



Network Security & Penetration testing



CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

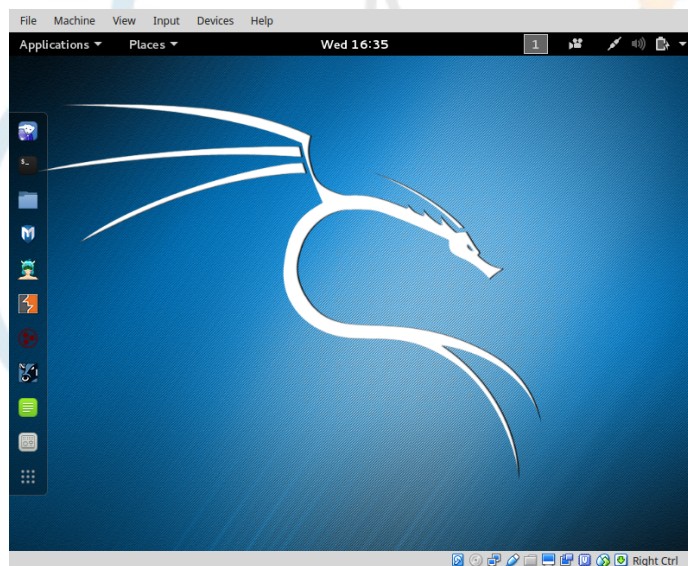
diarmuid@obriain.com



Kali Linux as a VM



- Using the Kali Linux image install VirtualBox, build the .ova image, install and run.
- Login to the image with the default root username (**root**) and password (**toor**).



<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

Kali Linux as a USB Drive



- <https://www.kali.org/downloads>
- Insert USB Drive and detect block device



```
ada:~$ lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
sdb	8:16	1	7.3G	0	disk	
└─sdb2	8:18	1	2.3M	0	part	
└─sdb1	8:17	1	685M	0	part	/media/ada/Ubuntu-Server 17.04 amd64
sr0	11:0	1	1024M	0	rom	
sda	8:0	0	931.5G	0	disk	
└─sda2	8:2	0	1K	0	part	
└─sda5	8:5	0	15.8G	0	part	[SWAP]
└─sda1	8:1	0	915.8G	0	part	/

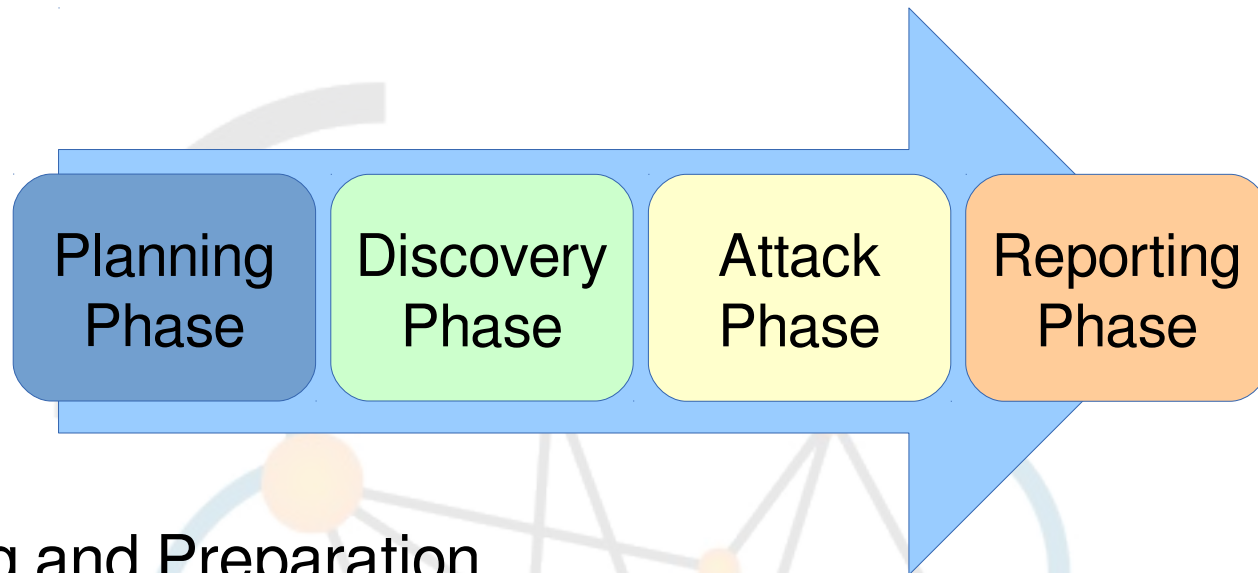
```
ada:~$ dd if=kali-linux-2017.2-amd64.iso | pv | sudo dd of=/dev/sdb bs=512k
[sudo] password for aloveface: babbage
5899648+0 records in0MiB/s] [ <=> ]
5899648+0 records out
3020619776 bytes (3.0 GB, 2.8 GiB) copied, 599.213 s, 5.0 MB/s
2.81GiB 0:09:59 [4.81MiB/s] [ <=> ]
0+40085 records in
0+40085 records out
3020619776 bytes (3.0 GB, 2.8 GiB) copied, 594.7 s, 5.1 MB/s
```

What is Penetration testing



- Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
 - Proactive
 - Authorised
 - Evaluation of IT infrastructure
 - Safely attempting to exploit system
 - Vulnerabilities
 - Improper configurations
 - Risky end-user behaviour.

What steps are used to carry out pen test



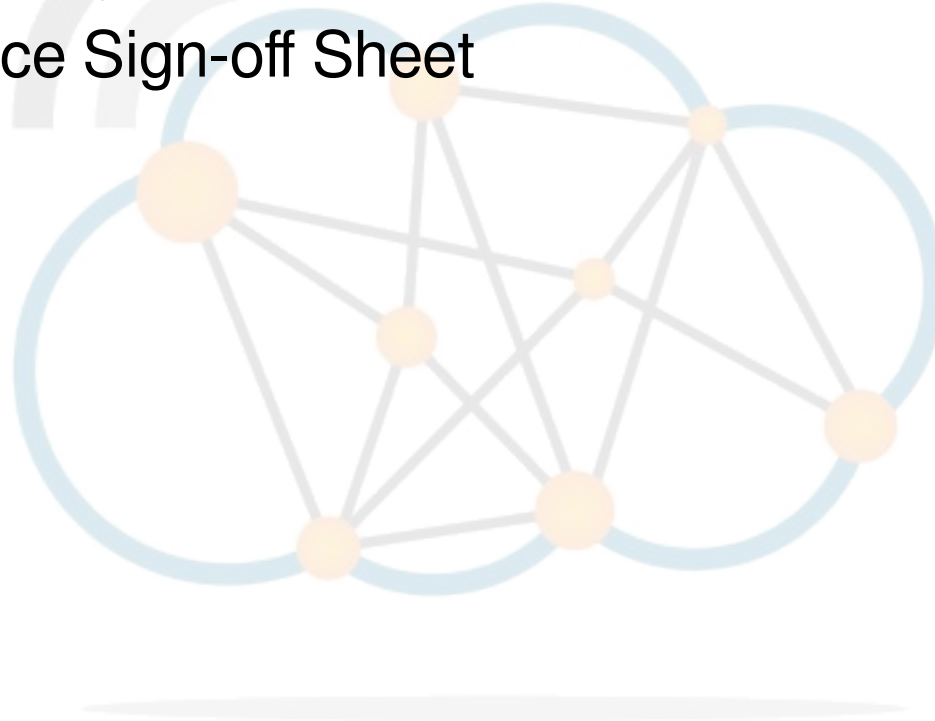
- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt
- Analysis and Reporting
- Cleaning up



- **Kick-off meeting**
 - Clear objective for pen-test
 - Timing and duration allowed for the pen-tests
 - Personnel involved
 - Are staff being informed of the tests?
 - Network and Computers involved
 - Operational requirements during the pen-test
 - How the results are to be presented at the conclusion of the test.



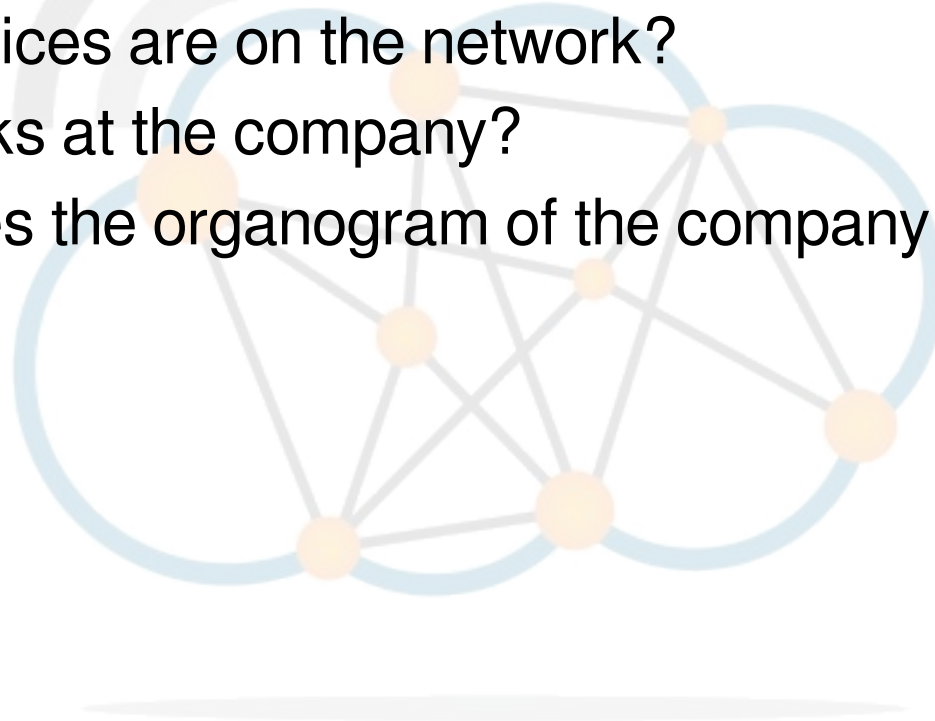
- **Penetration Test Plan**
 - Detailed plan
 - Confidentiality Statement
 - Acceptance Sign-off Sheet



Information gathering and analysis



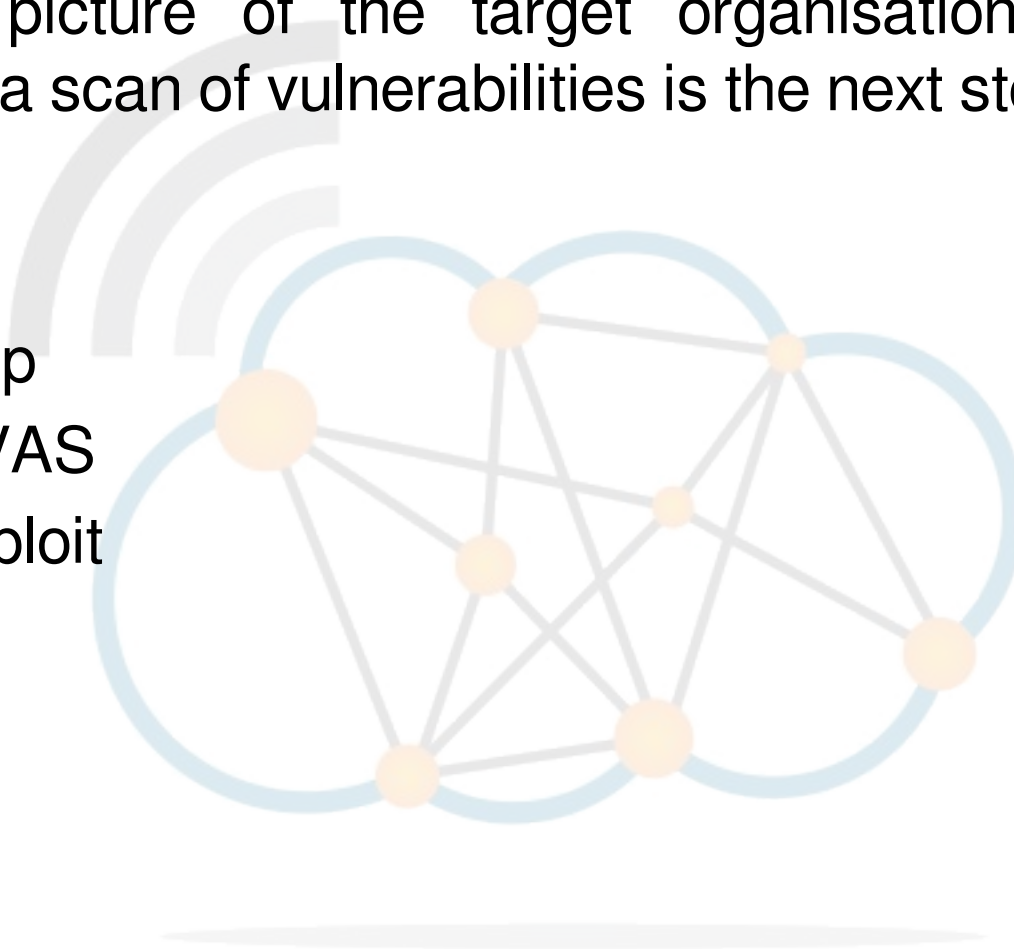
- Gathering of as much information as possible as a reconnaissance is essential.
 - What does the network look like?
 - What devices are on the network?
 - Who works at the company?
 - What does the organogram of the company look like?



Vulnerability detection



- Once a picture of the target organisation has been compiled a scan of vulnerabilities is the next step.
 - fierce
 - nmap
 - zenmap
 - OpenVAS
 - Metasploit



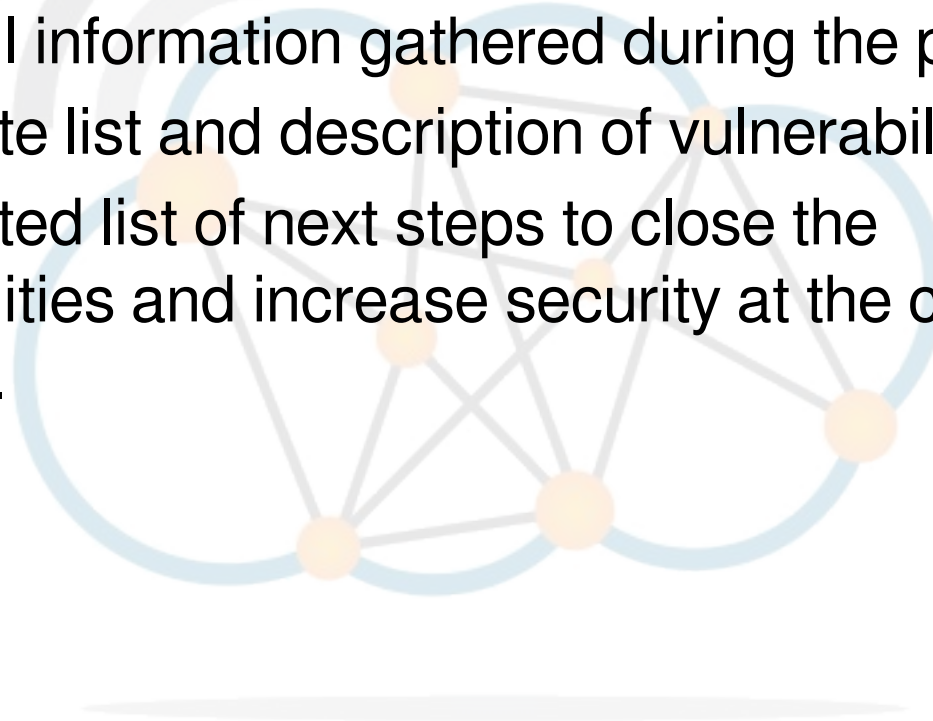
Penetration attempt



- Identifying the best targets from the machines showing vulnerability is important particularly if the time given is short.
- IT personnel nomenclature to use functional names like MAILSVR or FTPSERVER etc...
- Define the list of machines that are to be given special additional treatment.
- Try password cracking tools, dictionary, brute force and hybrid attacks.

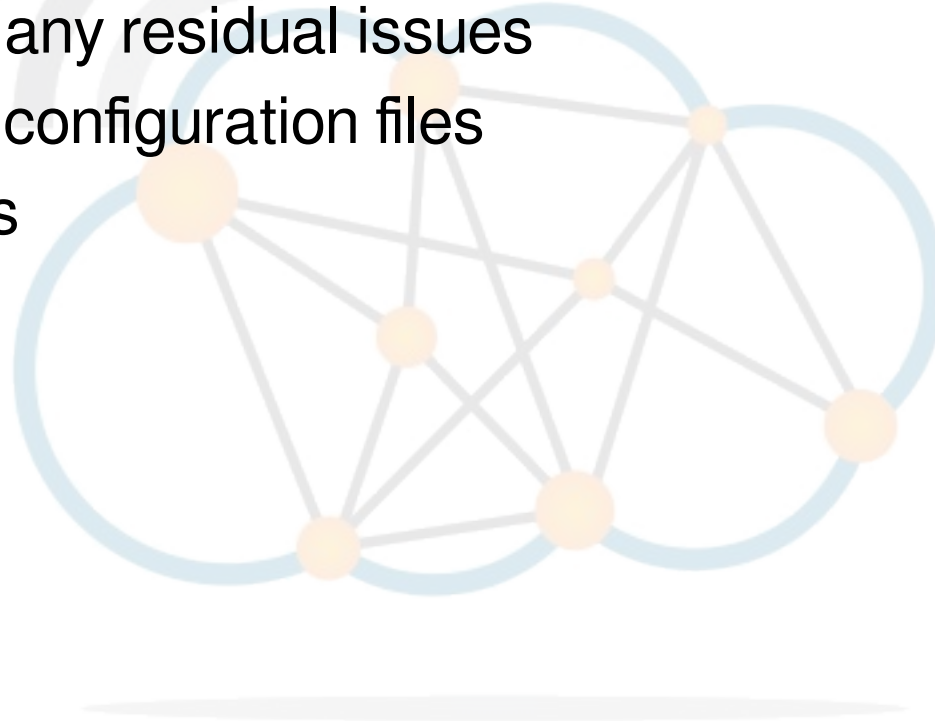


- A detailed report must be furnished to the client at the conclusion of the tests. It should include:
 - A summary of successful penetration tests.
 - A list of all information gathered during the pen-test.
 - A complete list and description of vulnerabilities found.
 - A suggested list of next steps to close the vulnerabilities and increase security at the client company.

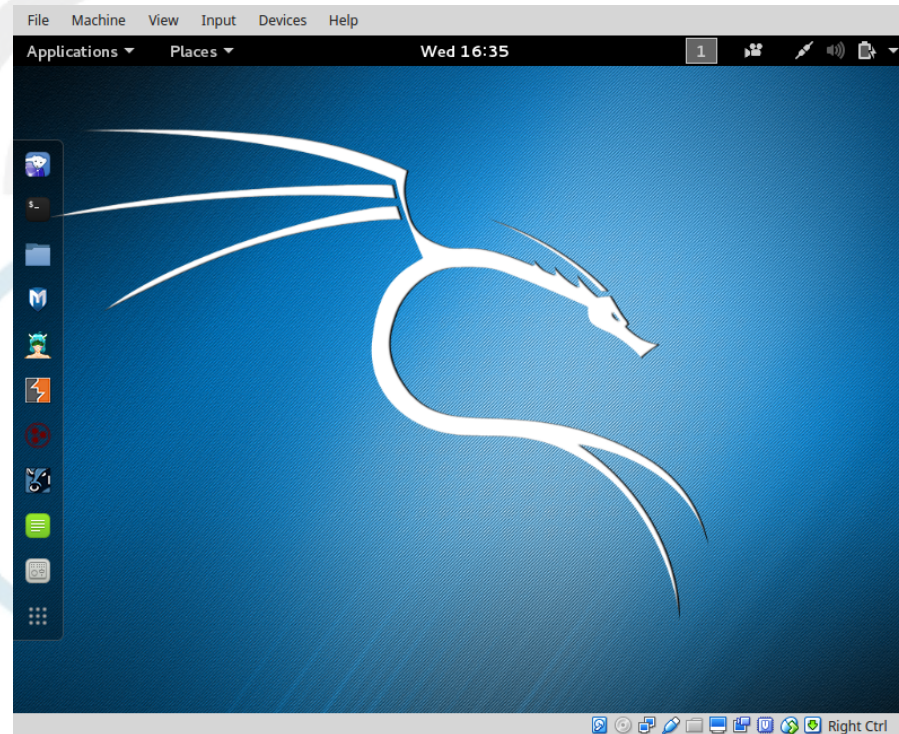




- During the pen-testing a detailed list of steps taken should be maintained.
- Pen-testers work with the client staff ensure that the steps have not left any residual issues
 - entries in configuration files
 - new users
 - groups
 - etc...



Kali Linux





- The GNU/Linux operating system includes a vast array of tools for each step of the pen-testing activity.
- All of the tools described here can be installed on any GNU/Linux distribution.
- Kali Linux is derived from Debian GNU/Linux is a distribution specifically designed for digital forensics and penetration testing.
- It is maintained and funded by Offensive Security Ltd.
- Comes pre-installed with over 600 penetration-testing programs.





- GNU/Linux distributions generally recommend the use of a non-privileged account while running the system and use a utility like ***sudo*** when and if escalation of privileges is required.
- Kali Linux is a security and auditing platform it contains tools that can only be ran under root privileges and therefore the root account is used.
- Care should be taken and is not the GNU/Linux distribution for Linux beginners.



Kali Linux – system update



