Sample Security Incident Response Report

Privileged and Confidential Attorney-Client Communication/Work Product

INCIDENT IDENTIFICATION INFORMATION

Date and Time of Notification: May 23, 2021	
Incident Detector’s Information: Student 1	
System Name: PumpPLC, PumpMonitor, Web01, TargetWindows01	Date and Time Detected: 9:01am
Title: Water Treatment Facility Security Incident Report	Location: Water Facility Network

INCIDENT SUMMARY

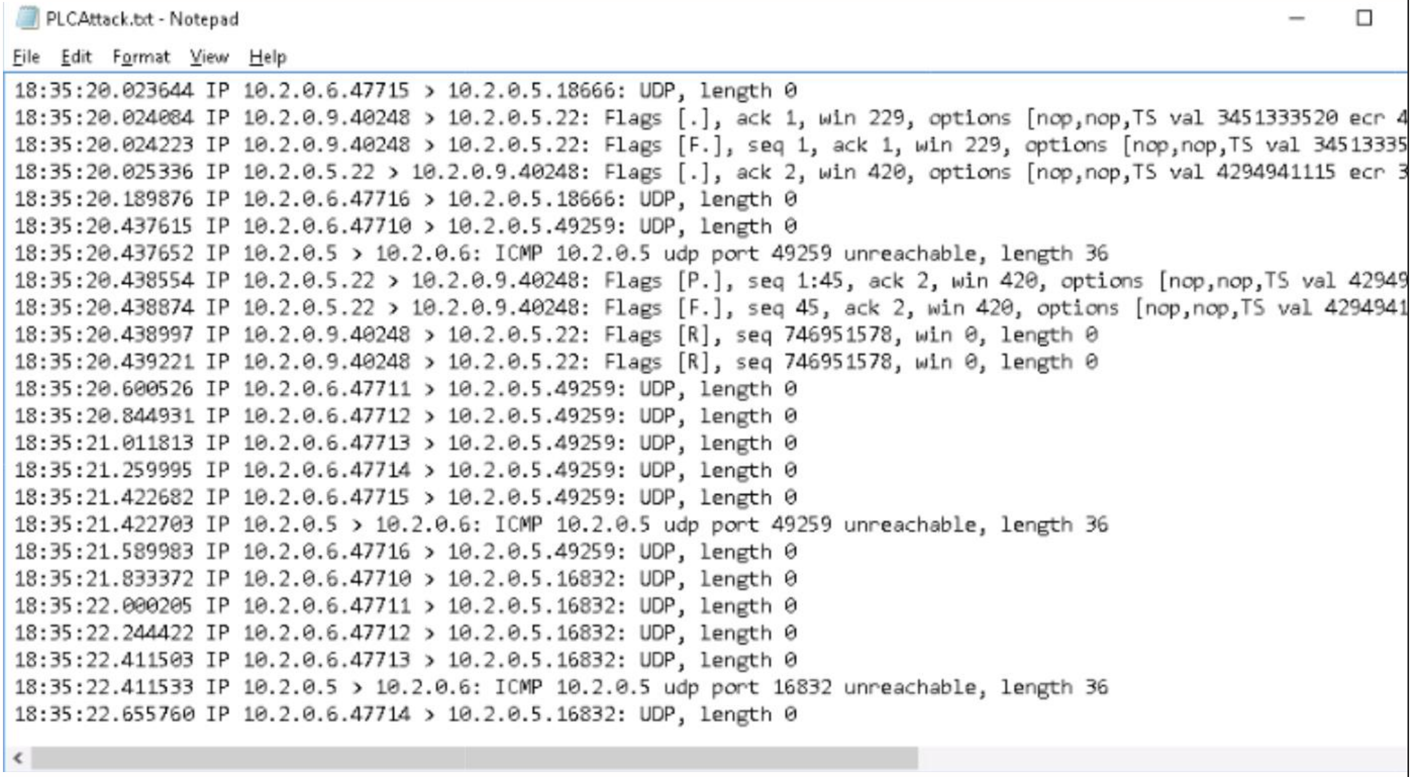
Type of Incident Detected:

☐ Denial of Service ☐ Malicious Code ☐ Unauthorized Use

☐ Unauthorized Access ☐ Suspicious Activity ☐ Other

Description of Incident:

We ran windump/Wireshark/tcpdump on the PumpMonitor and loaded the capture file(s) in Wireshark. This shows suspicious activity, specifically, an unnecessary protocol “UDP” in use.



