Network Forensics Report

Abstract

This report contain the findings of a forensics investigation of attack scene on a series of packet Capture(PCAP) nad the vpn and access log. This report provides evidence that the attack scene & how they create this malformed connection in victim server. Suspect established the cross Connection via the vpn connection from the ducducgo services to permoed the malformed attack In the victim server by user & root in the valid ssh connection.

This Report attachment services & the evidence also finds the attack & the addressing of the ips.

Tools Used

The tools used in this investigation were:

- Sha1sum
- Wireshark
- Python 3
- Visual Studio code
- Cyberchef
- Geolocation Founder
- Cat
- Grep
- wc

File Hash:

Access.log (f33e0edc100c7746ce2892926b64209455245423)

Route_1.pcapng (a552dec3e454f94e9c91921be9832c3823e9aa93)

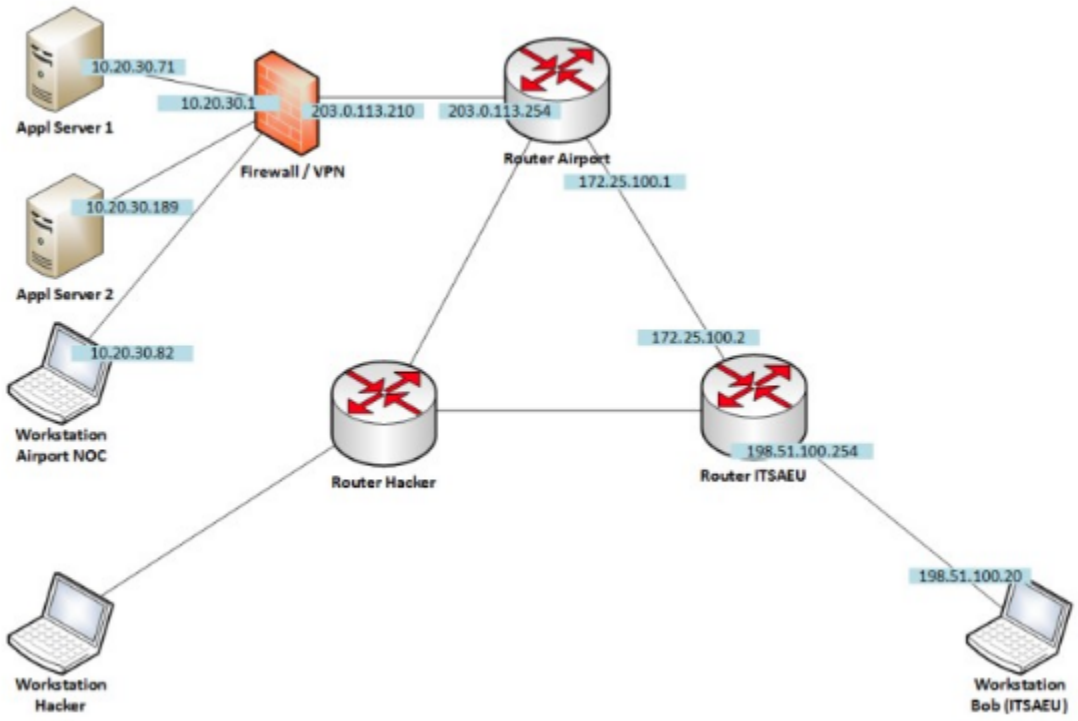
Route.pcap (49b557c22ed66589ac05556860301a345b012565)

Methodology & Findings

Capture 1 (Access.log)

Information given to the forensics investigator indicated the suspect download files which contained important or sensitive information from the authentication log file. Its included successful login attempt, invalid login, attack on user login, protocol and others various scenario. Upon Analysis, there were files transferred using various protocol using ssh & openvpn local server connection, protocol commonly used to access or tried authentication in the victim router network by their ovpn connection. All ip address can be found from this log that was tried to attempt.

Network Diagram:



Access.log File or auth.log file with openvpn.log files can be found from setup virtual machine file system log directory. Like **/var/log**

```
20:07:40 random-server sshd[8598]: Failed password for invalid user root from 61.177.172.104 port 12221 ssh2
20:07:47 random-server sshd[8598]: message repeated 2 times: [ Failed password for invalid user root from 61.177.172.104 port 12221 ssh2]
20:07:48 random-server sshd[8598]: error: maximum authentication attempts exceeded for invalid user root from 61.177.172.104 port 12221 s
preauth]
20:07:48 random-server sshd[8598]: Disconnecting invalid user root 61.177.172.104 port 12221: Too many authentication failures [preauth]
20:08:13 random-server sshd[8629]: Failed password for invalid user root from 218.92.0.210 port 43002 ssh2
20:08:14 random-server sshd[8633]: Failed password for invalid user root from 61.177.173.47 port 45002 ssh2
20:08:16 random-server sshd[8629]: Failed password for invalid user root from 218.92.0.210 port 43002 ssh2
20:08:17 random-server sshd[8633]: Failed password for invalid user root from 61.177.173.47 port 45002 ssh2
20:08:21 random-server sshd[8633]: Failed password for invalid user root from 61.177.173.47 port 45002 ssh2
20:08:22 random-server sshd[8633]: error: maximum authentication attempts exceeded for invalid user root from 61.177.173.47 port 45002 ss
reauth]
20:08:22 random-server sshd[8633]: Disconnecting invalid user root 61.177.173.47 port 45002: Too many authentication failures [preauth]
20:16:24 random-server sshd[8776]: Failed password for invalid user root from 61.177.172.108 port 50915 ssh2
20:16:31 random-server sshd[8776]: message repeated 2 times: [ Failed password for invalid user root from 61.177.172.108 port 50915 ssh2]
20:16:32 random-server sshd[8776]: error: maximum authentication attempts exceeded for invalid user root from 61.177.172.108 port 50915 s
preauth]
20:16:32 random-server sshd[8776]: Disconnecting invalid user root 61.177.172.108 port 50915: Too many authentication failures [preauth]
20:19:22 random-server sshd[8841]: Failed password for invalid user root from 61.177.173.48 port 29890 ssh2
20:19:29 random-server sshd[8841]: message repeated 2 times: [ Failed password for invalid user root from 61.177.173.48 port 29890 ssh2]
20:19:29 random-server sshd[8841]: error: maximum authentication attempts exceeded for invalid user root from 61.177.173.48 port 29890 ss
reauth]
20:19:29 random-server sshd[8841]: Disconnecting invalid user root 61.177.173.48 port 29890: Too many authentication failures [preauth]
20:20:50 random-server sshd[8911]: Failed password for invalid user root from 92.255.85.69 port 21862 ssh2
20:20:51 random-server sshd[8911]: Disconnected from invalid user root 92.255.85.69 port 21862 [preauth]
20:23:02 random-server sshd[8914]: Failed password for invalid user root from 114.92.195.10 port 51943 ssh2
20:23:08 random-server sshd[8914]: message repeated 2 times: [ Failed password for invalid user root from 114.92.195.10 port 51943 ssh2]
20:23:09 random-server sshd[8914]: error: maximum authentication attempts exceeded for invalid user root from 114.92.195.10 port 51943 ss
reauth]
```