```
root@kali:~# apt update
```

```
Get:1 http://security.kali.org sana/updates InRelease [11.9 kB]
```

```
Get:2 http://http.kali.org sana InRelease [20.3 kB]
```

```
Get:3 http://http.kali.org sana-proposed-updates InRelease [14.1 kB]
```

```
Get:4 http://security.kali.org sana/updates/main Sources [74.5 kB]
```

```
Get:5 http://http.kali.org sana/main Sources [9,089 kB]
```

```
Ign http://security.kali.org sana/updates/contrib Translation-en_US
```

```
. . . . .
```

```
. . . . .
```

```
Ign http://http.kali.org sana-proposed-updates/non-free Translation-en
```

```
Fetched 22.7 MB in 1min 41s (222 kB/s)
```

```
Reading package lists... Done
```

```
root@kali:~# apt dist-upgrade
```



KALI™

Information Gathering and Analysis



- fierce
- nmap
- zenmap





- Lightweight scanner that helps locate non-contiguous IP space and host-names against specified domains.
- It is used as a pre-cursor to ***nmap*** as it requires knowledge of the IP already. It locates likely targets both inside and outside a corporate network.
- Because it uses DNS primarily you will often find miss-configured networks that leak internal address space.
- That's especially useful in targeted malware.



```
root@kali:~# fierce -dns adomain.com
```

```
DNS Servers for adomain.com:
```

```
ns2.adomain.com
```

```
ns1.adomain.com
```

```
Trying zone transfer first...
```

```
Testing ns2.adomain.com
```

```
Request timed out or transfer not allowed.
```

```
Testing ns1.adomain.com
```

```
Request timed out or transfer not allowed.
```

```
Unsuccessful in zone transfer (it was worth a shot)
```

```
Okay, trying the good old fashioned way... brute force
```

```
Checking for wildcard DNS...
```

```
** Found 97919448768.adomain.com at 68.95.161.145.
```

```
** High probability of wildcard DNS.
```

```
Now performing 2280 test(s)...
```

```
68.95.161.6      unix.adomain.com
```

```
68.95.161.93    mx.adomain.com
```

```
68.95.161.92    mx.adomain.com
```

```
68.95.161.237   www.adomain.com
```

```
Subnets found (may want to probe here using nmap or unicornscan):
```

```
68.95.161.0-255 : 4 hostnames found.
```

```
176.58.111.0-255 : 1 hostnames found.
```

```
Done with Fierce scan: http://ha.ckers.org/fierce/
```

```
Found 4 entries.
```

```
Have a nice day.
```



- Network Mapper (nmap) is an open source tool for network exploration and security auditing.
- It forms the basis for most of the other tools that are used for penetration testing and scanning.