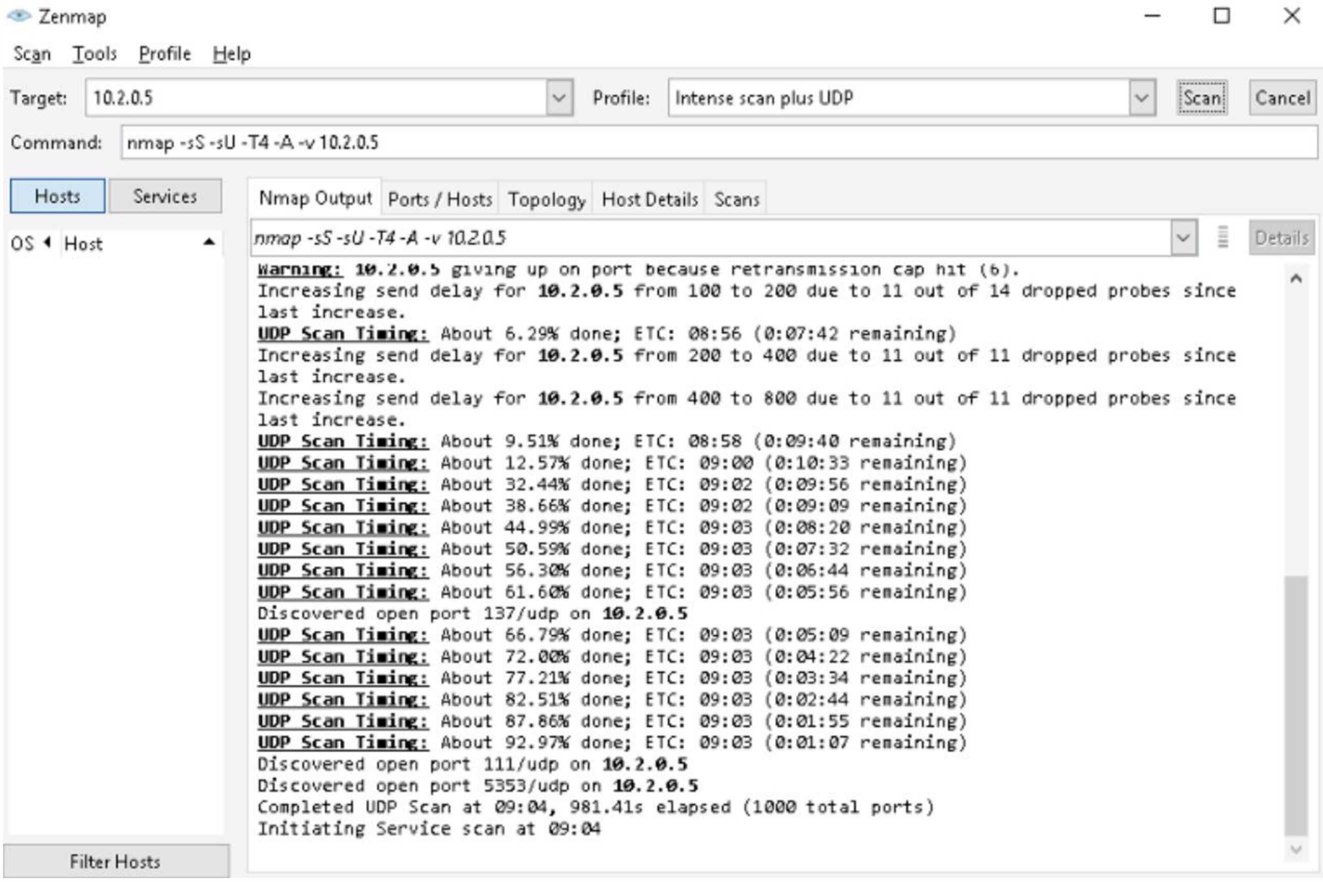
```
18:35:20.023644 IP 10.2.0.6.47715 > 10.2.0.5.18666: UDP, length 0
18:35:20.024084 IP 10.2.0.9.40248 > 10.2.0.5.22: Flags [.], ack 1, win 229, options [nop,nop,TS val 3451333520 ecr 4
18:35:20.024223 IP 10.2.0.9.40248 > 10.2.0.5.22: Flags [F.], seq 1, ack 1, win 229, options [nop,nop,TS val 34513335
18:35:20.025336 IP 10.2.0.5.22 > 10.2.0.9.40248: Flags [.], ack 2, win 420, options [nop,nop,TS val 4294941115 ecr 3
18:35:20.189876 IP 10.2.0.6.47716 > 10.2.0.5.18666: UDP, length 0
18:35:20.437615 IP 10.2.0.6.47710 > 10.2.0.5.49259: UDP, length 0
18:35:20.437652 IP 10.2.0.5 > 10.2.0.6: ICMP 10.2.0.5 udp port 49259 unreachable, length 36
18:35:20.438554 IP 10.2.0.5.22 > 10.2.0.9.40248: Flags [P.], seq 1:45, ack 2, win 420, options [nop,nop,TS val 42949
18:35:20.438874 IP 10.2.0.5.22 > 10.2.0.9.40248: Flags [F.], seq 45, ack 2, win 420, options [nop,nop,TS val 4294941
18:35:20.438997 IP 10.2.0.9.40248 > 10.2.0.5.22: Flags [R], seq 746951578, win 0, length 0
18:35:20.439221 IP 10.2.0.9.40248 > 10.2.0.5.22: Flags [R], seq 746951578, win 0, length 0
18:35:20.600526 IP 10.2.0.6.47711 > 10.2.0.5.49259: UDP, length 0
18:35:20.844931 IP 10.2.0.6.47712 > 10.2.0.5.49259: UDP, length 0
18:35:21.011813 IP 10.2.0.6.47713 > 10.2.0.5.49259: UDP, length 0
18:35:21.259995 IP 10.2.0.6.47714 > 10.2.0.5.49259: UDP, length 0
18:35:21.422682 IP 10.2.0.6.47715 > 10.2.0.5.49259: UDP, length 0
18:35:21.422703 IP 10.2.0.5 > 10.2.0.6: ICMP 10.2.0.5 udp port 49259 unreachable, length 36
18:35:21.589983 IP 10.2.0.6.47716 > 10.2.0.5.49259: UDP, length 0
18:35:21.833372 IP 10.2.0.6.47710 > 10.2.0.5.16832: UDP, length 0
18:35:22.000205 IP 10.2.0.6.47711 > 10.2.0.5.16832: UDP, length 0
18:35:22.244422 IP 10.2.0.6.47712 > 10.2.0.5.16832: UDP, length 0
18:35:22.411503 IP 10.2.0.6.47713 > 10.2.0.5.16832: UDP, length 0
18:35:22.411533 IP 10.2.0.5 > 10.2.0.6: ICMP 10.2.0.5 udp port 16832 unreachable, length 36
18:35:22.655760 IP 10.2.0.6.47714 > 10.2.0.5.16832: UDP, length 0
```

