:39	putty.exe				
System	4	TCP	Listen	DESKTOP-MD...	139	0.0.0.0	0	18/09/2022 21:33:43	System				
System	4	TCP	Listen	DESKTOP-MD...	139	0.0.0.0	0	18/09/2022 21:33:45	System				
vmware-hostd.exe	5948	TCP	Listen	DESKTOP-MD...	443	0.0.0.0	0	18/09/2022 00:22:05	VMwareHostd				

- Linux:
 - #lsof -i TCP:22, buscar procesos en un específico puerto
 - #lsof -i, lista todas las conexiones de red
 - #lsof -i 4/6, lista archivos abierto de red IPv4/6
 - #lsof -i TCP:1-1024, lista todos los procesos de archivos abiertos de puertos TCP en los rangos 1-1024.
 - #lsof /dev/hd4, busca todos los archivos abierto en el device /dev/dh4
 - #lsof /u/abe/foo, busca el proceso que tiene /u/abe/foo abierto


```

root@saturno_02mar20:~# lsof -i 4
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sshd 1474 root 3u IPv4 18831 0t0 TCP *:ssh (LISTEN)
sshd 1799 root 3u IPv4 64321487 0t0 TCP *:1022 (LISTEN)
sshd 9795 root 3u IPv4 67519905 0t0 TCP 167. [REDACTED] ssh->181. [REDACTED]:58063 (ESTABLISHED)
sshd 10224 root 3u IPv4 67527630 0t0 TCP 167. [REDACTED] ssh->181. [REDACTED]:64554 (ESTABLISHED)
root@saturno_02mar20:~#
root@saturno_02mar20:~# lsof -i 6
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sshd 1474 root 4u IPv6 18833 0t0 TCP *:ssh (LISTEN)
sshd 1799 root 4u IPv6 64321496 0t0 TCP *:1022 (LISTEN)
root@saturno_02mar20:~# lsof -i TCP:1-1024
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sshd 1474 root 3u IPv4 18831 0t0 TCP *:ssh (LISTEN)
sshd 1474 root 4u IPv6 18833 0t0 TCP *:ssh (LISTEN)
sshd 1799 root 3u IPv4 64321487 0t0 TCP *:1022 (LISTEN)
sshd 1799 root 4u IPv6 64321496 0t0 TCP *:1022 (LISTEN)
sshd 9795 root 3u IPv4 67519905 0t0 TCP 167. [REDACTED] ssh->181. [REDACTED]:58063 (ESTABLISHED)
sshd 10224 root 3u IPv4 67527630 0t0 TCP 167. [REDACTED] ssh->181. [REDACTED]:64554 (ESTABLISHED)
sshd 10303 root 3u IPv4 67527872 0t0 TCP 167. [REDACTED] :1022->b5 [REDACTED] br:58928 (ESTABLISHED)
sshd 10304 sshd 3u IPv4 67527872 0t0 TCP 167. [REDACTED] :1022->b5 [REDACTED] br:58928 (ESTABLISHED)
root@saturno_02mar20:~#
root@saturno_02mar20:~# lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sshd 1474 root 3u IPv4 18831 0t0 TCP *:ssh (LISTEN)
sshd 1474 root 4u IPv6 18833 0t0 TCP *:ssh (LISTEN)
sshd 1799 root 3u IPv4 64321487 0t0 TCP *:1022 (LISTEN)
sshd 1799 root 4u IPv6 64321496 0t0 TCP *:1022 (LISTEN)
sshd 9795 root 3u IPv4 67519905 0t0 TCP 167. [REDACTED] ssh->181. [REDACTED]:6:58063 (ESTABLISHED)
sshd 10224 root 3u IPv4 67527630 0t0 TCP 167. [REDACTED] ssh->181. [REDACTED]:6:64554 (ESTABLISHED)
sshd 10309 root 3u IPv4 67528008 0t0 TCP 167. [REDACTED] ssh->61. [REDACTED]:43368 (ESTABLISHED)
sshd 10310 sshd 3u IPv4 67528008 0t0 TCP 167. [REDACTED] ssh->61. [REDACTED]:43368 (ESTABLISHED)
root@saturno_02mar20:~#