```
cedat:~$ sudo apt install nmap zenmap xprobe
```



```
root@kali:~# nmap -Pn 192.168.89.1 | tee /tmp/nmap-output.txt
```

Starting Nmap 6.40 (<http://nmap.org>) at 2015-11-03 11:41 EAT

Nmap scan report for 192.168.89.1

Host is up (0.00086s latency).

Not shown: 65530 closed ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

23/tcp	open	telnet
--------	------	--------

80/tcp	open	http
--------	------	------

2000/tcp	open	cisco-sccp
----------	------	------------

8291/tcp	open	unknown
----------	------	---------

Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds

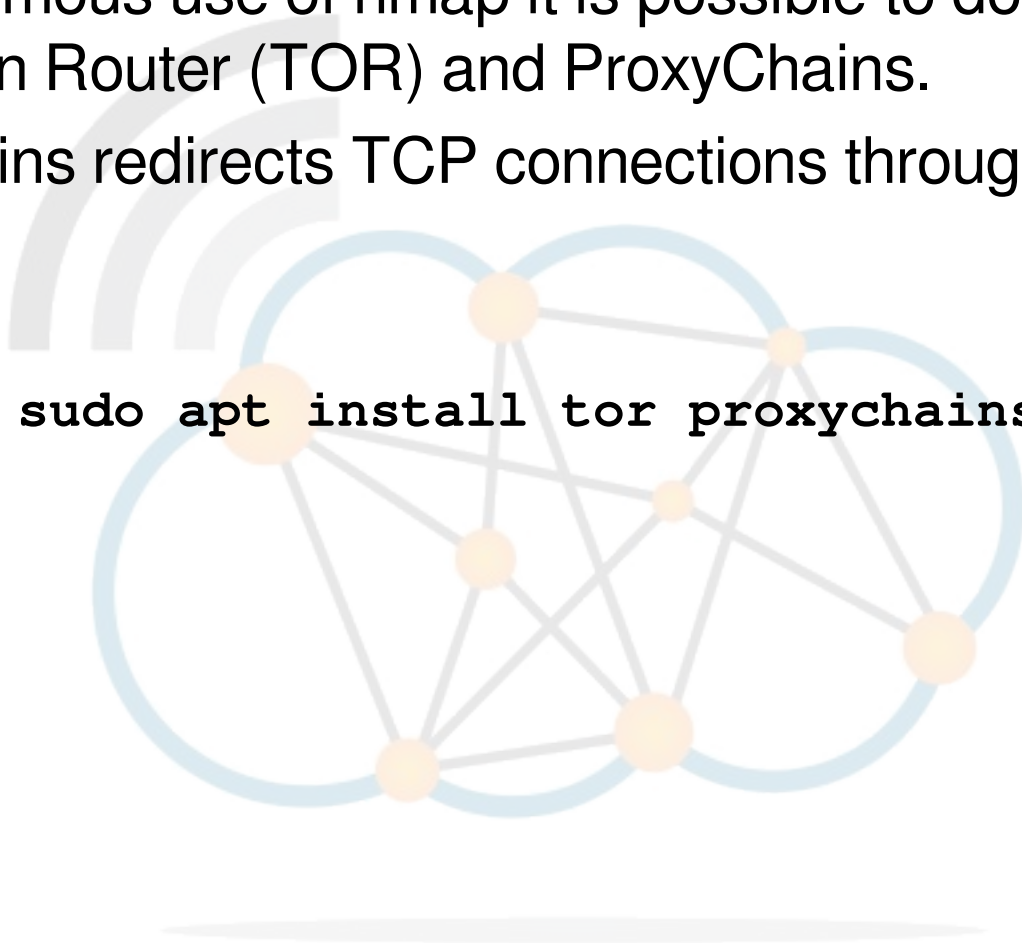
-Pn: Treat all hosts as being online, skip host discovery.

Anonymous use of nmap



- For anonymous use of nmap it is possible to do so using 'The Onion Router (TOR) and ProxyChains.
- ProxyChains redirects TCP connections through proxy servers.

```
cedat : ~$ sudo apt install tor proxychains
```



Anonymous use of nmap

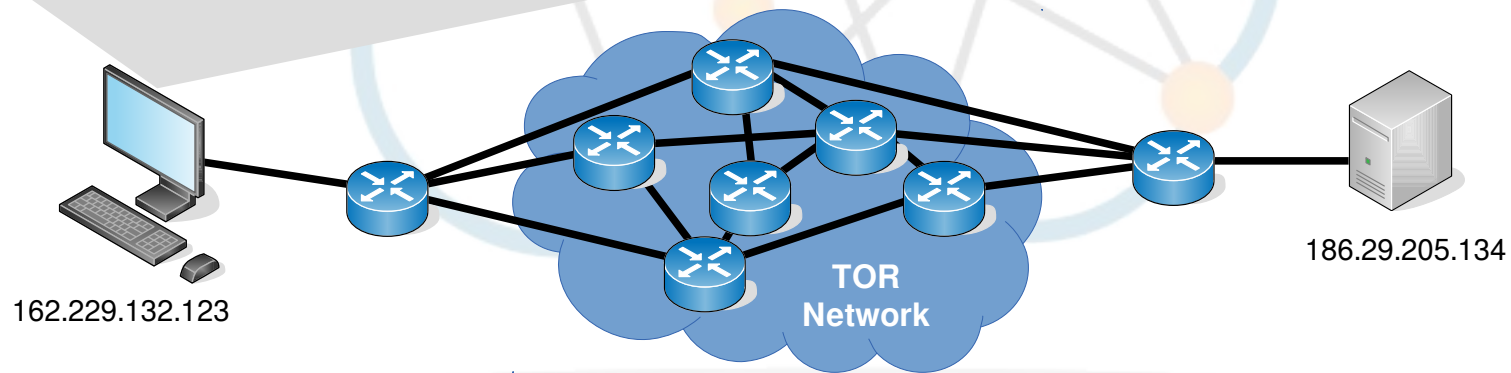


```
cedat:~$ proxychains nmap -Pn -sT -p 22,80 186.29.205.134
ProxyChains-3.1 (http://proxychains.sf.net)
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-04 22:07 EAT
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
Nmap scan report for li489-237.members.linode.com (186.29.205.134)
Host is up (0.61s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

-sT:

TCP connect scan via the OS
own Berkeley Socket API.



Anonymous use of nmap

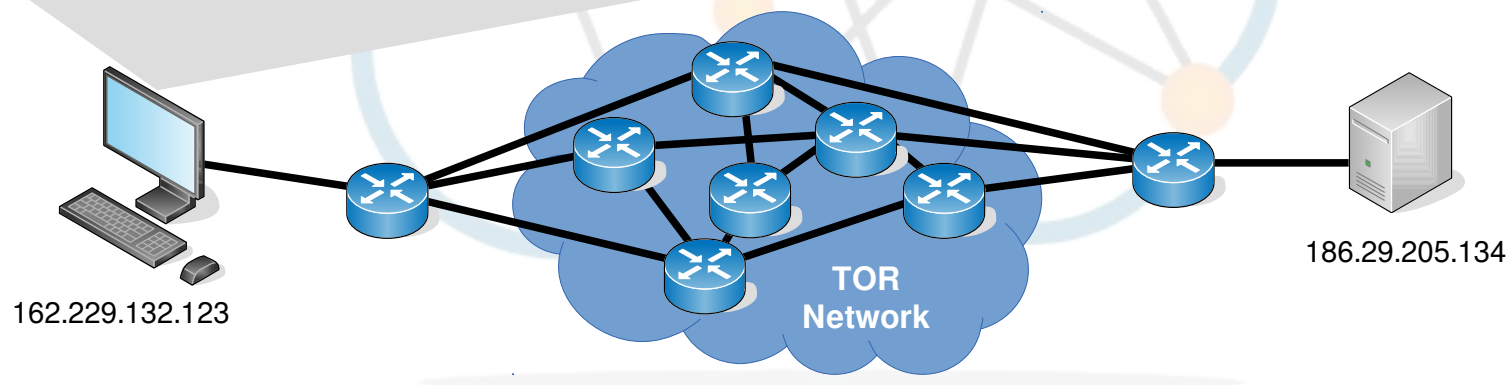


```
cedat:~$ proxychains nmap -Pn -sV -sT -p 22,80 186.29.205.134  
ProxyChains-3.1 (http://proxychains.sf.net)
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-04 22:07 EAT  
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK  
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK  
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK  
Nmap scan report for li489-237.members.linode.com (186.29.205.134)  
Host is up (0.61s latency).  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http
```

-sV:

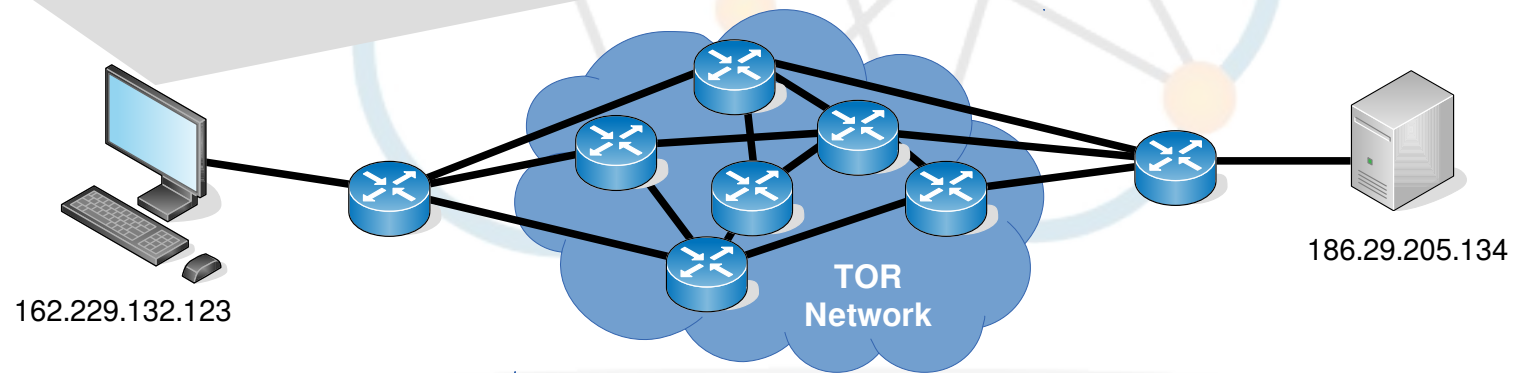
Enable version detection.
It can be used to help
differentiate the truly open
ports from the filtered
ones.



Anonymous use of nmap



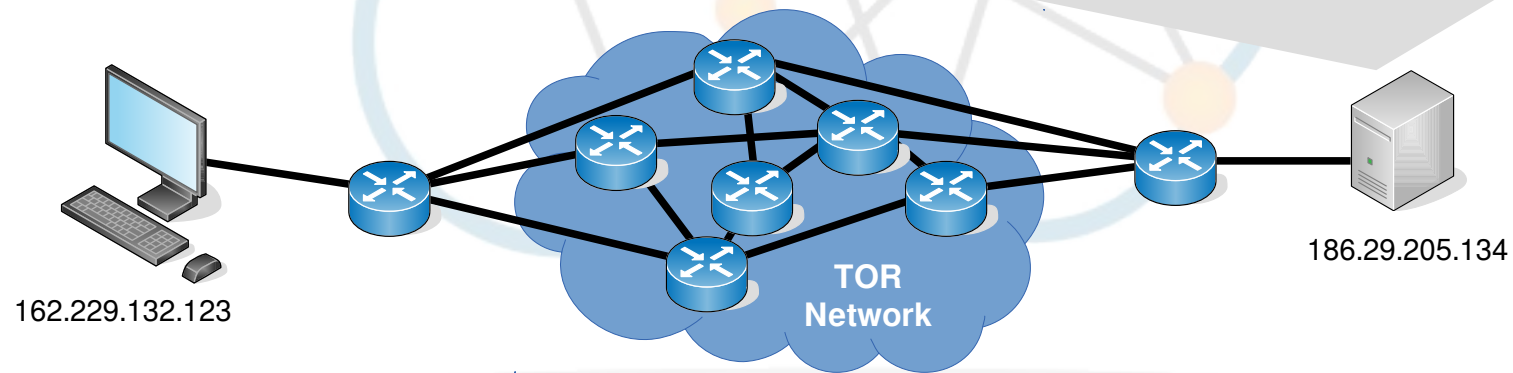
```
cedat:~$ proxychains ssh root@186.29.205.134
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9050-<>-186.29.205.134:22-<>-OK
root@186.29.205.134's password:
Permission denied, please try again.
root@186.29.205.134's password:
Permission denied, please try again.
root@186.29.205.134's password:
Permission denied (publickey,password).
```