Since UDP is used for connectionless data transfer, as in movies and music, it should not be in use on PumpMonitor (10.2.0.6) or PumpPLC (10.2.0.5). Multiple UDP packets with unreachable ports. We suspect a UDP-based attack.

PumpMonitor (10.2.0.6) appears to be committing an attack on PumpPLC (10.2.0.5). We conclude this because:

- Numerous unnecssary UDP packets are traveling from PumpMonitor to PumpPLC.
- Numerous ICMP packets from PumpPLC to PumpMonitor are reporting an unreachable port.

Zenmap shows that at least one UDP port is open on PumpPLC (10.2.0.5), making it vulnerable to a UDP-based attack.



Target: 10.2.0.5

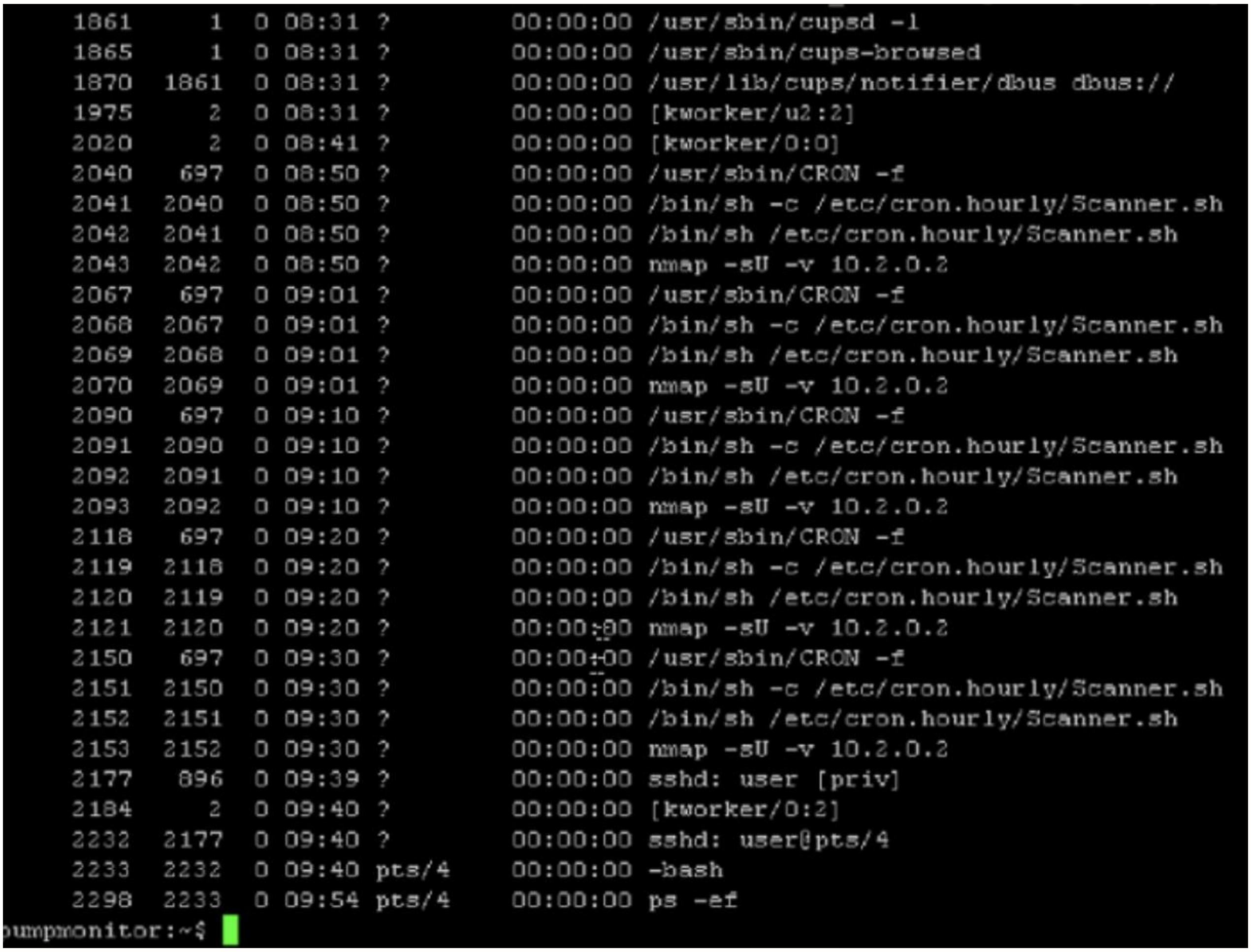
Profile: Intense scan plus UDP

Command: nmap -sS -sU -T4 -A -v 10.2.0.5

nmap -sS -sU -T4 -A -v 10.2.0.5

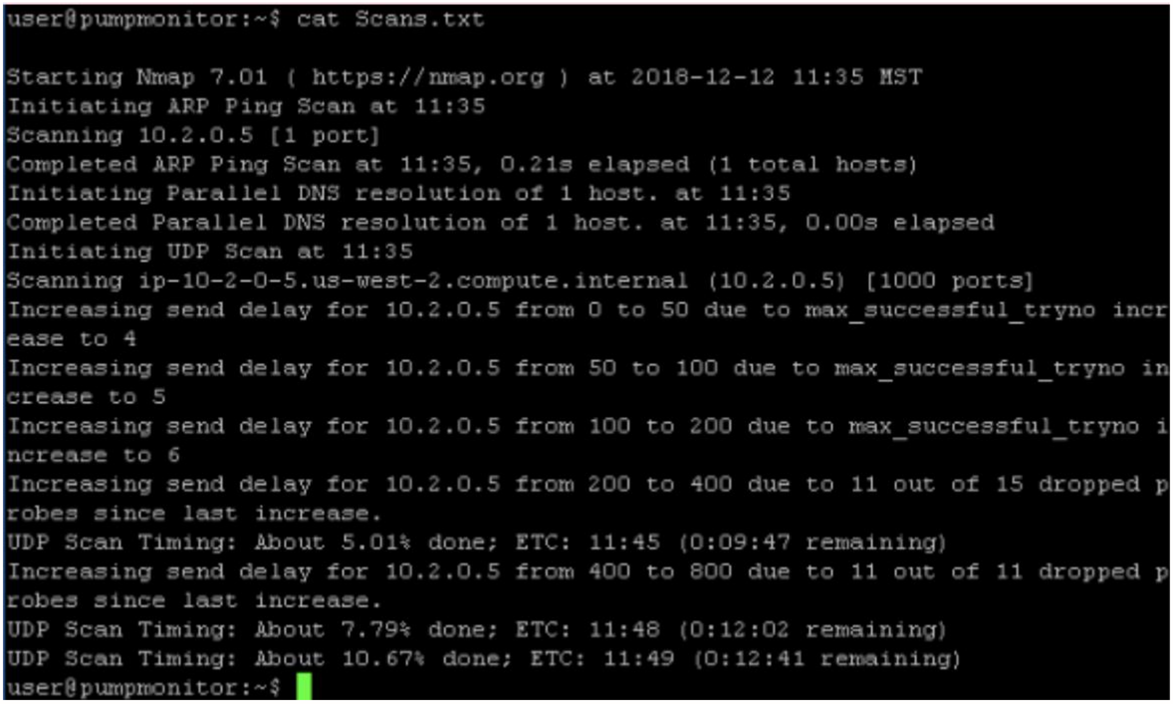
```
Warning: 10.2.0.5 giving up on port because retransmission cap hit (6).
Increasing send delay for 10.2.0.5 from 100 to 200 due to 11 out of 14 dropped probes since
last increase.
UDP Scan Timing: About 6.29% done; ETC: 08:56 (0:07:42 remaining)
Increasing send delay for 10.2.0.5 from 200 to 400 due to 11 out of 11 dropped probes since
last increase.