Here are some invalid login user attempt by the hacker connection tried to access in server.

```
10:52:21 random-server sshd[86555]: Failed password for invalid user root from 61.177.173.52 port 21451 ssh2
10:52:23 random-server sshd[86554]: Failed password for invalid user root from 61.177.173.48 port 26512 ssh2
10:52:25 random-server sshd[86555]: Failed password for invalid user root from 61.177.173.52 port 21451 ssh2
10:52:25 random-server sshd[86554]: Failed password for invalid user root from 61.177.173.48 port 26512 ssh2
10:52:27 random-server sshd[86555]: Failed password for invalid user root from 61.177.173.52 port 21451 ssh2
10:52:29 random-server sshd[86554]: Failed password for invalid user root from 61.177.173.48 port 26512 ssh2
10:54:31 random-server sshd[86648]: Failed password for invalid user root from 61.177.173.51 port 62757 ssh2
10:54:37 random-server sshd[86648]: message repeated 2 times: [ Failed password for invalid user root from 61.177.173.51 port 62757 ssh2

11:00:34 random-server sshd[86716]: Failed password for invalid user root from 61.177.173.50 port 28240 ssh2
11:00:41 random-server sshd[86716]: message repeated 2 times: [ Failed password for invalid user root from 61.177.173.50 port 28240 ssh2

11:03:29 random-server sshd[86748]: Failed password for invalid user root from 92.255.85.69 port 56786 ssh2
11:26:53 random-server sshd[86884]: Failed password for invalid user wry from 137.116.144.39 port 48144 ssh2
11:28:51 random-server sshd[86886]: Failed password for invalid user root from 92.255.85.69 port 60052 ssh2
11:49:45 random-server sshd[86911]: Failed password for invalid user root from 92.255.85.70 port 44732 ssh2
12:13:33 random-server sshd[86937]: Failed password for invalid user test2 from 92.255.85.69 port 15442 ssh2
12:38:49 random-server sshd[86969]: Failed password for invalid user test2 from 92.255.85.69 port 55728 ssh2
12:52:15 random-server sshd[86983]: Failed password for invalid user support from 80.72.28.2 port 57426 ssh2
12:59:25 random-server sshd[86992]: Failed password for invalid user operator from 141.98.10.154 port 33258 ssh2
13:01:14 random-server sshd[86994]: Failed password for invalid user test2 from 92.255.85.69 port 16310 ssh2
13:06:17 random-server sshd[87001]: Failed password for invalid user root from 103.188.176.251 port 37234 ssh2
13:17:33 random-server sshd[87013]: Failed password for adelandaluce from 73.120.245.111 port 59382 ssh2
13:17:43 random-server sshd[87013]: Failed password for adelandaluce from 73.120.245.111 port 59382 ssh2
13:18:26 random-server sshd[87008]: Failed password for fsyed3 from 67.163.46.231 port 59101 ssh2
13:24:20 random-server sshd[87045]: Failed password for invalid user contador from 92.255.85.70 port 59184 ssh2
13:30:30 random-server sshd[87084]: Failed password for adelandaluce from 73.120.245.111 port 49282 ssh2
13:30:38 random-server sshd[87087]: Failed password for invalid user root from 129.146.188.246 port 15345 ssh2
13:31:11 random-server sshd[87084]: Failed password for adelandaluce from 73.120.245.111 port 49282 ssh2
```

```
ty-HP-Pavilion-Laptop-15-cc0xx:~/Documents/pentest$ cat
iled Password" | cut -d " " -f 6,7 | wc -l
```

Like Length, How much tried to attempt using to user login & root access login included fault login attempt & successful login attempt in this attack.

Its also means the Authentication failure s list from this log, seen in given below image.Remote host also included in this log by the consider with openvpn connection. We need to find the attackers multiple changing ip address that we can clarify that their tried connection where its from. List will be shown in below.

```
Sep 11 10:33:43 random-server sshd[86233]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.172.108 user=r
oot
Sep 11 10:35:29 random-server sshd[86263]: Disconnecting invalid user root 61.177.173.37 port 50722: Too many authentication failures [preauth]
Sep 11 10:35:29 random-server sshd[86263]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.37 user=ro
ot
Sep 11 10:41:42 random-server sshd[86350]: Disconnecting invalid user root 61.177.173.36 port 55709: Too many authentication failures [preauth]
Sep 11 10:41:42 random-server sshd[86350]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.36 user=ro
ot
Sep 11 10:42:08 random-server sshd[86377]: Disconnecting invalid user root 61.177.173.50 port 54603: Too many authentication failures [preauth]
Sep 11 10:42:08 random-server sshd[86377]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.50 user=ro
ot
Sep 11 10:44:21 random-server sshd[86429]: Disconnecting invalid user root 61.177.172.124 port 17166: Too many authentication failures [preauth
]
Sep 11 10:44:21 random-server sshd[86429]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.172.124 user=r
oot
Sep 11 10:52:28 random-server sshd[86555]: Disconnecting invalid user root 61.177.173.52 port 21451: Too many authentication failures [preauth]
Sep 11 10:52:28 random-server sshd[86555]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.52 user=ro
ot
Sep 11 10:52:30 random-server sshd[86554]: Disconnecting invalid user root 61.177.173.48 port 26512: Too many authentication failures [preauth]
Sep 11 10:52:30 random-server sshd[86554]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.48 user=ro
ot
Sep 11 10:54:38 random-server sshd[86648]: Disconnecting invalid user root 61.177.173.51 port 62757: Too many authentication failures [preauth]
Sep 11 10:54:38 random-server sshd[86648]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.51 user=ro
ot
Sep 11 11:00:42 random-server sshd[86716]: Disconnecting invalid user root 61.177.173.50 port 28240: Too many authentication failures [preauth]
Sep 11 11:00:42 random-server sshd[86716]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.50 user=ro
ot
Sep 11 13:17:43 random-server sshd[87013]: Disconnecting authenticating user adelandaluce 73.120.245.111 port 59382: Too many authentication fa
ilures [preauth]
Sep 11 13:31:11 random-server sshd[87084]: Disconnecting authenticating user adelandaluce 73.120.245.111 port 49282: Too many authentication fa
ilures [preauth]
```

```
24 user=root
Sep 11 10:52:19 random-server sshd[86555]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.5
2 user=root
Sep 11 10:52:21 random-server sshd[86554]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.4
8 user=root
Sep 11 10:54:29 random-server sshd[86648]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.5
1 user=root
Sep 11 11:00:32 random-server sshd[86716]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.177.173.5
0 user=root
Sep 11 11:03:27 random-server sshd[86748]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.255.85.69
 user=root
Sep 11 11:26:51 random-server sshd[86884]: pam_unix(sshd:auth): check pass; user unknown
Sep 11 11:26:51 random-server sshd[86884]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=137.116.144.
39
Sep 11 11:28:49 random-server sshd[86886]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.255.85.69
 user=root
Sep 11 11:49:43 random-server sshd[86911]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.255.85.70
 user=root
Sep 11 12:13:30 random-server sshd[86937]: pam_unix(sshd:auth): check pass; user unknown
Sep 11 12:13:30 random-server sshd[86937]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.255.85.69

Sep 11 12:38:47 random-server sshd[86969]: pam_unix(sshd:auth): check pass; user unknown
Sep 11 12:38:47 random-server sshd[86969]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.255.85.69

Sep 11 12:52:13 random-server sshd[86983]: pam_unix(sshd:auth): check pass; user unknown
Sep 11 12:52:13 random-server sshd[86983]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=80.72.28.2
Sep 11 12:59:23 random-server sshd[86992]: pam_unix(sshd:auth): check pass; user unknown
Sep 11 12:59:23 random-server sshd[86992]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=141.98.10.15
4
Sep 11 13:01:12 random-server sshd[86994]: pam_unix(sshd:auth): check pass; user unknown
Sep 11 13:01:12 random-server sshd[86994]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.255.85.69
```