Anonymous use of nmap



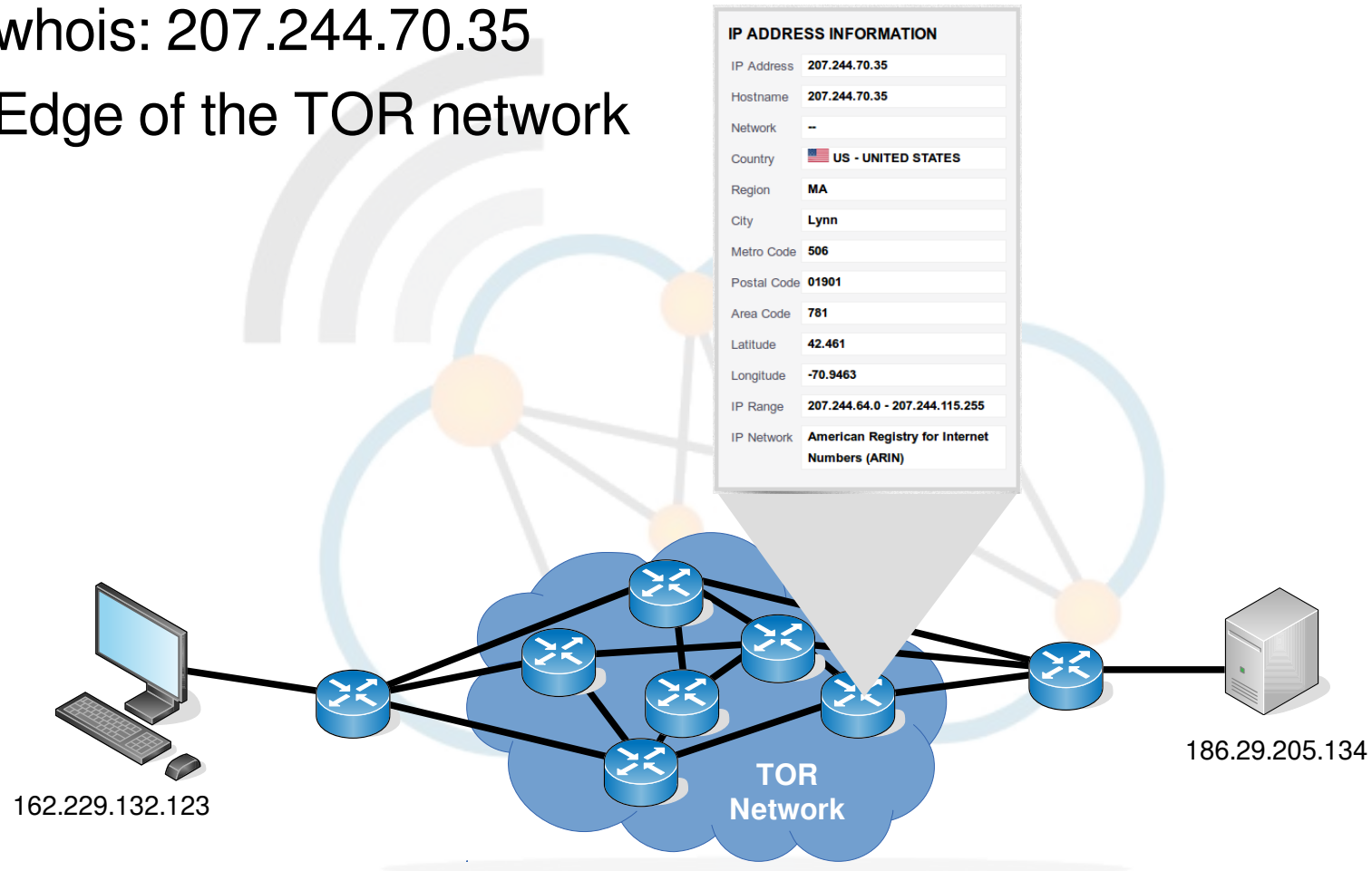
```
root@server:~# tail /var/log/auth.log
Nov  4 19:09:26 www sshd[1146]: Failed password for root from
207.244.70.35 port 45909 ssh2
Nov  4 19:09:33 www sshd[1146]: Failed password for root from
207.244.70.35 port 45909 ssh2
Nov  4 19:09:40 www sshd[1146]: Failed password for root from
207.244.70.35 port 45909 ssh2
Nov  4 19:09:40 www sshd[1146]: Connection closed by
207.244.70.35 [preauth]
Nov  4 19:09:40 www sshd[1146]: PAM 2 more authentication
failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=207.244.70.35  user=root
```



Anonymous use of nmap



- whois: 207.244.70.35
- Edge of the TOR network



Public key, possible Identifier



- Public key possible Identifier if traffic is being monitored in TOR.
- Generate new key for use over TOR.

```
cedat:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ece/.ssh/id_rsa): id_rsa_ANONY
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa_ANONY.
Your public key has been saved in id_rsa_ANONY.pub.
The key fingerprint is:
bc:34:b1:23:fd:5a:f2:4b:d9:88:af:70:f7:d6:39:a2
The key's randomart image is:
+--[ RSA 2048 ]-----+
|      .               |
|      o o             |
|      . S             |
|      o * +           |
|      . = B .. .      |
|      o O .o +        |
|      o.E+.. .        |
+-----+

```

Anonymous use of nmap



```
cedat:~$ proxychains ssh -i /home/ece/.ssh/id_rsa_ANONY root@186.29.205.134
```

```
ProxyChains-3.1 (http://proxychains.sf.net)
```

```
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
```

```
root@176.58.111.237's password: BADPASS
```

```
Permission denied, please try again.
```

```
root@176.58.111.237's password: GOODPASS
```

```
Linux www 4.1.5-x86_64-linode61 #7 SMP Mon Aug 24 13:46:31 EDT 2015 x86_64
```

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

```
Last login: Mon Nov 9 03:20:34 2015 from 160.242.131.178
```

Anonymous use of nmap




```
root@ece:~# tail /var/log/auth.log
```


```
Nov 10 09:46:10 ece sshd[21706]: Failed password for root from 43.229.53.25  
port 11978 ssh2
```

```
Nov 10 09:46:12 ece sshd[21706]: Failed password for root from 43.229.53.25  
port 11978 ssh2
```

```
Nov 10 09:46:12 ece sshd[21706]: Received disconnect from 43.229.53.25: 11:  
[preauth]
```

```
Nov 10 09:46:12 ece sshd[21706]: PAM 2 more authentication failures;  
logname= uid=0 euid=0 tty=ssh ruser= rhost=43.229.53.25 user=root
```

IP ADDRESS INFORMATION	
IP Address	43.229.53.25
Hostname	43.229.53.25
Network	Asia Pacific Network Information Centre
Country	 JP - JAPAN
Latitude	36
Longitude	138
IP Range	43.0.0.0 - 43.233.35.255
IP Network	American Registry for Internet Numbers (ARIN)

IP ADDRESS INFORMATION	
IP Address	81.7.15.115
Hostname	81-7-15-115.blue.kundencontroller.de
Network	RIPE Network Coordination Centre
Country	 DE - GERMANY
Latitude	51
Longitude	9
IP Range	81.7.0.0 - 81.7.63.255
IP Network	American Registry for Internet Numbers (ARIN)

Zenmap



Scan Tools Profile Help

Target: 192.168.89.1 Profile: Intense scan Scan Cancel

Command: nmap-T4 -A -v 192.168.89.1

Hosts Services

OS	Host
	192.168.89.1

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

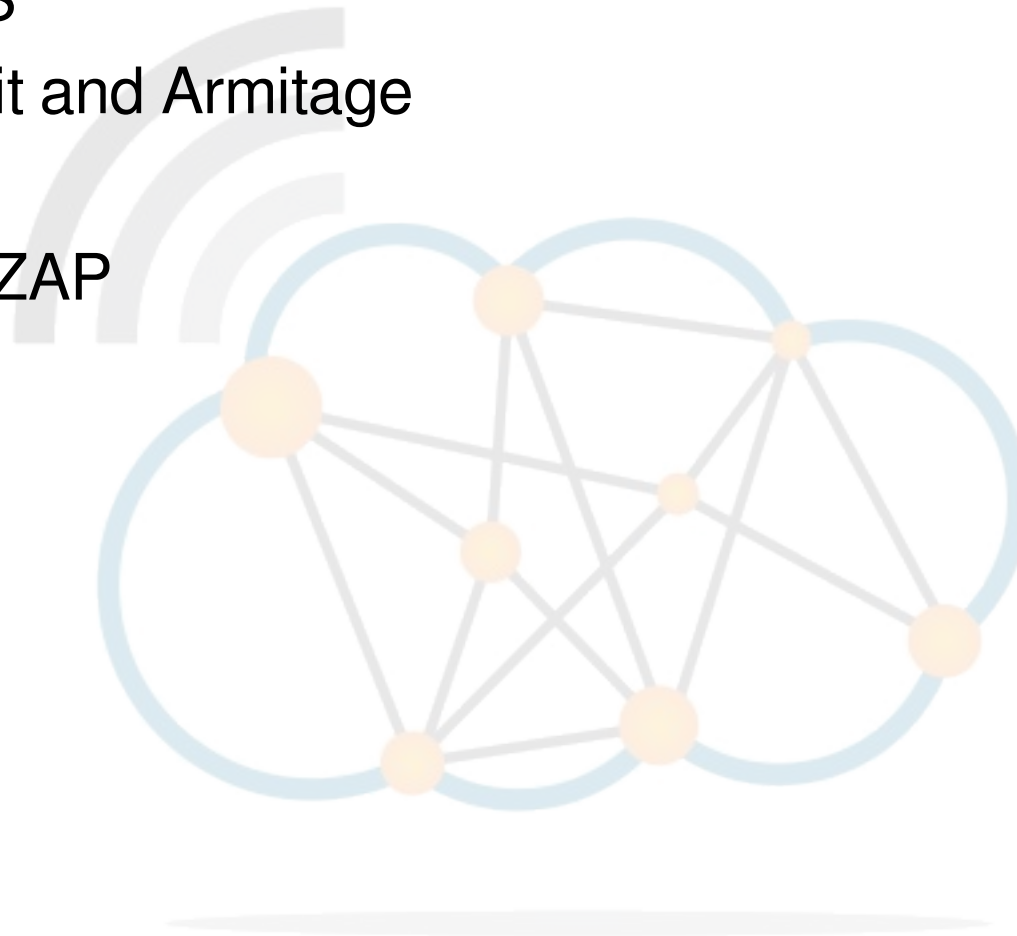
nmap-T4 -A -v 192.168.89.1 Details

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-03 11:48
EAT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 11:48
Scanning 192.168.89.1 [1 port]
Completed ARP Ping Scan at 11:48, 0.22s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 11:48
Completed Parallel DNS resolution of 1 host. at 11:48,
0.00s elapsed
Initiating SYN Stealth Scan at 11:48
Scanning 192.168.89.1 [1000 ports]
Discovered open port 80/tcp on 192.168.89.1
Discovered open port 22/tcp on 192.168.89.1
Discovered open port 21/tcp on 192.168.89.1
Discovered open port 23/tcp on 192.168.89.1
Discovered open port 2000/tcp on 192.168.89.1
Discovered open port 8291/tcp on 192.168.89.1
Completed SYN Stealth Scan at 11:48, 1.42s elapsed (1000
total ports)
Initiating Service scan at 11:48
Scanning 6 services on 192.168.89.1
Completed Service scan at 11:50, 131.10s elapsed (6
services on 1 host)
Initiating OS detection (try #1) against 192.168.89.1
NSE: Script scanning 192.168.89.1.
Initiating NSE at 11:50
```

Vulnerability detection and penetration



- OpenVAS
- Metasploit and Armitage
- Nikto
- OWASP ZAP





- GNU General Public License (GNU GPL) framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.
- The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.

OpenVAS setup



- Install OpenVAS 9 on kali Linux

```
root@kali:/# apt update; apt install openvas  
root@kali:/# openvas-setup
```

- OpenVAS User