Increasing send delay for 10.2.0.5 from 400 to 800 due to 11 out of 11 dropped probes since
last increase.
UDP Scan Timing: About 9.51% done; ETC: 08:58 (0:09:40 remaining)
UDP Scan Timing: About 12.57% done; ETC: 09:00 (0:10:33 remaining)
UDP Scan Timing: About 32.44% done; ETC: 09:02 (0:09:56 remaining)
UDP Scan Timing: About 38.66% done; ETC: 09:02 (0:09:09 remaining)
UDP Scan Timing: About 44.99% done; ETC: 09:03 (0:08:20 remaining)
UDP Scan Timing: About 50.59% done; ETC: 09:03 (0:07:32 remaining)
UDP Scan Timing: About 56.30% done; ETC: 09:03 (0:06:44 remaining)
UDP Scan Timing: About 61.60% done; ETC: 09:03 (0:05:56 remaining)
Discovered open port 137/udp on 10.2.0.5
UDP Scan Timing: About 66.79% done; ETC: 09:03 (0:05:09 remaining)
UDP Scan Timing: About 72.00% done; ETC: 09:03 (0:04:22 remaining)
UDP Scan Timing: About 77.21% done; ETC: 09:03 (0:03:34 remaining)
UDP Scan Timing: About 82.51% done; ETC: 09:03 (0:02:44 remaining)
UDP Scan Timing: About 87.86% done; ETC: 09:03 (0:01:55 remaining)
UDP Scan Timing: About 92.97% done; ETC: 09:03 (0:01:07 remaining)
Discovered open port 111/udp on 10.2.0.5
Discovered open port 5353/udp on 10.2.0.5
Completed UDP Scan at 09:04, 981.41s elapsed (1000 total ports)
Initiating Service scan at 09:04
```