Logname with uid & euid with the server response

*All IP addresses list & their details will be shown in attachment files. We can check from these.

```
SvDi2HK9vAoAR+bAmuZYpV9zIBVfD7/KlFVIJdTeo
Sep 5 20:00:53 random-server sshd[8418]: Accepted publickey for rrimocal from 24.136.6.187 port 49836 ssh2: ED25519 SHA256:jgdsj7P+8CyBy8yebc7U
Dq+ovpIbQYchlHzp6ZdSPLU
Sep 5 20:08:22 random-server sshd[8631]: Accepted publickey for rrimocal from 24.136.6.187 port 49988 ssh2: ED25519 SHA256:jgdsj7P+8CyBy8yebc7U
Dq+ovpIbQYchlHzp6ZdSPLU
Sep 6 08:27:37 random-server sshd[14917]: Accepted publickey for rsabo from 147.126.51.254 port 3002 ssh2: ED25519 SHA256:WEiV3BkQPSEyPRqvQQ+va
65eMme6XdXdklQ9j/5vWiw
Sep 7 11:15:38 random-server sshd[30724]: Accepted publickey for adhungana1 from 2400:1a00:b040:46fa:74cb:dbd2:fd65:1288 port 50857 ssh2: ED255
19 SHA256:IjsMAg5EXzuZMQHofwlaRxZ8/u1zEA6W13vhm3GctgE
Sep 7 12:47:23 random-server sshd[31433]: Accepted publickey for amansoor1 from 147.126.10.153 port 47769 ssh2: ED25519 SHA256:o0pyZICQjw1j2Ni6
hsS4vJDLmkcpgN2Et91PxYWUa/4
Sep 7 21:33:57 random-server sshd[37968]: Accepted publickey for rrusaiteme from 73.75.131.210 port 10897 ssh2: ED25519 SHA256:wzrpE+ACwgyZ2wKa
OilowW+drs1J4lsbJ9a3MGSXza0
Sep 9 13:47:41 random-server sshd[65044]: Accepted publickey for vventola from 98.34.68.250 port 62434 ssh2: ED25519 SHA256:xwPL61g7pdZGRa3pfbK
7Tk/1cdqteTRtfwJeyLZllYs
Sep 9 13:55:08 random-server sshd[65274]: Accepted publickey for usercbs from 97.207.31.82 port 49185 ssh2: RSA SHA256:qIltjtmVNWv2KROwxjO2xWIO
XwxESDbRjQEBZSeC27M
Sep 9 14:35:47 random-server sshd[66050]: Accepted publickey for usercbs from 97.207.31.82 port 50018 ssh2: RSA SHA256:qIltjtmVNWv2KROwxjO2xWIO
XwxESDbRjQEBZSeC27M
Sep 9 17:05:49 random-server sshd[68794]: Accepted publickey for usercbs from 97.207.31.82 port 51587 ssh2: RSA SHA256:qIltjtmVNWv2KROwxjO2xWIO
XwxESDbRjQEBZSeC27M
Sep 9 18:24:17 random-server sshd[70036]: Accepted publickey for avilladeleon from 2601:249:8081:34f0:1552:ef24:401b:e632 port 53557 ssh2: ED25
519 SHA256:OQL9b/xHlfza2+KxLCNQCtFRqalvtt+iZUJpAqUSSD4
Sep 9 19:16:16 random-server sshd[70825]: Accepted publickey for snaquin from 207.237.255.10 port 62491 ssh2: ED25519 SHA256:bYpXmlFjmSe8UW9bHf
Ukmal38EWZjkNSZ+K/bX1fiKw
Sep 9 19:56:22 random-server sshd[72001]: Accepted publickey for vventola from 2601:249:8400:86f0:50b1:1b9f:bc2:84e5 port 63564 ssh2: ED25519 S
HA256:xwPL61g7pdZGRa3pfbK7Tk/1cdqteTRtfwJeyLZllYs
Sep 9 20:09:25 random-server sshd[72247]: Accepted publickey for usercbs from 97.207.31.82 port 54529 ssh2: RSA SHA256:qIltjtmVNWv2KROwxjO2xWIO
XwxESDbRjQEBZSeC27M
Sep 9 20:28:56 random-server sshd[72668]: Accepted publickey for vventola from 2601:249:8400:86f0:50b1:1b9f:bc2:84e5 port 63783 ssh2: ED25519 S
HA256:xwPL61g7pdZGRa3pfbK7Tk/1cdqteTRtfwJeyLZllYs
Sep 10 02:25:04 random-server sshd[76280]: Accepted publickey for tsiddiqui5 from 147.126.81.97 port 11736 ssh2: ED25519 SHA256:H3l57QjftCyjQjx
s3KV5Fe9UoK1JhPB85GSCfVY1iLs
Sep 10 18:00:57 random-server sshd[79400]: Accepted publickey for tsiddiqui5 from 76.29.22.51 port 54728 ssh2: ED25519 SHA256:H3l57QjftCyjQjxs3
KV5Fe9UoK1JhPB85GSCfVY1iLs
Sep 11 14:12:14 random-server sshd[87374]: Accepted publickey for usercbs from 97.207.31.82 port 62877 ssh2: RSA SHA256:qIltjtmVNWv2KROwxjO2xWI
OXwxESDbRjQEBZSeC27M
trinity@trinity-HP-Pavilion-Laptop-15-cc0xx:~/Documents/pentest$
```

Here is the exact Accepted publickey means accepted user from the tried section. Hacker using a random server by using open vpn connection and established the connection. SHA256 hash for RSA encryption secure connection presented in this log.