```

- Para conocer tu dominio utilizaremos los siguientes comandos propios de Windows:
 - c:\> net group "domains computers" /domain
 - c:\> net group "domains controllers"
 - c:\> net group "domains controllers" /domain
 - DC0100 DC0240



4.- Port Scanning

- Usaremos nmap para Windows o Linux
- <https://nmap.org/>
- Opciones:
 - nmap -sT -Pn -O [#VÍCTIMA]; nmap -sT -Pn -p- [#VÍCTIMA]
 - nmap -sS -Pn -p 21,22,23,80,443,1433,3389 [#VÍCTIMA]
 - nmap -iL [LIST.TXT]; #VÍCTIMA, IP, IPs, Rango/Máscara.
- Tipos de Scanning:
 - TCP SYN Scan, -sS; TCP Connect Scan, -sT; Fin Scan, -sF
 - XMAS Scan, -sX; Null Scan, -sN
 - Versión Detection, -sV; UDP Scan, -sU
 - List Scan, -sL; Operating System Detection, -O
- Ejemplos:
- Scanning, host discovery
 - #nmap -n -sn [#VÍCTIMA]
 - #nmap -p -Pn -sV 21,22,23,53,80,443,1433,3389 [#VÍCTIMA]
- Scanning, detección de sistema operativo:
 - #nmap -O -osscan-limit [#VÍCTIMA]
 - #nmap -O -p -Pn -sV 21,22,23,53,80,443,1433,3389 [#VÍCTIMA]
 - #nmap -sT -sV -PO -O IP

```
Nmap scan report for 19[REDACTED]
Host is up (0.18s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
22/tcp    open  ssh          OpenSSH 5.3 (protocol 2.0)
113/tcp   closed ident
179/tcp   open  tcpwrapped
443/tcp   open  ssl/http     Apache httpd 2.2.15 ((CentOS))
3306/tcp   closed mysql
5432/tcp  open  postgresql   PostgreSQL DB
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following
SF-Port5432-TCP:V=7.92SVN%I=7%D=8/25%Time=63077DC5%P=i686-pc-linux-gnu%r(S
SF:MBProgNeg,85,"E\0\0\0\x84SFATAL\0C0A000\0Munsupported\x20frontend\x20pr
SF:otocol\x2065363\0.19778;\x20server\x20supports\x201\0\x20to\x203\0\0fp
SF:ostmaster\.c\0L1624\0RProcessStartupPacket\0\0");
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10
OS details: Linux 2.6.32, Linux 2.6.32 or 3.10
Service Info: Host: E[REDACTED]
```

5.- Identificación y validación de vulnerabilidades:

- Mapear vulnerabilidades en tu organización:
 - Cybersecurity & Infrastructure Security Agency
 - Known Exploited Vulnerabilities Catalog
 - Fuente: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Validar vulnerabilidad
 - SMBv1
 - Usaremos nmap, <https://nmap.org/>
 - Vulnerabilidad: SMB MS 017-010
 - Desde un Kali linux:
 - #cd /usr/share/nmap/scripts
 - #wget <https://raw.githubusercontent.com/cldrn/nmap-nse-scripts/master/scripts/smb-vuln-ms17-010.nse>
 - #nmap -d -sC -p445 --script smb-vuln-ms17-010.nse IP
 - Fuente: <https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17-010/>

```

root@kali:~#
root@kali:~# nmap -d -sC -p445 --script smb-vuln-ms17-010.nse 192.168.56.101
Starting Nmap 7.30 ( https://nmap.org ) at 2017-05-31 19:32 PET
----- Timing report -----
hostgroups: min 1, max 100000
RTT-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
NSE: Using Lua 5.3
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:32
Completed NSE at 19:32, 0.00s elapsed
Initiating ARP Ping Scan at 19:32
Scanning 192.168.56.101 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] & 0x080027c0 and arp[22:2] & 0x0806
Completed ARP Ping Scan at 19:32, 0.00s elapsed (1 total hosts)
Overall sending rates: 719.42 packets / s, 39219.83 bytes / s.
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 0, OK: 0, NX: 0, DR: 0, SF: 0, TR: 0, CN: 0]
Initiating SYN Stealth Scan at 19:32
Scanning 192.168.56.101 [1 port]
Packet capture filter (device eth0): dst host 192.168.56.102 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.56.101)))
Discovered open port 445/tcp on 192.168.56.101
Completed SYN Stealth Scan at 19:32, 0.00s elapsed (1 total ports)
Overall sending rates: 892.06 packets / s, 39250.67 bytes / s.
NSE: Script scanning 192.168.56.101.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:32
NSE: Starting smb-vuln-ms17-010 against 192.168.56.101.
NSE: [smb-vuln-ms17-010 192.168.56.101] SMB: Added account '' to account list
NSE: [smb-vuln-ms17-010 192.168.56.101] SMB: Added account 'guest' to account list
NSE: [smb-vuln-ms17-010 192.168.56.101] LM Password:
NSE: [smb-vuln-ms17-010 192.168.56.101] SMB: Extended login to 192.168.56.101 as PCWIN7\guest failed (NT_STATUS_LOGON_FAILURE)
NSE: [smb-vuln-ms17-010 192.168.56.101] LM Password:
NSE: [smb-vuln-ms17-010 192.168.56.101] Connected to share 'IPC$'
NSE: [smb-vuln-ms17-010 192.168.56.101] Valid SMB COM TRANSACTION response received
NSE: [smb-vuln-ms17-010 192.168.56.101] STATUS_INSUFF_SERVER_RESOURCES response received
NSE: [smb-vuln-ms17-010 192.168.56.101] This host is missing the patch for ms17-010!
NSE: Finished smb-vuln-ms17-010 against 192.168.56.101.
Completed NSE at 19:32, 0.01s elapsed
Nmap scan report for 192.168.56.101
Host is up, received arp response (0.90019s latency).
Scanned at 2017-05-31 19:32:23 PET for 6s
PORT      STATE SERVICE      REASON
445/tcp   open  microsoft-ds syn-ack ttl 128
MAC Address: 08:00:27:74:9D:CD (Oracle VirtualBox virtual NIC)

Host script results:
smb-vuln-ms17-010:
VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  Ids: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).
Disclosure date: 2017-03-14
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Final times for host: srtt: 189 rttvar: 3755 to: 100000
NSE: Script Post-scanning.
NSE: Starting runlevel 3 (of 1) scan.

```

- Referencia, validar vulnerabilidad:
 - CVE-2019-0708



- <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0708>
- Usaremos: rdpSCAN for CVE-2019-0708 bluekeep vuln
- <https://github.com/robertdavidgraham/rdpSCAN>
-
- Referencia, validar vulnerabilidad:
 - CVE-2018-13379
 - Usaremos nmap, <https://nmap.org/>
 - <https://github.com/purplesecmx/nmapscripts/blob/master/CVE-2018-13379.nse>
 - Validar: /usr/share/nmap/scripts
 - #wget
<https://github.com/purplesecmx/nmapscripts/blob/master/CVE-2018-13379.nse> -P /usr/share/nmap/scripts

```
root@saturno 02mar20:/usr/share/nmap/scripts# wget https://github.com/purplesecmx/nmapscripts/blob/master/CVE-2018-13379.nse -P /usr/share/nmap/scripts
--2022-09-19 17:31:06-- https://github.com/purplesecmx/nmapscripts/blob/master/CVE-2018-13379.nse
Resolving github.com (github.com)... 140.82.121.3
Connecting to github.com (github.com)|140.82.121.3|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '/usr/share/nmap/scripts/CVE-2018-13379.nse'

CVE-2018-13379.nse          [ <> ] 183.85K --.-KB/s  in 0.04s

2022-09-19 17:31:07 (4.75 MB/s) - '/usr/share/nmap/scripts/CVE-2018-13379.nse' saved [188261]

root@saturno 02mar20:/usr/share/nmap/scripts#
```