```
root@kali:/# openvasmd --create-user=MyOpenVASuser  
--role=Admin
```

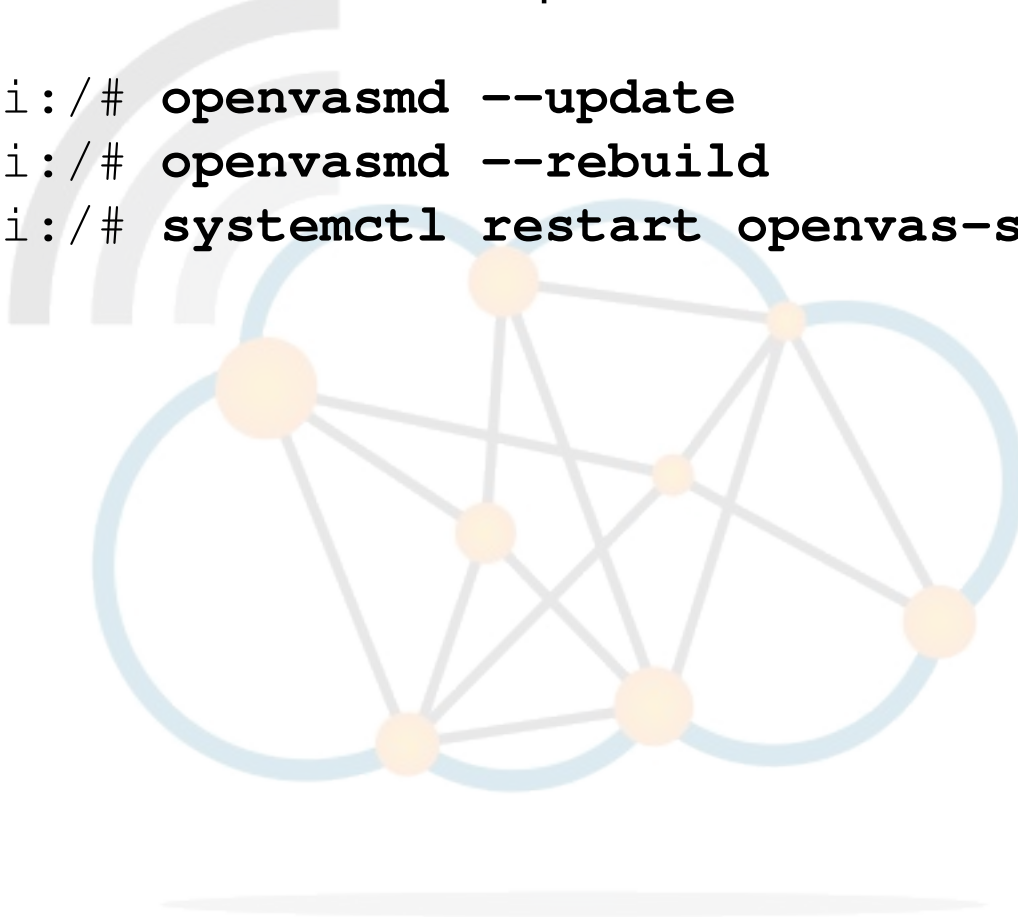
```
root@kali:/# openvasmd --user=MyOpenVASuser --new-  
password=MyOpenVAspass
```

OpenVAS update NVTs



- Update the NVT database, this step should be carried out regularly.

```
root@kali:/# openvasmd --update  
root@kali:/# openvasmd --rebuild  
root@kali:/# systemctl restart openvas-scanner
```



OpenVAS Greenbone Assistant Access



- By default it is only possible to access the greenbone assistant from the localhost. To allow access from other hosts.

```
root@kali:/# sed -i.bak -e 's/--listen=127.0.0.1/--  
listen=0.0.0.0/' /lib/systemd/system/greenbone-  
security-assistant.service
```

```
root@kali:/# systemctl daemon-reload  
root@kali:/# systemctl restart greenbone-security-  
assistant
```

OpenVAS Greenbone Assistant Access



- The OpenVAS installation can be checked and any problems fixed. When all is OK it should give an OK message.

```
root@kali:/# openvas-check-setup
```

```
It seems like your OpenVAS-9 installation is OK.
```

- Start the OpenVAS Server

```
root@kali:/# openvas-start
```

```
Starting OpenVas Services
```

Check OpenVAS Services are running



- At this stage the OpenVAS manager, scanner, and Greenbone Security Assistant (GSAD) services should be listening:

```
root@kali:/# netstat -antp
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address
-------	--------	--------	---------------	-----------------

State	PID/Program name
-------	------------------

tcp	0	0	127.0.0.1:9390	0.0.0.0:*	LISTEN	2745/openvasmd
tcp	0	0	127.0.0.1:80	0.0.0.0:*	LISTEN	4421/gsad
tcp	0	0	127.0.0.1:9392	0.0.0.0:*	LISTEN	4420/gsad


OpenVAS Webclient - <https://127.0.0.1:9392>



<https://127.0.0.1:9392>

or

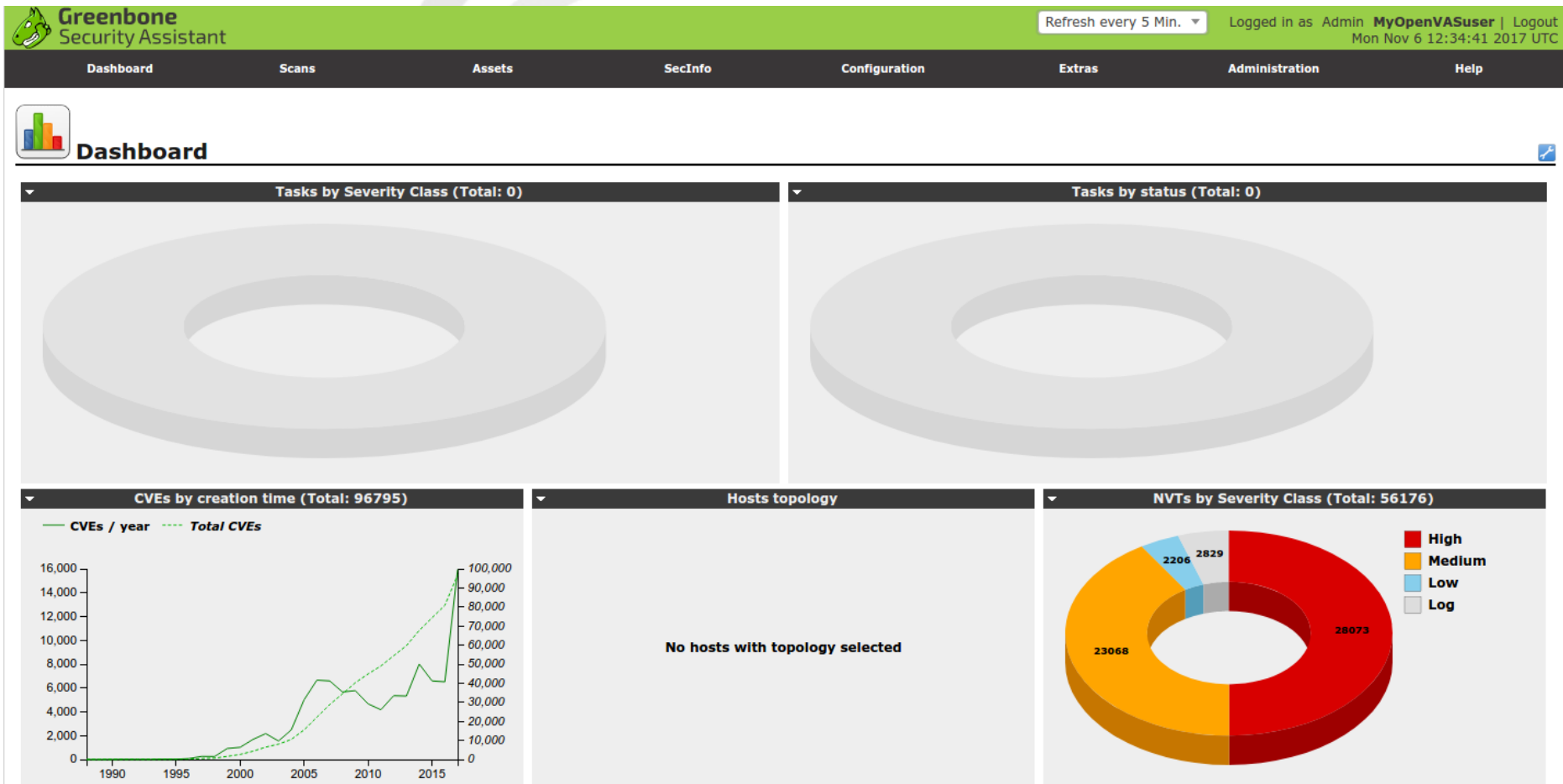
<https://<ip address of server>:9392>



Username:

Password:

Login




OpenVAS Webclient - Scans >> Tasks



Task Wizard

Task Wizard



- 1.
- 2.
- 3.
- 4.

Quick start: Immediately scan an IP address


IP address or hostname:

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

- Create a new Target
- Create a new Task
- Start this scan task right away
- Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

Start Scan

OpenVAS Webclient - Scans >> Reports



Dashboard

Scans

Assets

SecInfo

Configuration

Extras

Administration

Help



? Anonymous X...      **Stopped at 1 %**

Filter:

autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

ID: 12b4b230-17dd-4ab2-b71c-3ea5b252e525
Modified:
Created: Mon Nov 6 12:47:41 2017
Owner: MyOpenVASuser


Report: Results (1 of 3)

Vulnerability	Severity	QoD	Host	Location	Actions
TCP timestamps	2.6 (Low)	80%	192.168.89.2	general/tcp	 

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

OpenVAS Webclient – Detailed reports








**Greenbone**
Security Assistant

No auto-refresh


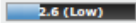



Logged In as Admin **MyOpenVASuser** | Logout
Mon Nov 6 13:17:44 2017 UTC

DashboardScansAssetsSecInfoConfigurationExtrasAdministrationHelp



**Result: TCP timestamps**

ID: f2900a4c-7738-4421-8079-1db51df8cf1c
Created: Mon Nov 6 12:57:51 2017
Modified: Mon Nov 6 12:57:51 2017
Owner: MyOpenVASuser

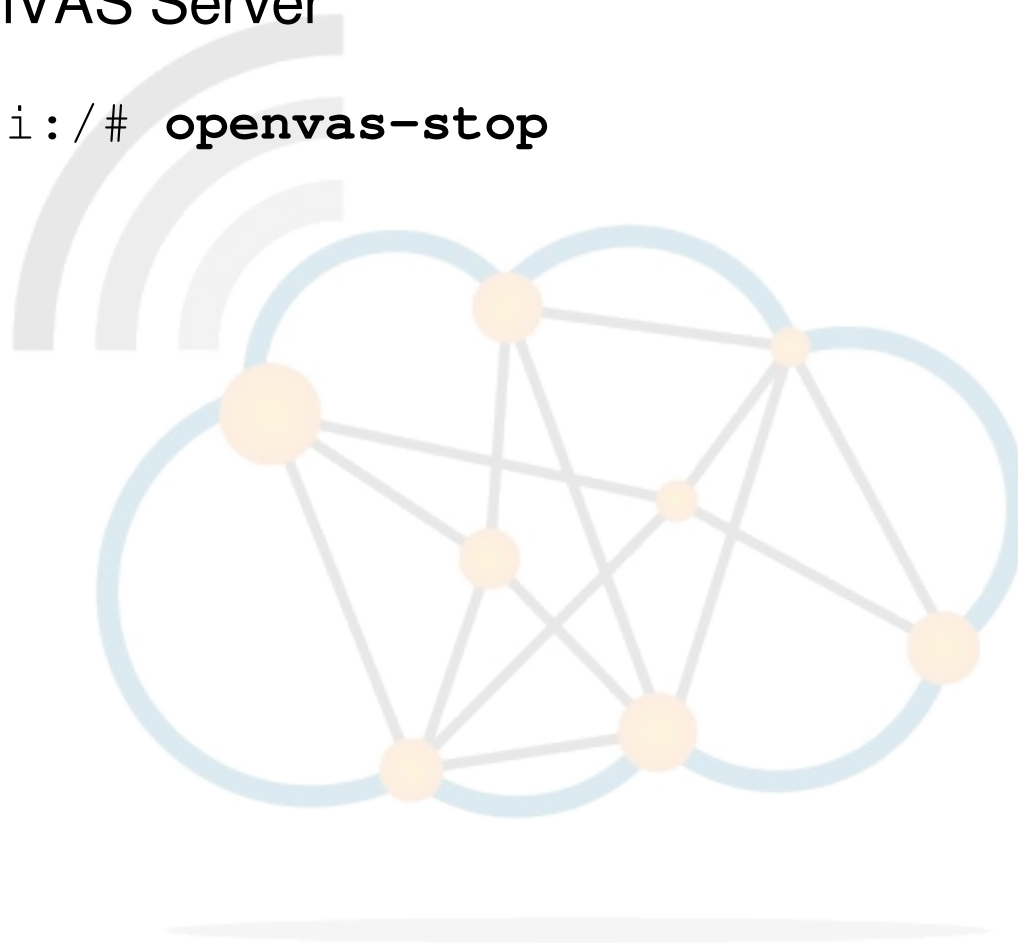
Vulnerability		Severity	QoD	Host	Location	Actions
TCP timestamps			80%	192.168.89.2	general/tcp	 
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.						
Vulnerability Detection Result It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 7643302 Packet 2: 7643557						
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.						
Solution Solution type:  Mitigation To disable TCP timestamps on Linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when Initiating TCP connections, but use them if the TCP peer that is Initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152						
Affected Software/OS TCP/IPv4 Implementations that implement RFC1323.						
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323.						
Vulnerability Detection Method Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: \$Revision: 7277 \$						
References Other: http://www.ietf.org/rfc/rfc1323.txt						

OpenVAS stop



- Stop OpenVAS Server

```
root@kali:/# openvas-stop
```





- Penetration testing framework from Rapid7 that enables the finding, exploitation, and validation vulnerabilities.