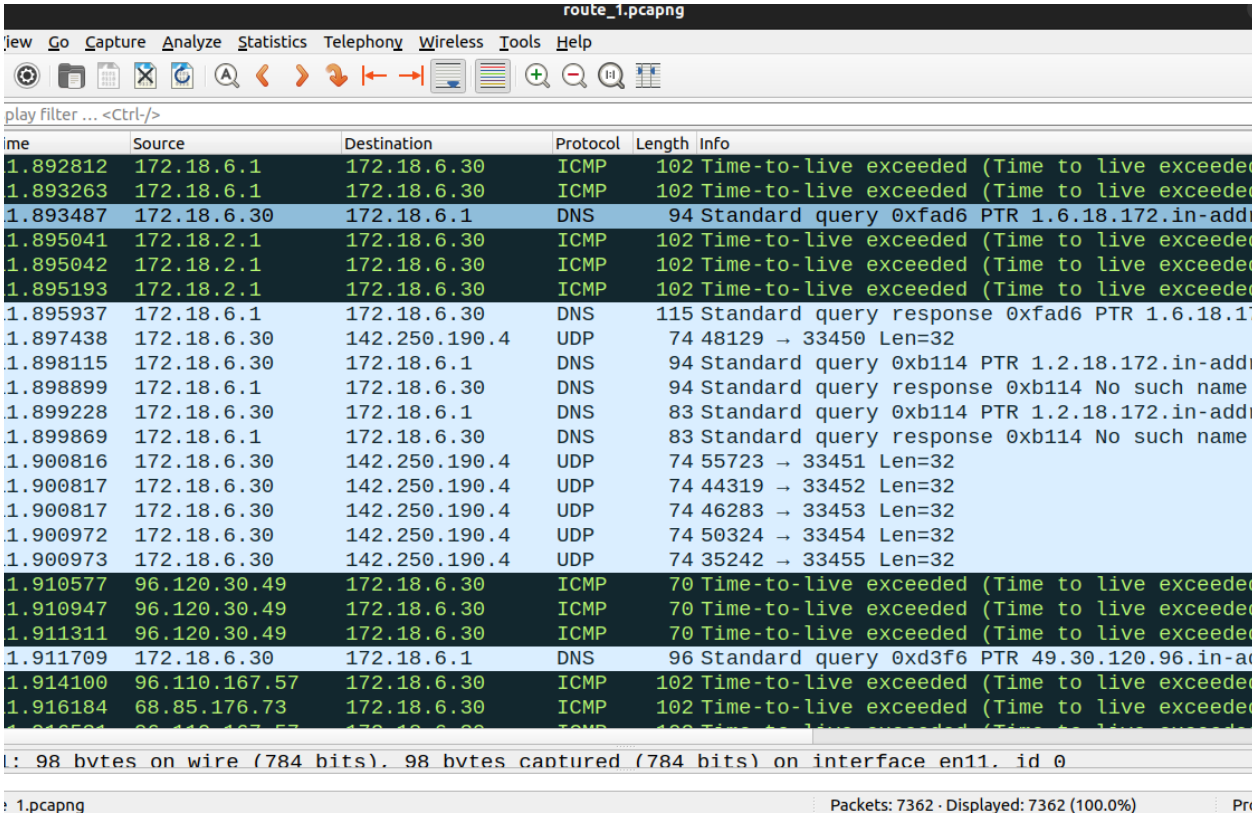
Capture 2 (Openvpn.log)

```
14:20:20 trinity-HP-Pavilion-Laptop-15-cc0xx sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
14:25:57 trinity-HP-Pavilion-Laptop-15-cc0xx gnome-keyring-daemon[2368]: asked to register item /org/freedesktop/secrets/
tion/login/1, but it's already registered
14:30:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[8202]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
14:30:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[8202]: pam_unix(cron:session): session closed for user root
15:17:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[11541]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
15:17:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[11541]: pam_unix(cron:session): session closed for user root
15:30:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[12062]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
15:30:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[12062]: pam_unix(cron:session): session closed for user root
15:32:42 trinity-HP-Pavilion-Laptop-15-cc0xx gdm-password]: gkr-pam: unlocked login keyring
15:59:57 trinity-HP-Pavilion-Laptop-15-cc0xx gdm-password]: gkr-pam: unlocked login keyring
16:17:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[14794]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
16:17:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[14794]: pam_unix(cron:session): session closed for user root
16:30:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[15226]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
16:30:01 trinity-HP-Pavilion-Laptop-15-cc0xx CRON[15226]: pam_unix(cron:session): session closed for user root
Plain Text ∨  Tab Width: 8 ∨  Ln 237559, Col 118 ∨  INS
```

Openvpn file .ovpn connection for attack and attempt to the user & root session in the Target server.

Openvpn log data also included in the authentication access log dataset.

Capture 2 (router packet from Destination site)



ime	Source	Destination	Protocol	Length	Info
1.892812	172.18.6.1	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede
1.893263	172.18.6.1	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede
1.893487	172.18.6.30	172.18.6.1	DNS	94	Standard query 0xfad6 PTR 1.6.18.172.in-addr
1.895041	172.18.2.1	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede
1.895042	172.18.2.1	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede
1.895193	172.18.2.1	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede
1.895937	172.18.6.1	172.18.6.30	DNS	115	Standard query response 0xfad6 PTR 1.6.18.1
1.897438	172.18.6.30	142.250.190.4	UDP	74	48129 → 33450 Len=32
1.898115	172.18.6.30	172.18.6.1	DNS	94	Standard query 0xb114 PTR 1.2.18.172.in-addr
1.898899	172.18.6.1	172.18.6.30	DNS	94	Standard query response 0xb114 No such name
1.899228	172.18.6.30	172.18.6.1	DNS	83	Standard query 0xb114 PTR 1.2.18.172.in-addr
1.899869	172.18.6.1	172.18.6.30	DNS	83	Standard query response 0xb114 No such name
1.900816	172.18.6.30	142.250.190.4	UDP	74	55723 → 33451 Len=32
1.900817	172.18.6.30	142.250.190.4	UDP	74	44319 → 33452 Len=32
1.900817	172.18.6.30	142.250.190.4	UDP	74	46283 → 33453 Len=32
1.900972	172.18.6.30	142.250.190.4	UDP	74	50324 → 33454 Len=32
1.900973	172.18.6.30	142.250.190.4	UDP	74	35242 → 33455 Len=32
1.910577	96.120.30.49	172.18.6.30	ICMP	70	Time-to-live exceeded (Time to live exceede
1.910947	96.120.30.49	172.18.6.30	ICMP	70	Time-to-live exceeded (Time to live exceede
1.911311	96.120.30.49	172.18.6.30	ICMP	70	Time-to-live exceeded (Time to live exceede
1.911709	172.18.6.30	172.18.6.1	DNS	96	Standard query 0xd3f6 PTR 49.30.120.96.in-a
1.914100	96.110.167.57	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede
1.916184	68.85.176.73	172.18.6.30	ICMP	102	Time-to-live exceeded (Time to live exceede

De-authentication & Acknowledgement

- Account was used to log into the local server via TELNET- (username and password)