On PumpMonitor (10.2.0.6) we discovered suspicious network activity and malicious processes. To observe processes, we used ps -ef to find suspicious processes, Scanner.sh and nmap:



```
     1861     1  0 08:31 ?        00:00:00 /usr/sbin/cupsd -l
     1865     1  0 08:31 ?        00:00:00 /usr/sbin/cups-browsed
     1870  1861  0 08:31 ?        00:00:00 /usr/lib/cups/notifier/dbus dbus://
     1975     2  0 08:31 ?        00:00:00 [kworker/u2:2]
     2020     2  0 08:41 ?        00:00:00 [kworker/0:0]
     2040   697  0 08:50 ?        00:00:00 /usr/sbin/CRON -f
     2041  2040  0 08:50 ?        00:00:00 /bin/sh -c /etc/cron.hourly/Scanner.sh
     2042  2041  0 08:50 ?        00:00:00 /bin/sh /etc/cron.hourly/Scanner.sh
     2043  2042  0 08:50 ?        00:00:00 nmap -sU -v 10.2.0.2
     2067   697  0 09:01 ?        00:00:00 /usr/sbin/CRON -f
     2068  2067  0 09:01 ?        00:00:00 /bin/sh -c /etc/cron.hourly/Scanner.sh
     2069  2068  0 09:01 ?        00:00:00 /bin/sh /etc/cron.hourly/Scanner.sh
     2070  2069  0 09:01 ?        00:00:00 nmap -sU -v 10.2.0.2
     2090   697  0 09:10 ?        00:00:00 /usr/sbin/CRON -f
     2091  2090  0 09:10 ?        00:00:00 /bin/sh -c /etc/cron.hourly/Scanner.sh
     2092  2091  0 09:10 ?        00:00:00 /bin/sh /etc/cron.hourly/Scanner.sh
     2093  2092  0 09:10 ?        00:00:00 nmap -sU -v 10.2.0.2
     2118   697  0 09:20 ?        00:00:00 /usr/sbin/CRON -f
     2119  2118  0 09:20 ?        00:00:00 /bin/sh -c /etc/cron.hourly/Scanner.sh
     2120  2119  0 09:20 ?        00:00:00 /bin/sh /etc/cron.hourly/Scanner.sh
     2121  2120  0 09:20 ?        00:00:00 nmap -sU -v 10.2.0.2
     2150   697  0 09:30 ?        00:00:00 /usr/sbin/CRON -f
     2151  2150  0 09:30 ?        00:00:00 /bin/sh -c /etc/cron.hourly/Scanner.sh
     2152  2151  0 09:30 ?        00:00:00 /bin/sh /etc/cron.hourly/Scanner.sh
     2153  2152  0 09:30 ?        00:00:00 nmap -sU -v 10.2.0.2
     2177   896  0 09:39 ?        00:00:00 sshd: user [priv]
     2184     2  0 09:40 ?        00:00:00 [kworker/0:2]
     2232  2177  0 09:40 ?        00:00:00 sshd: user@pts/4
     2233  2232  0 09:40 pts/4    00:00:00 -bash
     2298  2233  0 09:54 pts/4    00:00:00 ps -ef
umpmonitor:~$
```

The output of Scanner.sh and the nmap processes were redirected to /home/user/Scans.txt which contains:



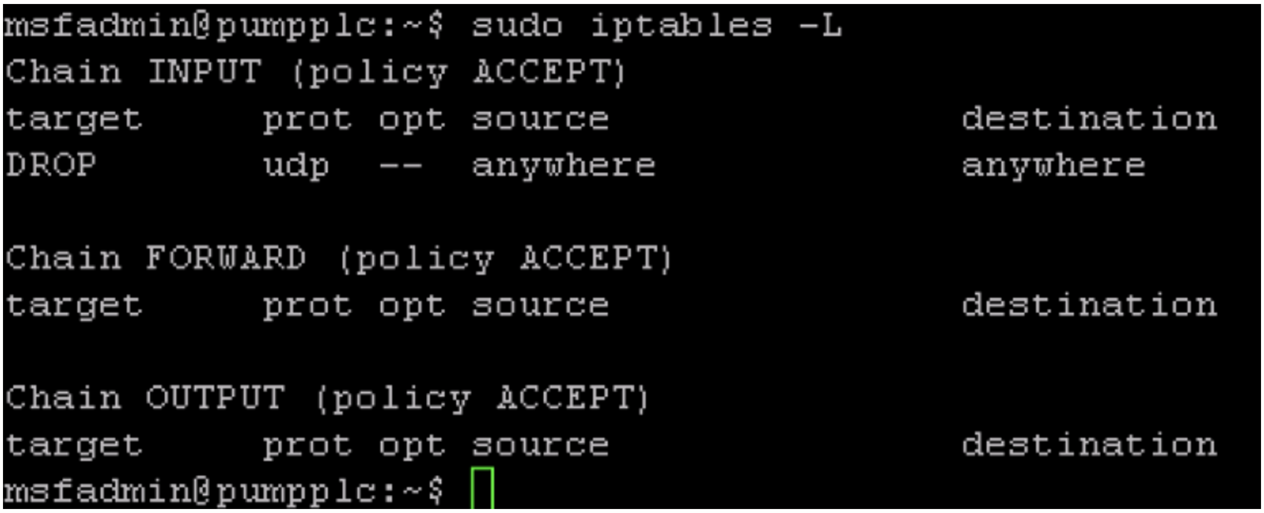
```
user@pumpmonitor:~$ cat Scans.txt

Starting Nmap 7.01 ( https://nmap.org ) at 2018-12-12 11:35 MST
Initiating ARP Ping Scan at 11:35
Scanning 10.2.0.5 [1 port]
Completed ARP Ping Scan at 11:35, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:35
Completed Parallel DNS resolution of 1 host. at 11:35, 0.00s elapsed
Initiating UDP Scan at 11:35
Scanning ip-10-2-0-5.us-west-2.compute.internal (10.2.0.5) [1000 ports]
Increasing send delay for 10.2.0.5 from 0 to 50 due to max_successful_tryno incr
ease to 4
Increasing send delay for 10.2.0.5 from 50 to 100 due to max_successful_tryno in
crease to 5
Increasing send delay for 10.2.0.5 from 100 to 200 due to max_successful_tryno i
ncrease to 6
Increasing send delay for 10.2.0.5 from 200 to 400 due to 11 out of 15 dropped p
robes since last increase.
UDP Scan Timing: About 5.01% done; ETC: 11:45 (0:09:47 remaining)
Increasing send delay for 10.2.0.5 from 400 to 800 due to 11 out of 11 dropped p
robes since last increase.
UDP Scan Timing: About 7.79% done; ETC: 11:48 (0:12:02 remaining)
UDP Scan Timing: About 10.67% done; ETC: 11:49 (0:12:41 remaining)
user@pumpmonitor:~$
```