Starting Metasploit



- Start the Postgresql database Server

```
root@kali:/# service postgresql start
```

- Initial configuration of the database

```
root@kali:/# msfdb init
```

- Update the database regularly

```
root@kali:/# apt update; apt install metasploit-  
framework
```

Metasploit MSF console



```
root@kali:~# msfconsole
```

```
[*] Starting the Metasploit Framework Console ....
```

```
  /      \
 /        \
(( _ _ _ , , _ _ ))
  ( _ ) O O ( _ )
    \ _ /
    o_o \   M S F
         \   | \
         \   |  *
         |||  WW|||
         |||  |||
```

```
=[ metasploit v4.16.14-dev ]
+ -- --=[ 1699 exploits - 969 auxiliary - 299 post ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf >
```

Metasploit load modules



```
root@kali:~# load openvas
```

```
[*] Welcome to OpenVAS integration by kost and averagesecurityguy.  
[*]  
[*] OpenVAS integration requires a database connection. Once the  
[*] database is ready, connect to the OpenVAS server using openvas_connect.  
[*] For additional commands use openvas_help.  
[*]  
[*] Successfully loaded plugin: OpenVAS
```

```
msf > openvas_help
```

```
[*] openvas_help          Display this help  
[*] openvas_debug        Enable/Disable debugging  
[*] openvas_version      Display the version of the OpenVAS server  
[*]  
[*] CONNECTION  
[*] =====  
[*] openvas_connect       Connects to OpenVAS  
[*] openvas_disconnect    Disconnects from OpenVAS  
[*]  
[*] TARGETS  
[*] =====  
[*] openvas_target_create Create target  
[*] openvas_target_delete Deletes target specified by ID  
[*] openvas_target_list   Lists targets  
[*]
```

Armitage



- Graphical cyber attack management tool for the Metasploit Framework that visualises targets and recommends exploits.
- Through Armitage, a user may launch scans and exploits, get exploit recommendations, and use the advanced features of the Metasploit Framework.



ARMITAGE

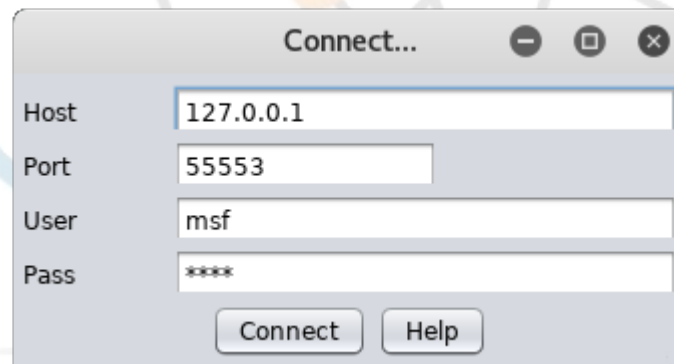


- Start Postgresql Database Server

```
root@kali:/# systemctl start postgresql
```

- Start Armitage

```
root@kali:/# armitage
```

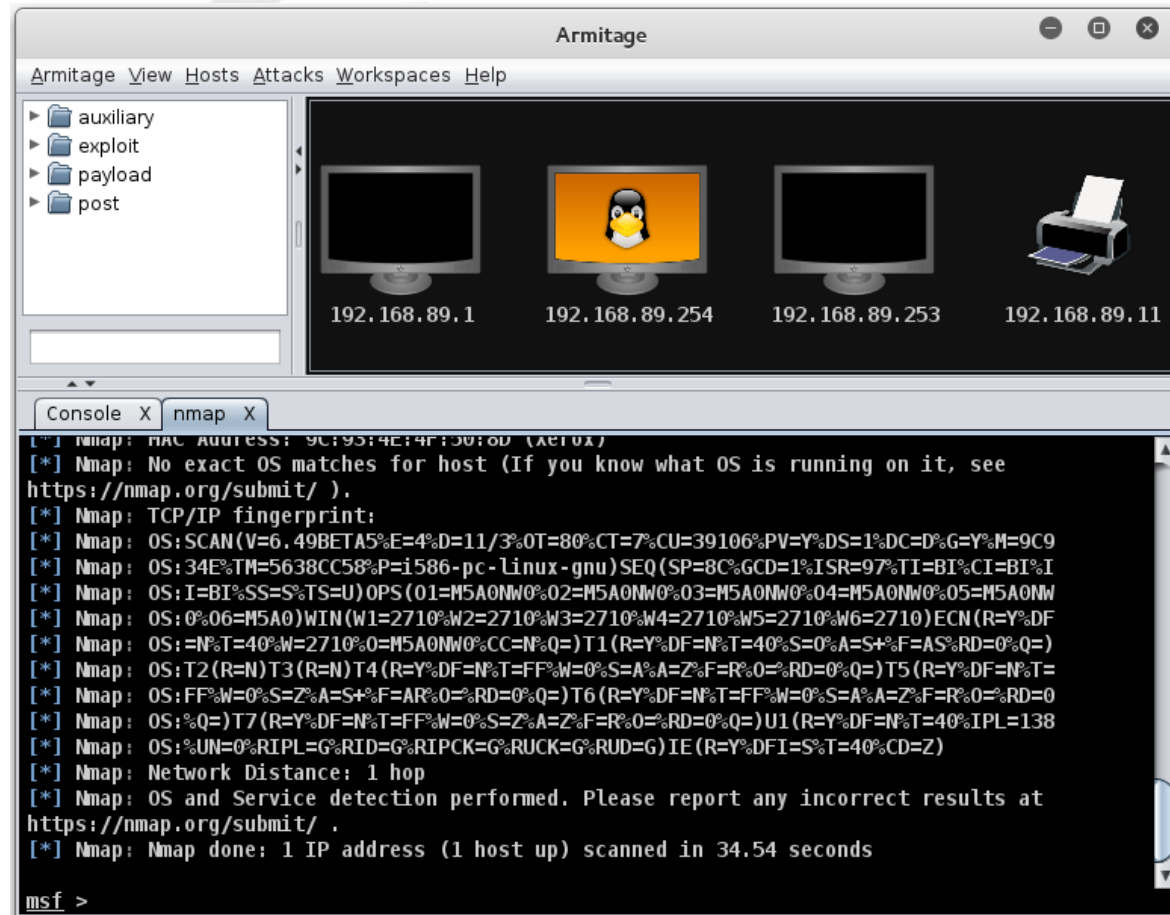


A screenshot of the 'Connect...' dialog box in the Armitage application. The dialog has a title bar with standard window controls. It contains four input fields: 'Host' with the value '127.0.0.1', 'Port' with '55553', 'User' with 'msf', and 'Pass' with masked characters '****'. At the bottom, there are two buttons: 'Connect' and 'Help'.

Field	Value
Host	127.0.0.1
Port	55553
User	msf
Pass	****



Hosts → nmap Scan → Quick Scan (OS Detect)



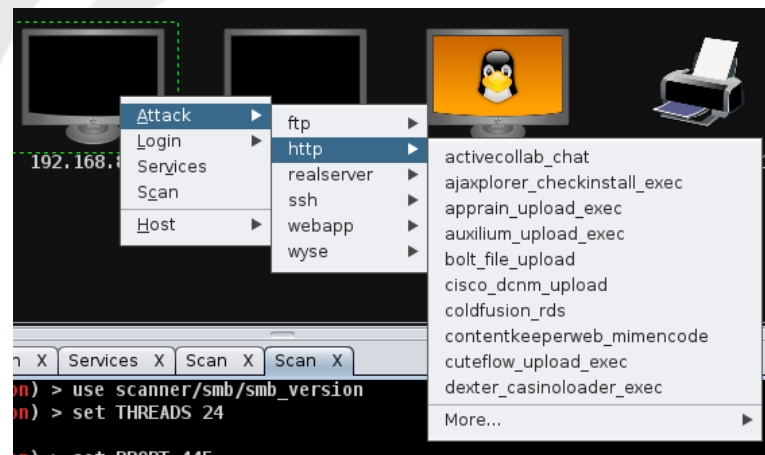
Armitage - Scanning



Armitage - Attack vectors



Attacks → Find Attacks



Armitage – Making an attack



Attack 192.168.89.1

GestioliP Remote Command Execution

This module exploits a command injection flaw to create a shell script on the filesystem and execute it. If GestioliP is configured to use no authentication, no password is required to exploit the vulnerability. Otherwise, an authenticated user is required to exploit.

Option	Value
LHOST	192.168.89.252
LPORT	8578
PASSWORD +	
Proxies	
RHOST +	192.168.89.1
RPORT	80
TARGETURI	/gestioip/
USERNAME +	gipadmin
VHOST	