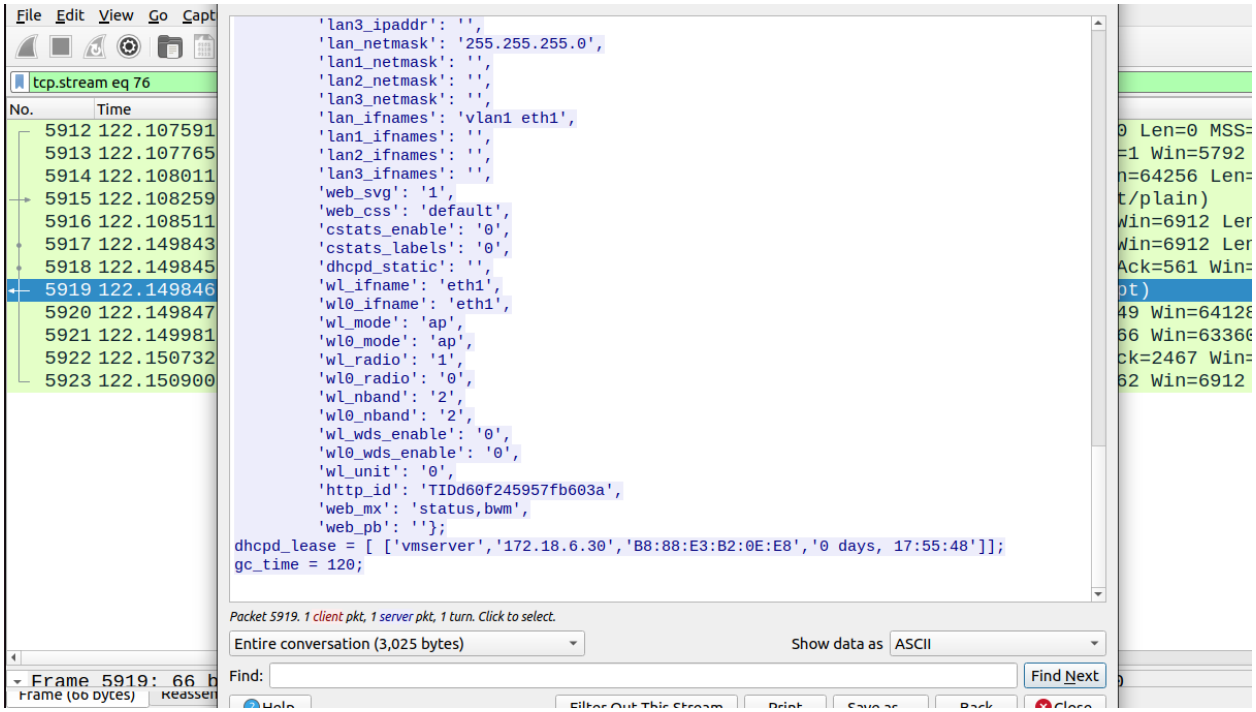
  p2-server login: sstevenson

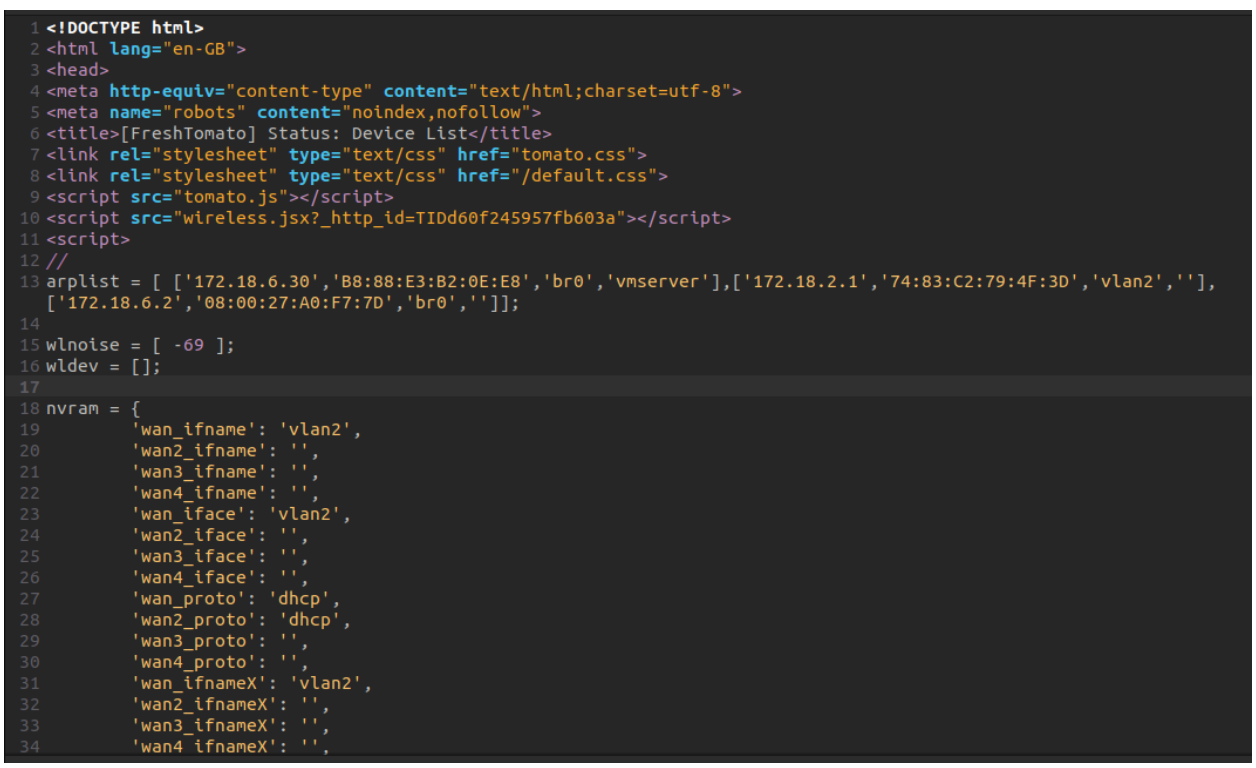
  Password: R3@LLYG00Dp@$$w0rd!

```
........... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'.........
38400,38400....#.vmserver:0....'..DISPLAY.vmserver:0......xterm-256color......
20.04.3 LTS
...p2-server login: ssssttteevveennssoonn
.
Password: R3@LLYG00Dp@$$w0rd!
.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-86-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 26 Sep 2021 10:37:35 PM UTC

  System load:  0.0                Processes:               113
  Usage of /:   33.7% of 18.57GB   Users logged in:         1
  Memory usage: 6%                 IPv4 address for enp0s3: 172.18.6.2
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.


Last login: Sun Sep 26 20:59:47 UTC 2021 from 172.18.6.30 on pts/0
.]0;sstevenson@p2-server: ~..[01;32msstevenson@p2-server.[00m:.[01;34m~.[00m$
llssbb__rreelleeaassee  --aa
```

- Account was used to log into the local router via HTTP-http_id=TIDd60f245957fb603a

Associated js & source File Attached.