6.- Gestión de IOCs (Indicators of Compromise):

- Existe la necesidad de importar IOCs de los últimos ciberataques.
- Referencia 1: Ransomware Zeppeling
 - Fecha: Original release date: August 11, 2022
 - Zeppelin actors gain access to victim networks via [RDP exploitation \[T1133\]](#), [exploiting SonicWall firewall vulnerabilities \[T1190\]](#), and [phishing campaigns \[T1566\]](#).
 - <https://www.cisa.gov/uscert/ncas/alerts/aa22-223a>
 - IOCs:

MD5	SHA1	SHA256
981526650af8d6f8f20177a26abb513a	4fee2cb5c98abbe556e9c7ccfebe9df4f8cde53f	001938ed01bfde6b100927ff8199c65d1bfff30381b80b846f2e3fe5a0d2df21d
c25d45e9bbfea29cb6d9ee0d9bf2864d	eaef8d315cca71e997063a2baec5cc73fad9453	a42185d506e08160cb96c81801fbc173fb071f4a2f284830580541e057f4423b
183b6b0c90c1e0276a2015752344a4cf	1cb5e8132302b420af9b1e5f333c507d8b2a2441	aa7e2d63fc991990958dfb795a0aed254149f185f403231eaebe35147f4b5ebe
9349e1cc3de7c7f6893a21bd6c3c4a6b	db398e38ee6221d7e4aa49d8f96799cca4d87e1	a2a9385cbbcfacc2d541f5bd92c38b0376b15002901b2fd1cc62859e161a8037
c8f75487d0d496a3746ec81a5ecc6dc	4b91a91a98a2f0128c80f8ceef0f5d293adf0cd	54d567812eca7fc5f2ff566e7fb8a93618b6d2357ce71776238e0b94d55172b1
477eedb422041385e59a4fff72cb97c1	9892cc90e6712d3548e45f34f14f362bccedf0be	fb59f163a2372d09cd0fc75341d3972dd3087d2d507961303656b1d791b17c6
5841ef35aaff08bb03d25e5afe3856a2	ffd228b0d7afe7cab4e9734f7093e7ba01c5a06e	1e3c5a0aa079f8dfcc49cdca82891ab78d016a919d9810120b79c5deb332f388
d6c4b253ab1d169cf312fec12cc9a28f	0f47c279fea1423c7a0e7bc967d9ff3fae7a0de8	347f14497df4df73bc414f4e852c5490b12bd991a4b3811712bac7476a3f1bc9

- Herramientas, validar IOCs:
 - Virus Total, <https://www.virustotal.com/gui/home/upload>
 - Alient Vault, <https://otx.alienvault.com/>
 - AbuseIPDB - IP Address Blacklist, <https://abuseipdb.com>
 - Ejemplo:
 - SHA256:
001938ed01bfde6b100927ff8199c65d1bfff30381b80b846f2e3fe5a0d2df21d

- Referencia 2: Ransomware Voice Society
 - Fecha: Original release date: September 06, 2022 | Last revised: September 08, 2022
 - Over the past several years, the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks.
 - Vice Society actors have been observed exploiting the PrintNightmare vulnerability (CVE-2021-1675 and CVE-2021-34527) to escalate privileges [T1068].
 - <https://www.cisa.gov/uscert/ncas/alerts/aa22-249a>

- IOCs:

Indicators of Compromise (IOCs)

Email Addresses
v-society.official@onionmail[.]org
ViceSociety@onionmail[.]org
OnionMail email accounts in the format of [First Name][Last Name]@onionmail[.]org

IP Addresses for C2	Confidence Level
5.255.99[.]59	High Confidence
5.161.136[.]176	Medium Confidence
198.252.98[.]184	Medium Confidence
194.34.246[.]90	Low Confidence

See Table 1 for file hashes obtained from FBI incident response investigations in September 2022.