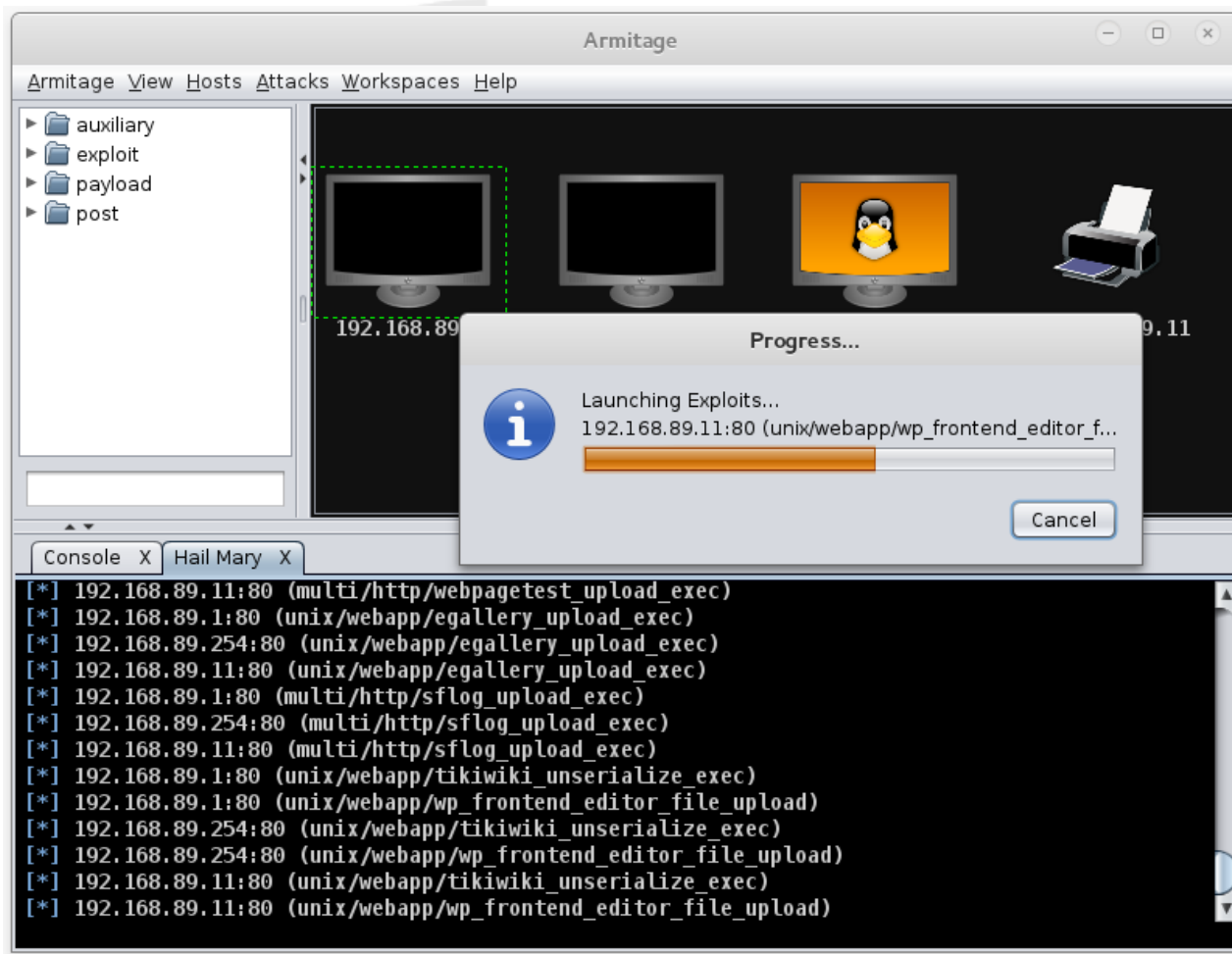
Targets: 0 => Automatic GestioliP 3.0

☐ Use a reverse connection

☐ Show advanced options

Launch

Armitage – 'Hail Mary' attack



Armitage - Reporting



View → Reporting

host	port	state	proto	name	created_at	updated_at	info
192.168.89.1	21		tcp	ftp		1446562557662	220 MikroTik FTP server (MikroTik 6.0rc13) ready\r\n0d\r\n0a
192.168.89.1	22		tcp	ssh		1446562560331	SSH-2.0-ROSSH
192.168.89.1	23		tcp	telnet		1446562606093	MikroTik v6.0rc13\r\n0aLogin:
192.168.89.1	80		tcp	http		1446562306810	
192.168.89.1	2000		tcp	bandwidth-test		1446562306824	MikroTik bandwidth-test server
192.168.89.254	22		tcp	ssh		1446562372449	SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
192.168.89.254	80		tcp	http		1446562369503	Apache/2.4.7 (Ubuntu)
192.168.89.254	139		tcp	netbios-ssn		1446562306916	Samba smbd 3.X workgroup: DOBRIAIN-THINKPAD-E550
192.168.89.254	445		tcp	smb		1446562375424	Unix (Samba 4.1.6-Ubuntu)
192.168.89.11	80		tcp	http		1446563548065	HTTP server (302-http://192.168.89.11/index.asp)
192.168.89.11	515		tcp	printer		1446562904812	
192.168.89.11	631		tcp	ipp		1446562904836	
192.168.89.11	9100		tcp	jetdirect		1446562904854	



- Shell utility to scan web servers for known vulnerabilities.
- Update Nikto.

```
root@kali:~# nikto -update  
+ Retrieving 'db_tests'  
+ Retrieving 'db_variables'  
+ Retrieving 'db_tests'  
+ Retrieving 'db_outdated'  
+ Retrieving 'db_server_msgs'  
+ Retrieving 'nikto_robots.plugin'  
+ Retrieving 'nikto_cookies.plugin'  
+ Retrieving 'db_favicon'  
+ Retrieving 'CHANGES.txt'
```


Running Nikto



```
root@kali:~# nikto -host 192.168.89.1
```

```
- Nikto v2.1.4
```

```
-----  
+ Target IP: 192.168.89.1
```

```
+ Target Hostname: 192.168.89.1
```

```
+ Target Port: 80
```

```
+ Start Time: 2015-10-29 22:55:58  
-----
```

```
+ Server: No banner retrieved
```

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

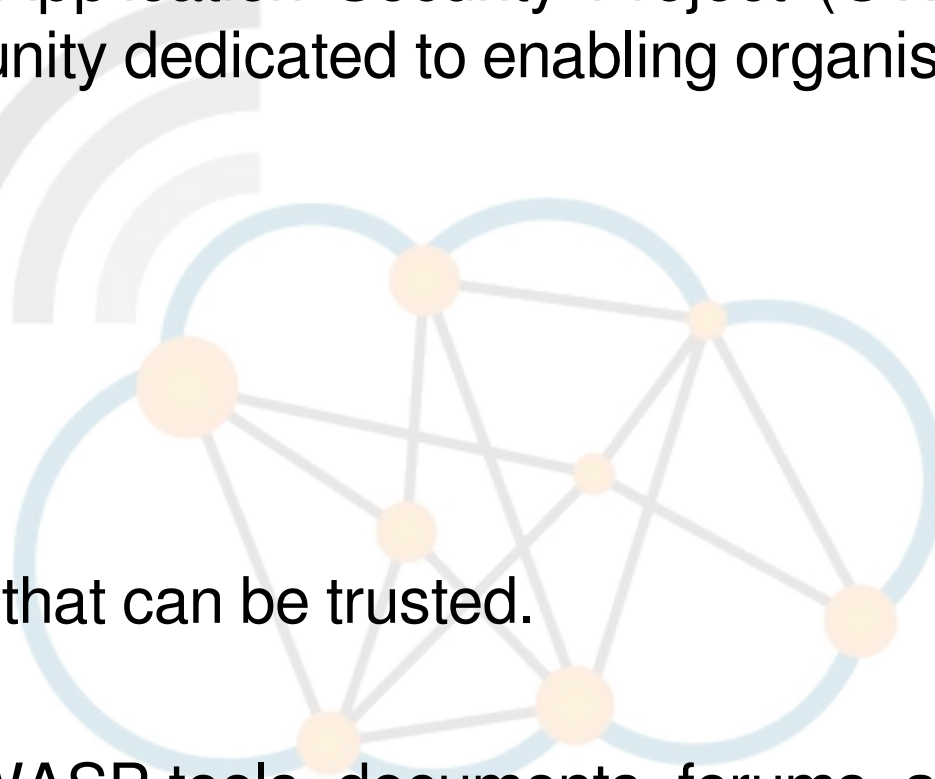
```
+ robots.txt contains 1 entry which should be manually viewed.
```

```
+ 6456 items checked: 1 error(s) and 1 item(s) reported on remote host
```

```
+ End Time: 2015-10-29 23:02:37 (399 seconds)  
-----
```

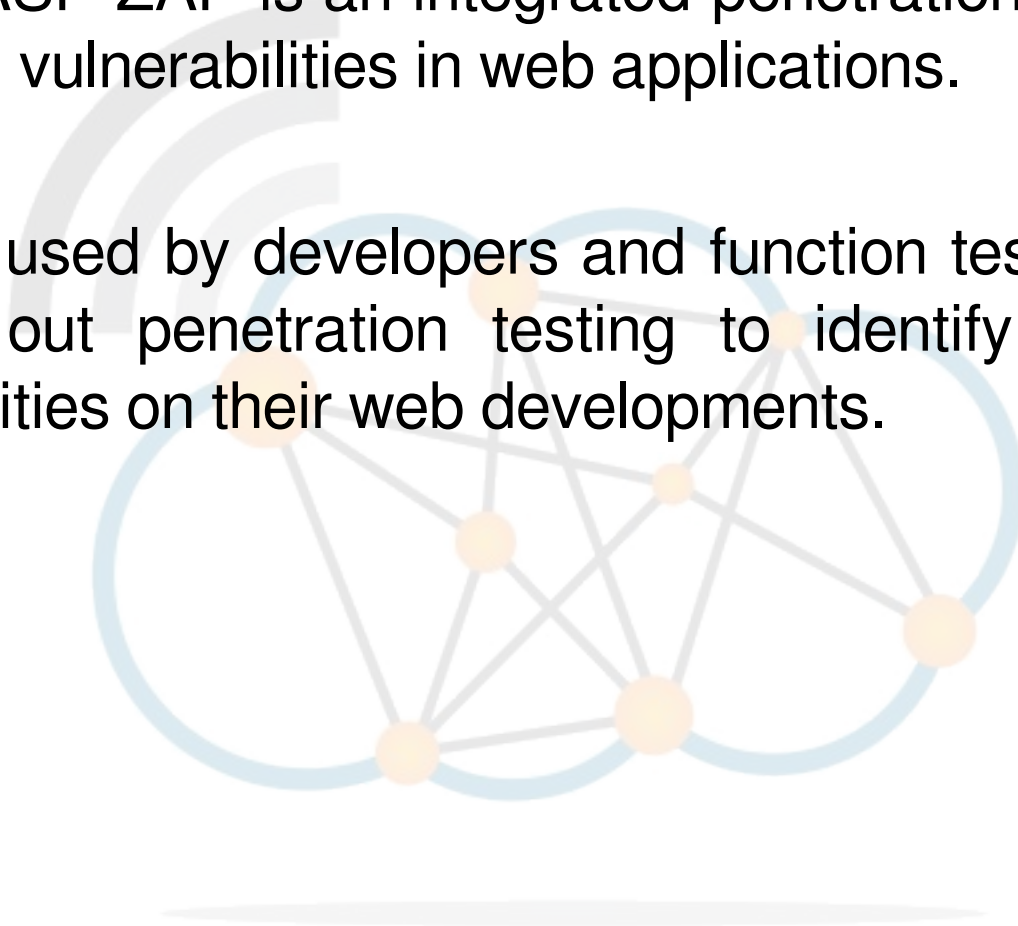
```
+ 1 host(s) tested
```

- Open Web Application Security Project (OWASP) is an open community dedicated to enabling organisations to:
 - Conceive
 - Develop
 - Acquire
 - Operate
 - Maintain
- applications that can be trusted.
- All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security.





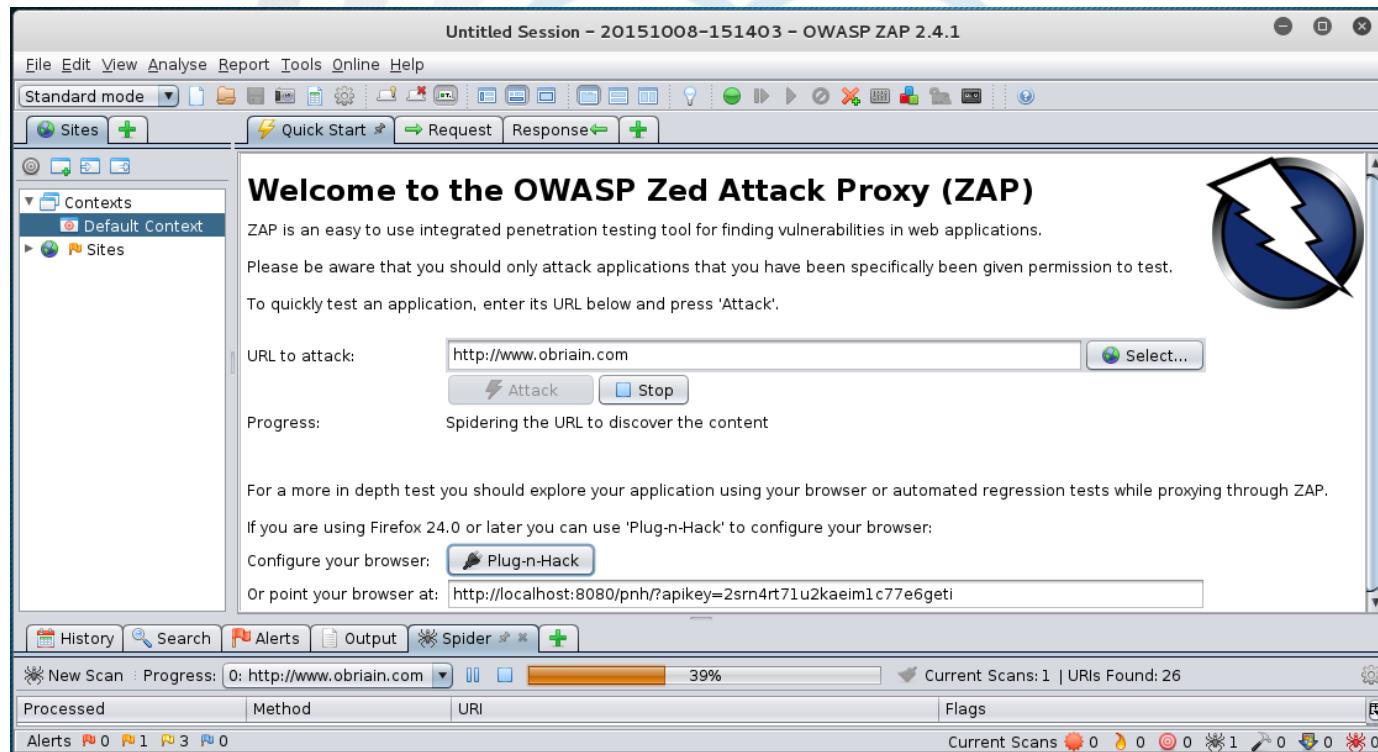
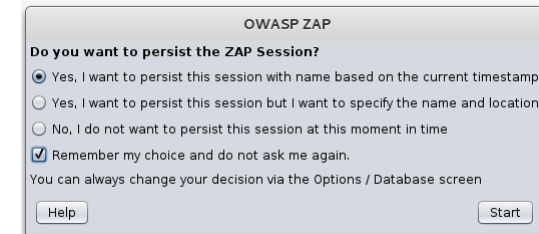
- The OWASP ZAP is an integrated penetration testing tool for finding vulnerabilities in web applications.
- It can be used by developers and function test engineers to carry out penetration testing to identify and close vulnerabilities on their web developments.