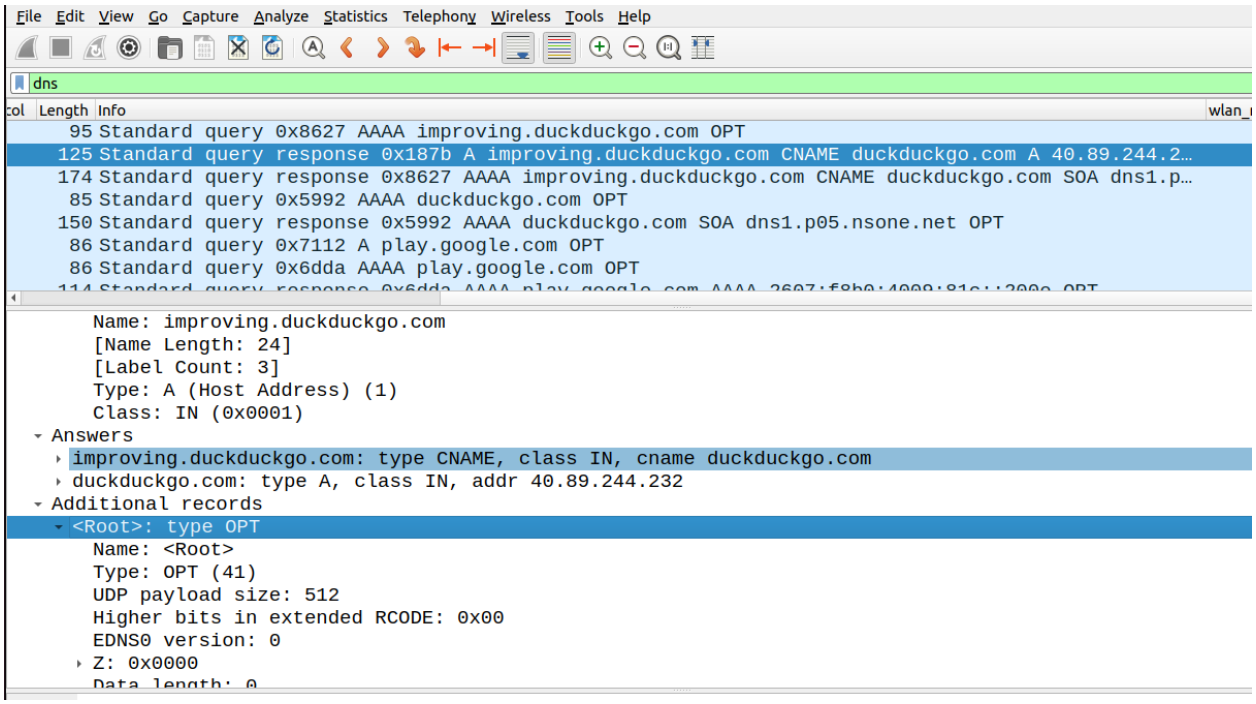


```
<!DOCTYPE html>
<html lang="en-GB">
<head>
<meta http-equiv="content-type" content="text/html;charset=utf-8">
<meta name="robots" content="noindex,nofollow">
<title>[FreshTomato] Status: Device List</title>
<link rel="stylesheet" type="text/css" href="tomato.css">
<link rel="stylesheet" type="text/css" href="/default.css">
<script src="tomato.js"></script>
<script src="wireless.jsx?_http_id=TIDd60f245957fb603a"></script>
<script>
//
arplist = [ ['172.18.6.30','B8:88:E3:B2:0E:E8','br0','vmserver'],['172.18.2.1','74:83:C2:79:4F:3D','vlan2',''],
['172.18.6.2','08:00:27:A0:F7:7D','br0',''']];

wlnoise = [ -69 ];
wldev = [];

nvram = {
        'wan_ifname': 'vlan2',
        'wan2_ifname': '',
        'wan3_ifname': '',
        'wan4_ifname': '',
        'wan_iface': 'vlan2',
        'wan2_iface': '',
        'wan3_iface': '',
        'wan4_iface': '',
        'wan_proto': 'dhcp',
        'wan2_proto': 'dhcp',
        'wan3_proto': '',
        'wan4_proto': '',
        'wan_ifnameX': 'vlan2',
        'wan2_ifnameX': '',
        'wan3_ifnameX': '',
        'wan4_ifnameX': '',
```

This is the source file screenshot and main source file attached with the evidence section.

- According to DNS in the capture, IP address hosts the duckduckgo.com website–

IP: 40.89.244.232



In this section, we can see that hacker using duckduckgo service for hide the source connection. From the previous authentication log files we saw that multiple ip connection attempt for authentication in pam_unix. We can find from dns packet section for ducducgo.

- DNS server(s) is/are being used to resolve names to IPs-

```
▾ Domain Name System (response)
    Transaction ID: 0x55e8
  ▸ Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 1
  ▾ Queries
    ▾ 234.232.208.50.in-addr.arpa: type PTR, class IN
        Name: 234.232.208.50.in-addr.arpa
        [Name Length: 27]
        [Label Count: 6]
        Type: PTR (domain name PoinTeR) (12)
        Class: IN (0x0001)
  ▾ Authoritative nameservers
    ▾ 232.208.50.in-addr.arpa: type SOA, class IN, mname dns101.comcast.net
        Name: 232.208.50.in-addr.arpa
```

Here we found the most phase of network forensics, dns resolve names ips for
The openvpn connection.

Capture 2 (router packet from source site)

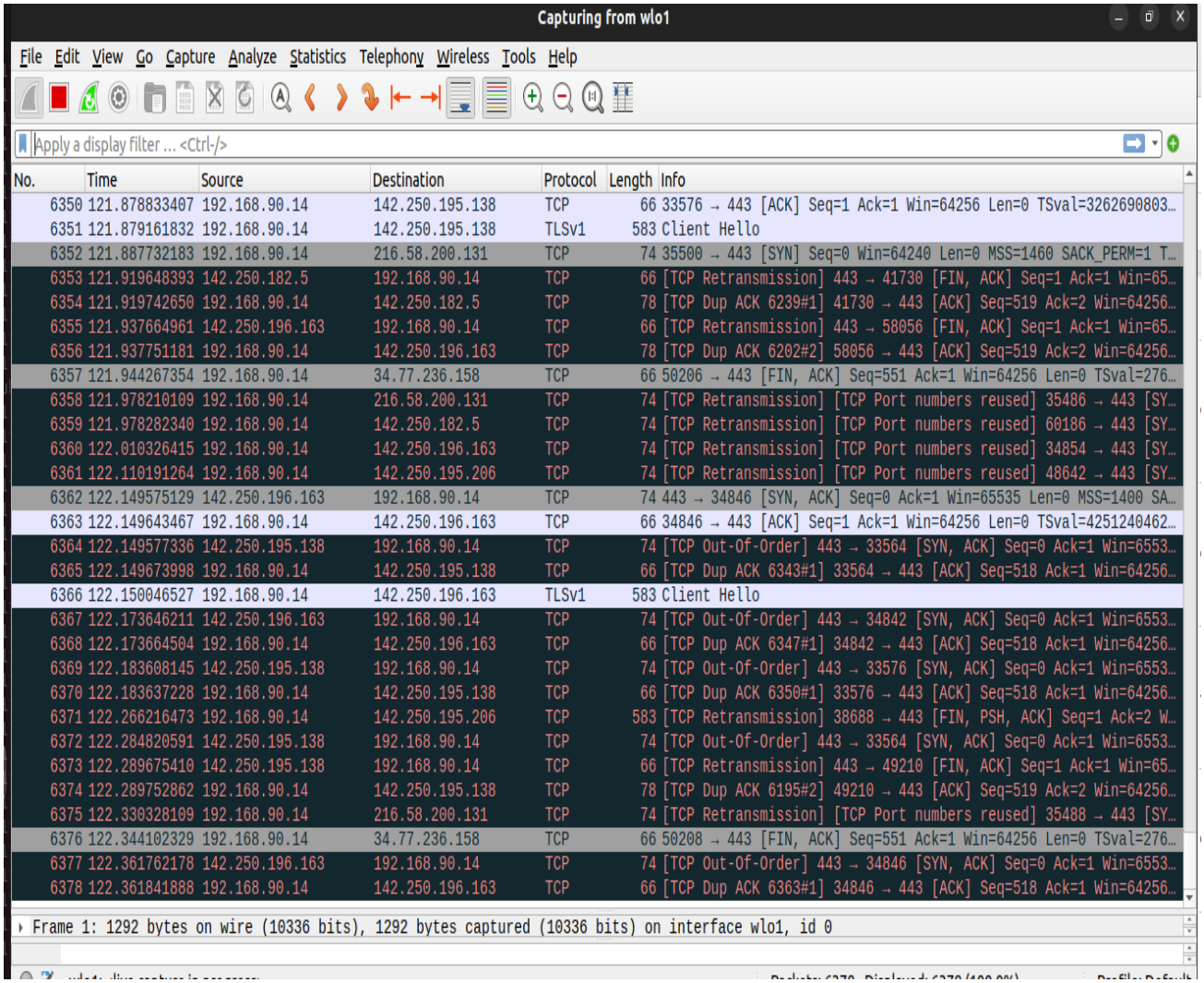
route.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