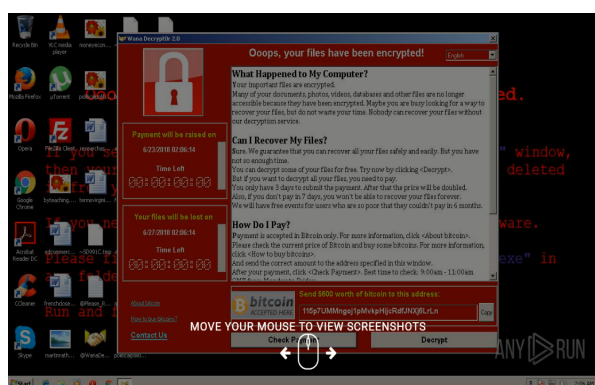
Table 1: File Hashes as of September 2022

MD5	SHA1
fb91e471cfa246beb9618e1689f1ae1d	a0ee0761602470e24bcea5f403e8d1e8bfa29832
	3122ea585623531df2e860e7d0df0f25cce39b21
	41dc0ba220f30c70aea019de214eccd650bc6f37
	c9c2b6a5b930392b98f132f5395d54947391cb79

- Herramientas, validar IOCs:
 - Virus Total, <https://www.virustotal.com/gui/home/upload>
 - Aliente Vault, <https://otx.alienvault.com/>
 - AbuseIPDB - IP Address Blacklist, <https://abuseipdb.com>

7.- Análisis de malware estático:

- Existe la necesidad de una vez obtenido el malware analizar y comprender cuales son sus objetivos una vez comprometida la víctima, si es un ransomware, troyano, keylogger, etc.
- Para ello, existen dos tipos de análisis de malware estático y dinámico.
- Para realizar análisis estático, vamos a usar un sandboxing en la nube:
- Anyrun, fuente: <https://any.run/>
- Analizar WannaCry
- SHA256:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- MD5: 84C82835A5D21BBCF75A61706D8AB549
- SHA1: 5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467
- Identificar:
 - Procesos
 - IOC
 - HTTP Request
 - Connections
 - DNS Request
 - Threats



Process information

PID	CMD	Path	Indicators	Parent process
2984	"C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set (default) bootstatuspolicy ignoreallfailures & bcdedit /set (default) recoveryenabled no & wbadm delete catalog -quiet	C:\Windows\System32\cmd.exe	🛡️	@WanaDecryptor@.exe
Information <ul style="list-style-type: none"> User: admin Company: Microsoft Corporation Integrity Level: HIGH Description: Windows Command Processor Exit code: 0 Version: 6.1.7601.17514 (win7sp1_rtm.101119-1850) 				
2824	vssadmin delete shadows /all /quiet	C:\Windows\system32\vssadmin.exe	-	cmd.exe
Information <ul style="list-style-type: none"> User: admin Company: Microsoft Corporation Integrity Level: HIGH Description: Command Line Interface for Microsoft® Volume Shadow Copy Service Exit code: 0 Version: 6.1.7600.16385 (win7_rtm.090713-1255) 				
2036	C:\Windows\system32\vssvc.exe	C:\Windows\system32\vssvc.exe	-	services.exe
Information <ul style="list-style-type: none"> User: SYSTEM Company: Microsoft Corporation Integrity Level: SYSTEM Description: Microsoft® Volume Shadow Copy Service Version: 6.1.7600.16385 (win7_rtm.090713-1255) 				
3000	wmic shadowcopy delete	C:\Windows\System32\Wbem\WMIC.exe	-	cmd.exe