OWASP ZAP



```
root@kali:~# zaproxy  
Found Java version 1.7.0_79  
Available memory: 2021 MB  
Setting jvm heap size: -Xmx512m
```



OWASP ZAP Results



The screenshot shows the OWASP ZAP Alerts tab. The left sidebar lists alerts: Alerts (5), Directory Browsing (5), X-Frame-Options Header Not Set (63), Private IP Disclosure (9), Web Browser XSS Protection Not Enabled (63), and X-Content-Type-Options Header Missing (63). The main panel displays details for the 'X-Frame-Options Header Not Set' alert.

X-Frame-Options Header Not Set

URL:

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence:

CWE Id: 0

WASC Id: 0

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.

Other Info:

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use

Reference:

<http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx>

Alerts: 0 2 3 0

Current Scans: 0 1 0 0 0 0 0

OWASP ZAP Reporting



ZAP Scanning Report - Iceweasel

ZAP Scanning Report

file:///root/Website.html

Search

Most Visited

Offensive Security

Kali Linux

Kali Docs

Kali Tools

Exploit-DB

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	68
Low	135
Informational	0

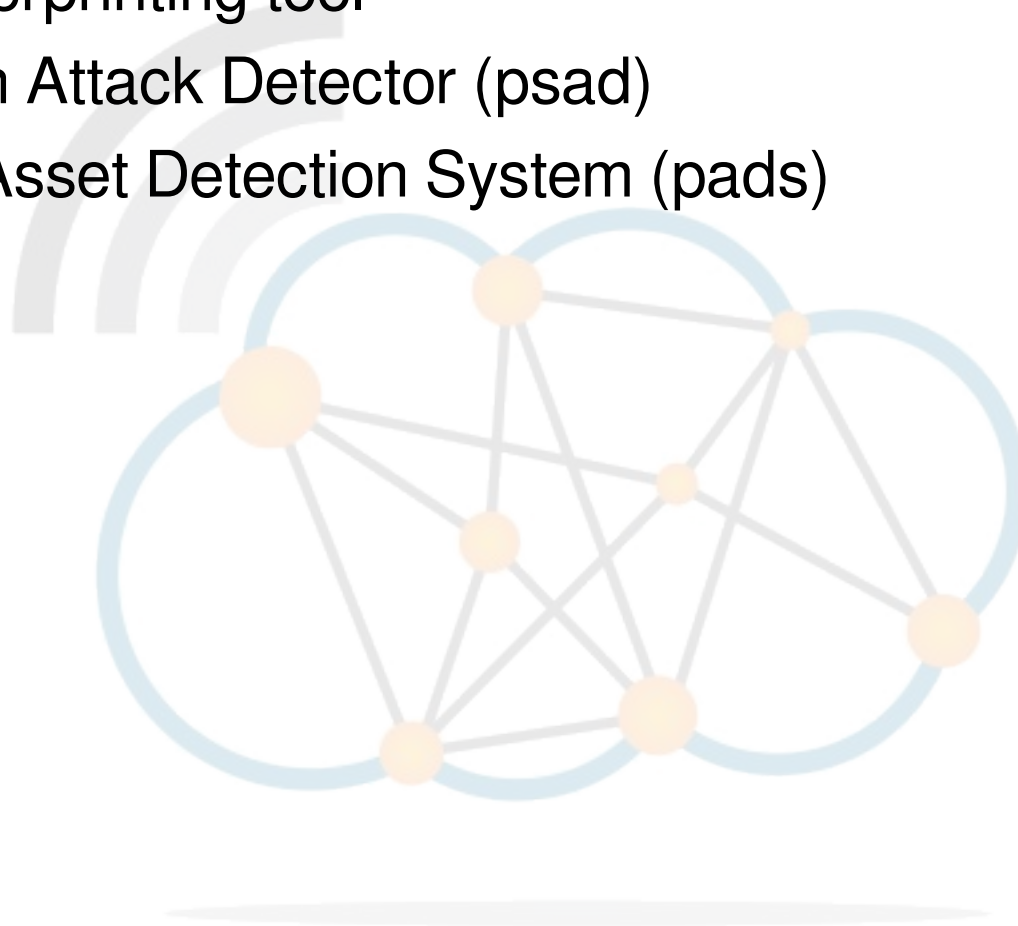
Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://www.obriain.com
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Detection Systems



- p0f – fingerprinting tool
- Port Scan Attack Detector (psad)
- Passive Asset Detection System (pads)





```
cedat:~$ sudo p0f -i eth0 -do /tmp/p0f-output.txt  
--- p0f 3.07b by Michal Zalewski <lcamtuf@coredump.cx> ---
```

```
[!] Consider specifying -u in daemon mode (see README).  
[+] Closed 1 file descriptor.  
[+] Loaded 320 signatures from 'p0f.fp'.  
[+] Intercepting traffic on interface 'eth0'.  
[+] Default packet filtering configured [+VLAN].  
[+] Log file '/tmp/p0f-output.txt' opened for writing.  
[+] Daemon process created, PID 3191 (stderr not kept).
```

Good luck, you're on your own now!

```
cedat:~$ tail /tmp/p0f-output.txt  
[2015/11/03 03:59:41] mod=syn|cli=10.0.2.15/51461|  
srv=192.168.89.1/50501|subj=cli|app=NMap SYN scan|dist=<= 21|  
params=random_ttl|raw_sig=4:43+21:0:1460:1024,0:mss::0  
[2015/11/03 03:59:41] mod=syn|cli=10.0.2.15/51461|  
srv=192.168.89.1/57509|subj=cli|app=NMap SYN scan|dist=<= 8|
```


- **p0f** is ran as a daemon so to kill it send the SIGKILL signal.

```
cedat:~$ ps -ef| grep p0f
root  3191  1  0 03:55 ?      00:00:00 ./p0f -i eth0 -do /tmp/p0f-output.txt
root  3218  3138  0 04:02 pts/1    00:00:00 grep p0f
```

```
cedat:~$ kill -SIGKILL 3191
```

```
cedat:~$ ps -ef | grep p0f
root      3231  3138  0 04:06 pts/1    00:00:00 grep p0f
```

Port Scan Attack Detector (psad)



- **psad** makes use of iptables log messages from the /var/log/messages file to detect, alert, and optionally block port scans and other suspect traffic.

```
cedat:~$ sudo apt install psad
Setting up psad (2.2-3.1) ...
[ ok ] Starting Port Scan Attack Detector: psad.
```

- Set the IP Tables logging rules.

```
cedat:~$ sudo iptables -F

cedat:~$ sudo iptables -A INPUT -j LOG

cedat:~$ sudo iptables -A FORWARD -j LOG

cedat:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -j LOG
-A FORWARD -j LOG
```

psad – update signatures



- ***psad*** update signatures.

```
cedat:~$ sudo psad -sig-update
```

```
cedat:~$ sudo service psad restart
```

```
[info] Stopping the psadwatchd process.
```

```
[info] Stopping the kmsgsd process.
```

```
[info] Stopping the psad process.
```

```
[ ok ] Stopping Port Scan Attack Detector: psad.
```

```
[ ok ] Starting Port Scan Attack Detector: psad.
```

psad – Monitor output to file



- Monitor the changes as they occur in the ***status.out*** file.

```
cedat:~$ sudo tail -f /var/log/psad/status.out
```

```
UDP, Chain: INPUT, Count: 1, DP: 27444, Sid: 237
```

```
SRC: 78.143.141.200, DL: 2, Dsts: 1, Pkts: 46, Unique sigs: 0,  
Email alerts: 4
```

```
DST: 192.168.89.1, Local IP Scanned ports: UDP 34114-60963, Pkts:  
46, Chain: INPUT, Intf: eth0
```

```
Total scan sources: 2
```

```
Total scan destinations: 1
```

```
... ..
```

Passive Asset Detection System (pads)



- **pads** a libpcap based detection engine used to passively detect network assets.
- Discovered devices are logged in ***/var/lib/pads/assets.csv***.

```
cedat:~$ sudo apt install pads
```

```
Setting up pads (1.2-11) ...
```

```
[ ok ] Starting Passive Asset Detection System: pads.
```

- Review the captured assets.

```
cedat:~$ cat /var/lib/pads/assets.csv
```

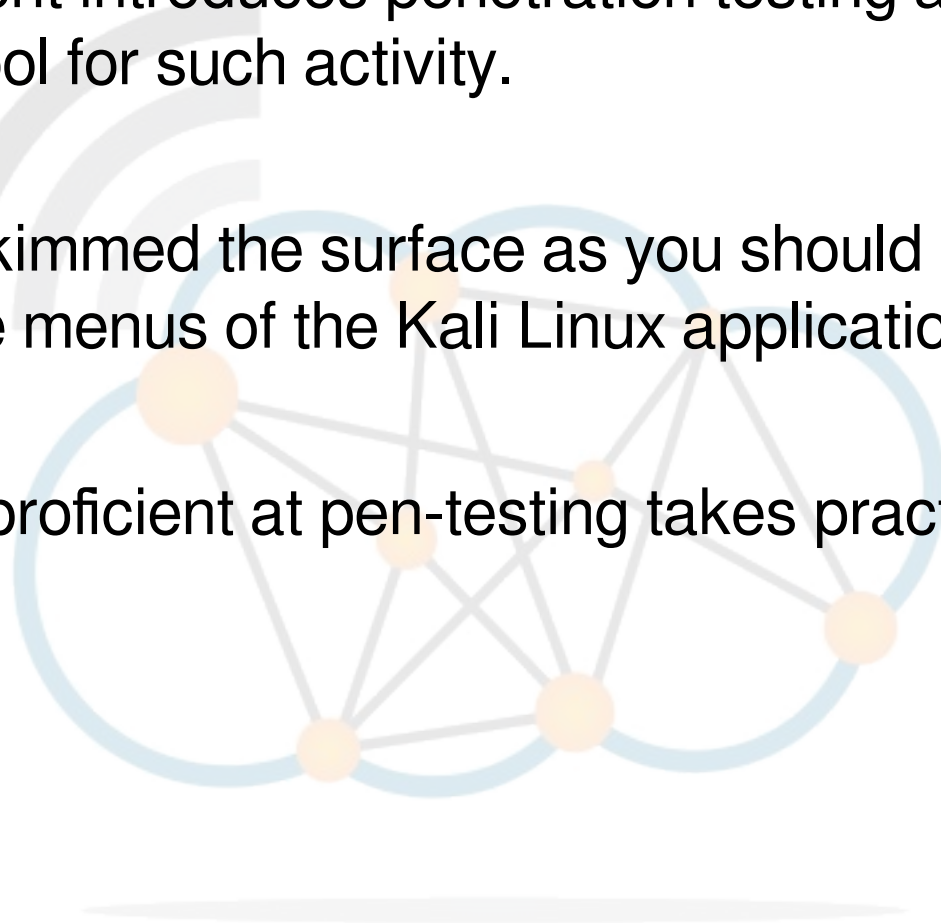
```
asset,port,proto,service,application,discovered
```

```
109.106.96.153,0,0,ARP (Intel Corporation), 0:04:23:B1:8F:E2,  
1404421526
```

Summary



- This document introduces penetration testing and Kali Linux as a tool for such activity.
- It has only skimmed the surface as you should realise just browsing the menus of the Kali Linux applications tab.
- To become proficient at pen-testing takes practice.



Lab Exercise



- Carry out a pen-test on the IP address given to you by the instructor.