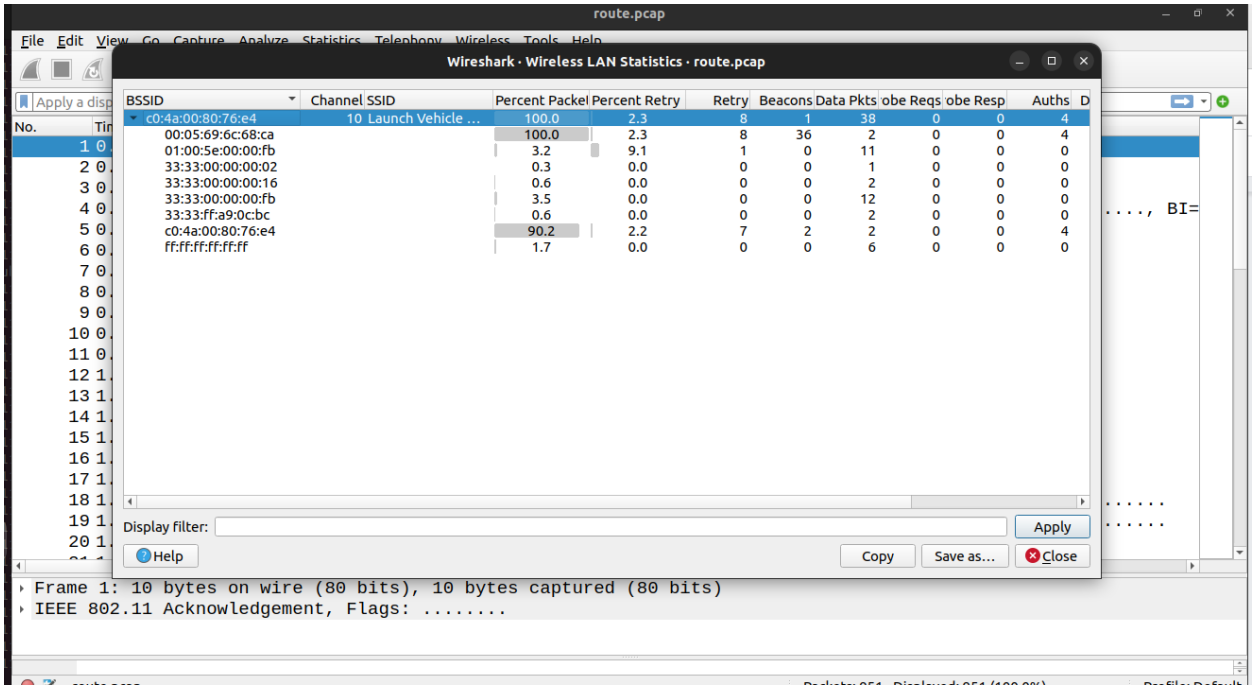
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19	1.512499	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=1, FN=0, Flags=.....
20	1.515569		VMware_6c:68:ca…	802.…	10	Acknowledgement, Flags=.....
21	1.517206	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=2, FN=0, Flags=.....
22	1.517286	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=0, FN=0, Flags=.....
23	1.517293	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=1, FN=0, Flags=.....
24	1.523129	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=3, FN=0, Flags=.....
25	1.525311	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=2, FN=0, Flags=.....
26	1.525317	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=3, FN=0, Flags=.....
27	1.526348		VMware_6c:68:ca…	802.…	10	Acknowledgement, Flags=.....
28	1.529234	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=4, FN=0, Flags=.....
29	1.533125	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=5, FN=0, Flags=.....
30	1.535434	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=4, FN=0, Flags=.....
31	1.535442	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=5, FN=0, Flags=.....
32	1.536609	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=6, FN=0, Flags=.....
33	1.536613		VMware_6c:68:ca…	802.…	10	Acknowledgement, Flags=.....
34	1.539234	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=7, FN=0, Flags=.....
35	1.539240	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=6, FN=0, Flags=.....
36	1.543741	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=8, FN=0, Flags=.....
37	1.544623		VMware_6c:68:ca…	802.…	10	Acknowledgement, Flags=.....
38	1.547643	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=9, FN=0, Flags=.....
39	1.547652	VMware_6c:68:ca	Tp-LinkT_80:76:…	802.…	26	Deauthentication, SN=7, FN=0, Flags=.....
40	1.547657	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=8, FN=0, Flags=.....
41	1.553482	Tp-LinkT_80:76:…	VMware_6c:68:ca	802.…	26	Deauthentication, SN=10, FN=0, Flags=.....

Routing Information packet Generation for Deauthentication & Acknowledgement



Capture source site packet when attacker used openvpn connection for setup and target the attack



Wireless Packet Statistics

We are extracted the packet for the wireless to check the hacker activities. We found their Malformed source code here(Also attached in evidence)-

```
//
wl_ifaces = [ ['eth1','0','1','FreshTomato24','A0:04:60:CA:6C:B6',1,16,'ap','00:00:00:00:00:00']];

//
wl_bands = [ [ '2'] ];

//
nvram = {
        'wl_nband': '2',
        'wl0_nband': '2',
        'wl_unit': '0',
        'http_id': 'TIDd60f245957fb603a',
        'web_mx': 'status,bwm',
        'web_pb': ''};

function wl_fface(uidx) {
return wl_ifaces[uidx][1];
}
function wl_unit(uidx) {
return wl_ifaces[uidx][2];
}
function wl_sunit(uidx) {
return wl_ifaces[uidx][3];
}
```

```
function wl_uidx(unit) {
for (var u = 0; u < wl_ifaces.length; ++u) {
if (wl_ifaces[u][2] == unit) return u;
}
return -1;
}
function wl_ifidx(ifname) {
for (var u = 0; u < wl_ifaces.length; ++u) {
if (wl_ifaces[u][0] == ifname) return u;
}
return -1;
}
function wl_ifidxx(ifname) {
for (var u = 0; u < wl_ifaces.length; ++u) {
if (wl_ifaces[u][1] == ifname) return u;
}
return -1;
}
function wl_display_ifname(uidx) {
return wl_ifaces[uidx][0]+(wl_sunit(uidx) < 0 ?
' (wl'+wl_fface(uidx)+')' : '')+((wl_bands[uidx].length == 1) ?
(wl_bands[uidx][0] == '1') ? ' / 5 GHz' : ' / 2.4 GHz') : ((nvram['wl'+wl_unit(uidx)+'_nband'] ==
' / 5 GHz' : ' / 2.4 GHz'));
}
```