ACTIONS

Identification Measures (Incident Verified, Assessed, Options Evaluated):

On PumpPLC (10.2.0.5), we modified the firewall configuration with sudo iptables -A INPUT -p udp -j DROP to deny/drop all UDP packets, and confirmed the configuration is correct.



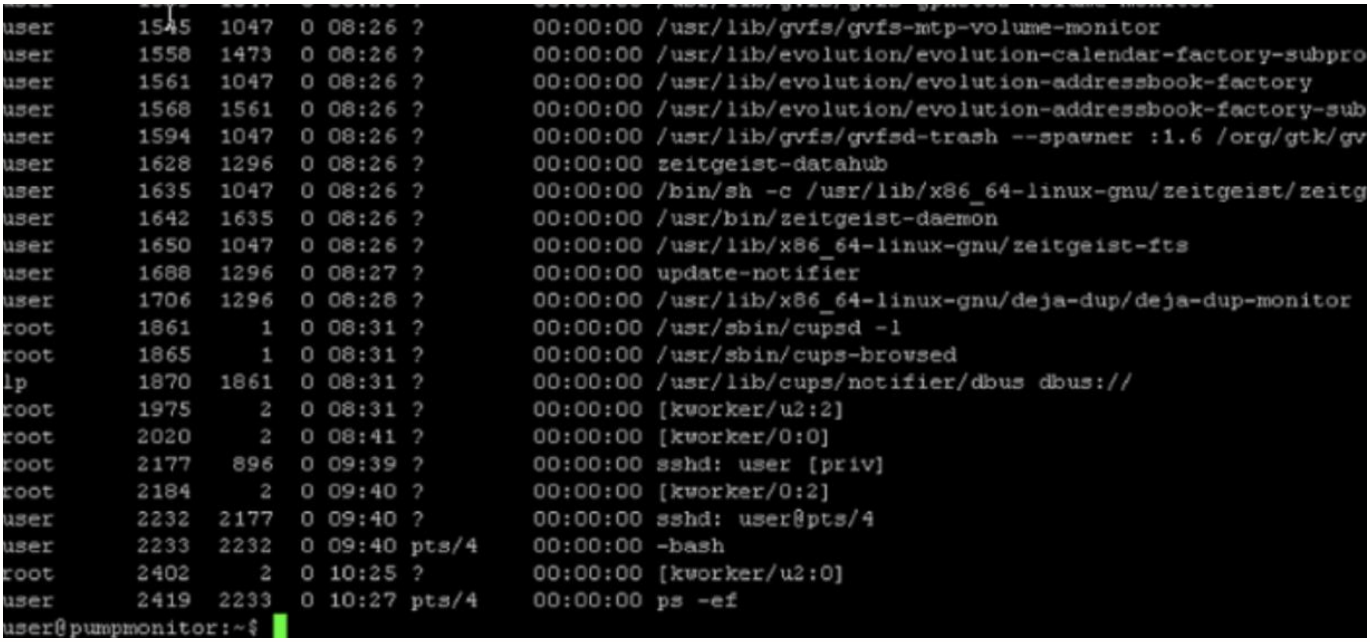
```
msfadmin@pumpplc:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       udp  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@pumpplc:~$
```

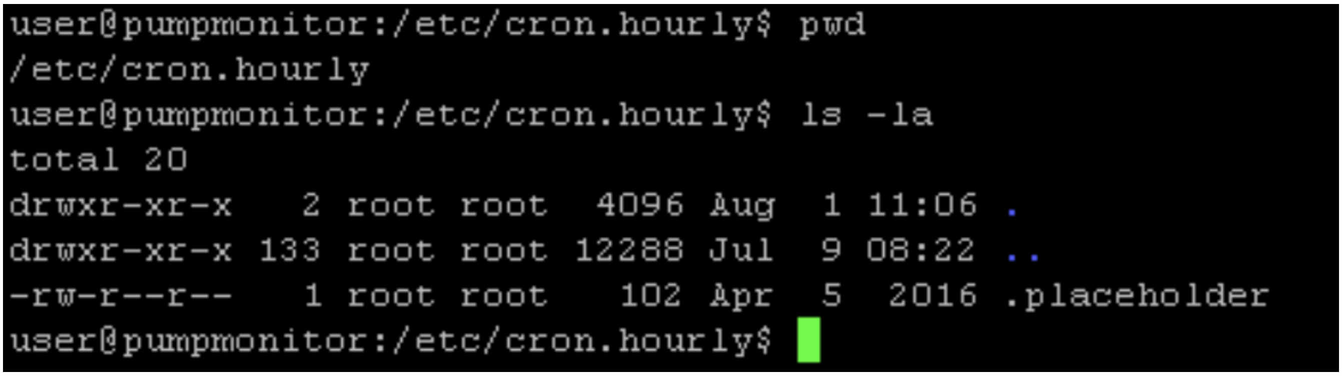
We mitigated the attack on PumpMonitor (10.2.0.6):

We killed the Scanner.sh and nmap processes and then ensured they are no longer running.



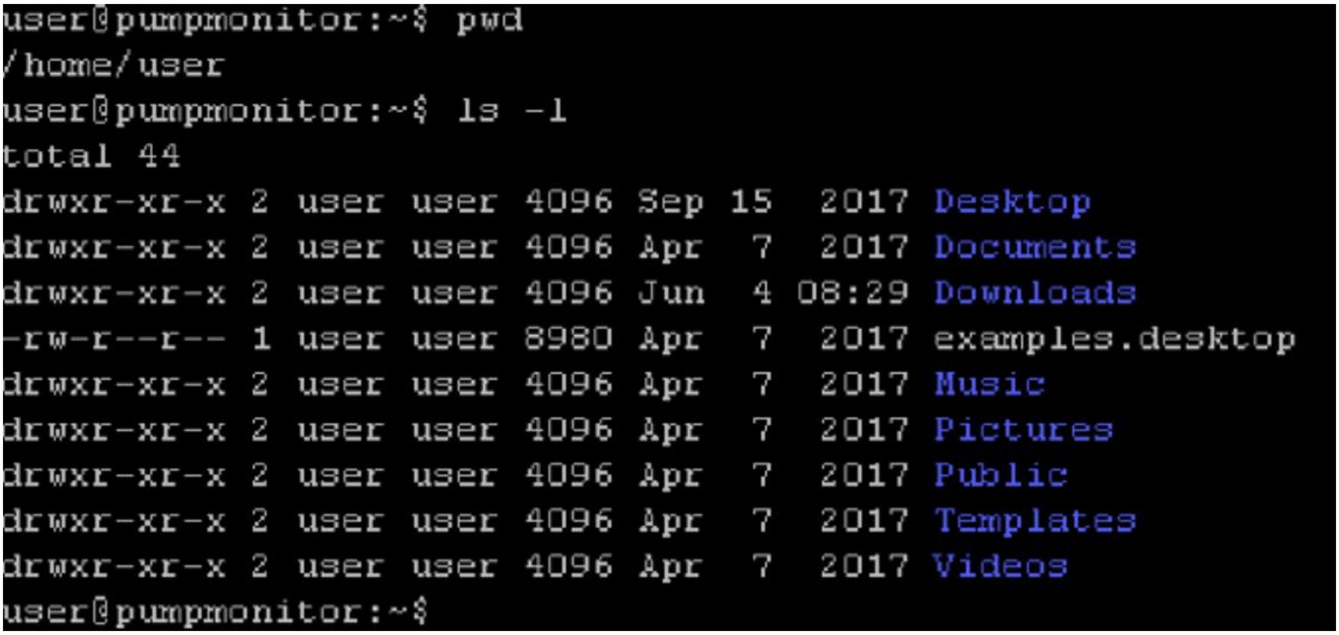
```
user      1545  1047  0 08:26 ?        00:00:00 /usr/lib/gvfs/gvfs-mtp-volume-monitor
user      1558  1473  0 08:26 ?        00:00:00 /usr/lib/evolution/evolution-calendar-factory-subpro
user      1561  1047  0 08:26 ?        00:00:00 /usr/lib/evolution/evolution-addressbook-factory
user      1568  1561  0 08:26 ?        00:00:00 /usr/lib/evolution/evolution-addressbook-factory-sub
user      1594  1047  0 08:26 ?        00:00:00 /usr/lib/gvfs/gvfsd-trash --spawner :1.6 /org/gtk/gv
user      1628  1296  0 08:26 ?        00:00:00 zeitgeist-datahub
user      1635  1047  0 08:26 ?        00:00:00 /bin/sh -c /usr/lib/x86_64-linux-gnu/zeitgeist/zeitg
user      1642  1635  0 08:26 ?        00:00:00 /usr/bin/zeitgeist-daemon
user      1650  1047  0 08:26 ?        00:00:00 /usr/lib/x86_64-linux-gnu/zeitgeist-fts
user      1688  1296  0 08:27 ?        00:00:00 update-notifier
user      1706  1296  0 08:28 ?        00:00:00 /usr/lib/x86_64-linux-gnu/deja-dup/deja-dup-monitor
root      1861     1  0 08:31 ?        00:00:00 /usr/sbin/cupsd -l
root      1865     1  0 08:31 ?        00:00:00 /usr/sbin/cups-browsed
lp        1870  1861  0 08:31 ?        00:00:00 /usr/lib/cups/notifier/dbus dbus://
root      1975     2  0 08:31 ?        00:00:00 [kworker/u2:2]
root      2020     2  0 08:41 ?        00:00:00 [kworker/0:0]
root      2177   896  0 09:39 ?        00:00:00 sshd: user [priv]
root      2184     2  0 09:40 ?        00:00:00 [kworker/0:2]
user      2232  2177  0 09:40 ?        00:00:00 sshd: user@pts/4
user      2233  2232  0 09:40 pts/4    00:00:00 -bash
root      2402     2  0 10:25 ?        00:00:00 [kworker/u2:0]
user      2419  2233  0 10:27 pts/4    00:00:00 ps -ef
user@pumpmonitor:~$
```