And the status section is-

```
ault:
(!stats.wanup[uidx - 1]) {
ts.wanip[uidx - 1] = '0.0.0.0';
ts.wannetmask[uidx - 1] = '0.0.0.0';
ts.wangateway[uidx - 1] = '0.0.0.0';



ts.ip6_wan = ((typeof(sysinfo.ip6_wan) != 'undefined') ? sysinfo.ip6_wan : '')+'';
ts.ip6_wan_dns1 = ((typeof(sysinfo.ip6_wan_dns1) != 'undefined') ? sysinfo.ip6_wan_dns1 : '')+'';
ts.ip6_wan_dns2 = ((typeof(sysinfo.ip6_wan_dns2) != 'undefined') ? sysinfo.ip6_wan_dns2 : '')+'';
ts.ip6_lan = ((typeof(sysinfo.ip6_lan) != 'undefined') ? sysinfo.ip6_lan : '')+'';
ts.ip6_lan_ll = ((typeof(sysinfo.ip6_lan_ll) != 'undefined') ? sysinfo.ip6_lan_ll : '')+'';
ts.ip6_lan1 = ((typeof(sysinfo.ip6_lan1) != 'undefined') ? sysinfo.ip6_lan1 : '')+'';
ts.ip6_lan1_ll = ((typeof(sysinfo.ip6_lan1_ll) != 'undefined') ? sysinfo.ip6_lan1_ll : '')+'';
ts.ip6_lan2 = ((typeof(sysinfo.ip6_lan2) != 'undefined') ? sysinfo.ip6_lan2 : '')+'';
ts.ip6_lan2_ll = ((typeof(sysinfo.ip6_lan2_ll) != 'undefined') ? sysinfo.ip6_lan2_ll : '')+'';
ts.ip6_lan3 = ((typeof(sysinfo.ip6_lan3) != 'undefined') ? sysinfo.ip6_lan3 : '')+'';
ts.ip6_lan3_ll = ((typeof(sysinfo.ip6_lan3_ll) != 'undefined') ? sysinfo.ip6_lan3_ll : '')+'';
ts.wanstatus = ['Connected','Disconnected'];
 (var uidx = 1; uidx <= nvram.mwan_num; ++uidx)
(stats.wanstatus[uidx - 1] != 'Connected')
ts.wanstatus[uidx - 1] = '<b>'+stats.wanstatus[uidx - 1]+'</b>';
ts.channel = [];
ts.interference = [];
ts.qual = [];
 (var uidx = 0; uidx < wl_ifaces.length; ++uidx) {
 i = wlstats[uidx].channel * 1;
(i < 0)
 -i;
ts.channel.push('<a href="tools-survey.asp">'+((i) ? i+'' : 'Auto')+((wlstats[uidx].mhz) ? ' - '+(wlstats[uidx].mhz / 1000.0).toFixe
all>GHz</small>' : '')+'</a>'+((a < 0) ? ' <small>(scanning...)</small>' : ''));
ts.interference.push((wlstats[uidx].intf >= 0) ? ((wlstats[uidx].intf) ? 'Severe' : 'Acceptable') : '');
 wlstats[uidx].nbw * 1;
tats[uidx].nbw = (a > 0) ? (a+' <small>MHz</small>') : 'Auto';
```

From Analyze the source packet & the source code, we can identify the pptp server ip stat and The netmask of hacker connection. We can prove it from the Authentication log file again. Let Me check that-

```
andom-server sshd[32053]: Accepted publickey for vuser1 from 185.97.1.8 port 54471 ssh2: RSA
andom-server sshd[9803]: Accepted publickey for vuser2 from 121.54.148.170 port 57577 ssh2: RSA
andom-server sshd[18703]: Accepted publickey for vuser2 from 121.54.148.170 port 57932 ssh2: RSA
andom-server sshd[23817]: Accepted publickey for vuser2 from 121.54.148.170 port 58203 ssh2: RSA
andom-server sshd[14435]: Invalid user pi from 64.139.73.170
andom-server sshd[14439]: Invalid user pi from 64.139.73.170
andom-server sshd[14435]: Failed password for invalid user pi from 64.139.73.170 port 43492 ssh2
andom-server sshd[14439]: Failed password for invalid user pi from 64.139.73.170 port 43496 ssh2
andom-server sshd[12472]: Accepted publickey for vuser2 from 121.54.148.170 port 59193 ssh2: RSA
andom-server sshd[14402]: Accepted publickey for vuser1 from 185.97.1.8 port 56745 ssh2: RSA
andom-server sshd[31334]: Accepted publickey for vuser2 from 121.54.148.170 port 59919 ssh2: RSA
andom-server sshd[28592]: Accepted publickey for vuser2 from 121.54.148.170 port 60365 ssh2: RSA
andom-server sshd[12036]: Accepted publickey for vuser2 from 121.54.148.170 port 61638 ssh2: RSA
andom-server sshd[7695]: Accepted publickey for vuser2 from 121.54.148.170 port 62273 ssh2: RSA
andom-server sshd[10360]: Accepted publickey for vuser2 from 121.54.148.170 port 62280 ssh2: RSA
andom-server sshd[20825]: Accepted publickey for vuser2 from 121.54.148.170 port 62312 ssh2: RSA
andom-server sshd[18392]: Accepted publickey for vuser2 from 2600:215:80:5f00:e127:a0d4:a1e0:9bb port 64624 ssh2: RSA
andom-server sshd[4336]: Accepted publickey for vuser2 from 2600:215:80:5f00:c843:96b8:ec24:245e port 49748 ssh2: RSA
andom-server sshd[13242]: Accepted publickey for vuser2 from 2600:215:80:5f00:c843:96b8:ec24:245e port 49785 ssh2: RSA
random-server sshd[24692]: Invalid user support from 113.190.158.52
random-server sshd[24692]: Failed password for invalid user support from 113.190.158.52 port 49413 ssh2
random-server sshd[17600]: Invalid user admin1 from 14.241.155.9
random-server sshd[17600]: Failed none for invalid user admin1 from 14.241.155.9 port 64633 ssh2
random-server sshd[21174]: Invalid user user1 from 110.136.88.232
random-server sshd[21174]: Failed password for invalid user user1 from 110.136.88.232 port 18688 ssh2
random-server sshd[2094]: Failed password for invalid user root from 117.6.64.147 port 5903 ssh2
random-server sshd[24524]: Invalid user system from 116.206.200.44
random-server sshd[24524]: Failed password for invalid user system from 116.206.200.44 port 64222 ssh2
random-server sshd[8263]: Invalid user administrator from 27.77.236.86
random-server sshd[8263]: Failed password for invalid user administrator from 27.77.236.86 port 58027 ssh2
random-server sshd[16796]: Invalid user Administrator from 113.160.208.69
random-server sshd[16796]: Failed password for invalid user Administrator from 113.160.208.69 port 56027 ssh2
random-server sshd[25717]: Invalid user guest from 14.246.221.234
random-server sshd[25717]: Failed password for invalid user guest from 14.246.221.234 port 58400 ssh2
random-server sshd[15140]: Invalid user Administrator from 123.255.200.130
```