We deleted Scanner.sh script from the /etc/cron.hourly directory so that it cannot launch another attack.



```
user@pumpmonitor:/etc/cron.hourly$ pwd
/etc/cron.hourly
user@pumpmonitor:/etc/cron.hourly$ ls -la
total 20
drwxr-xr-x   2 root root  4096 Aug  1 11:06 .
drwxr-xr-x 133 root root 12288 Jul  9 08:22 ..
-rw-r--r--   1 root root   102 Apr  5  2016 .placeholder
user@pumpmonitor:/etc/cron.hourly$
```

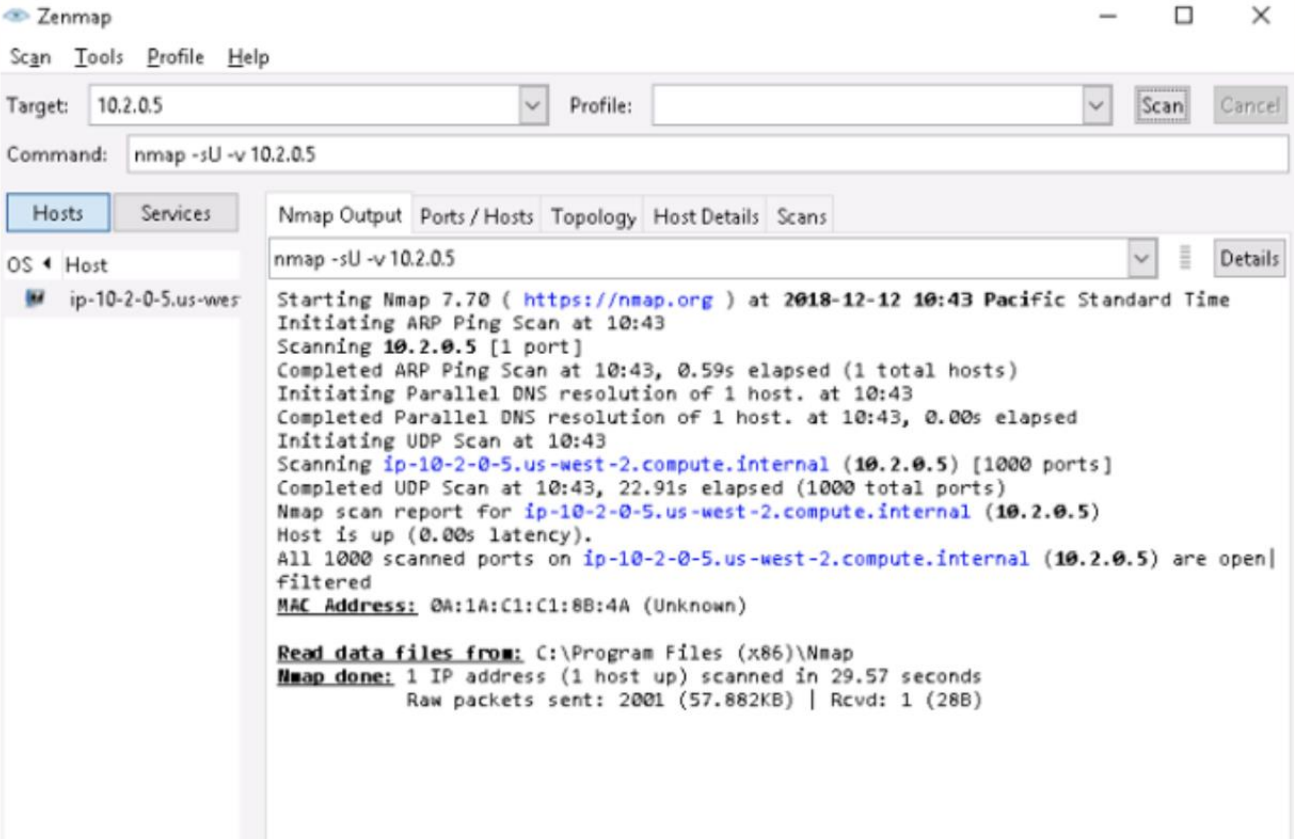
We removed the Scans.txt file from /home/user:



```
user@pumpmonitor:~$ pwd
/home/user
user@pumpmonitor:~$ ls -l
total 44
drwxr-xr-x 2 user user 4096 Sep 15  2017 Desktop
drwxr-xr-x 2 user user 4096 Apr  7  2017 Documents
drwxr-xr-x 2 user user 4096 Jun  4 08:29 Downloads
-rw-r--r-- 1 user user 8980 Apr  7  2017 examples.desktop
drwxr-xr-x 2 user user 4096 Apr  7  2017 Music
drwxr-xr-x 2 user user 4096 Apr  7  2017 Pictures
drwxr-xr-x 2 user user 4096 Apr  7  2017 Public
drwxr-xr-x 2 user user 4096 Apr  7  2017 Templates
drwxr-xr-x 2 user user 4096 Apr  7  2017 Videos
user@pumpmonitor:~$
```

We confirmed that the problems are fixed.

- First, on TargetWindows01, we ran a scan of PumpPLC to show that no UDP ports are open, and therefore, it is no longer vulnerable to UDP-based attacks.



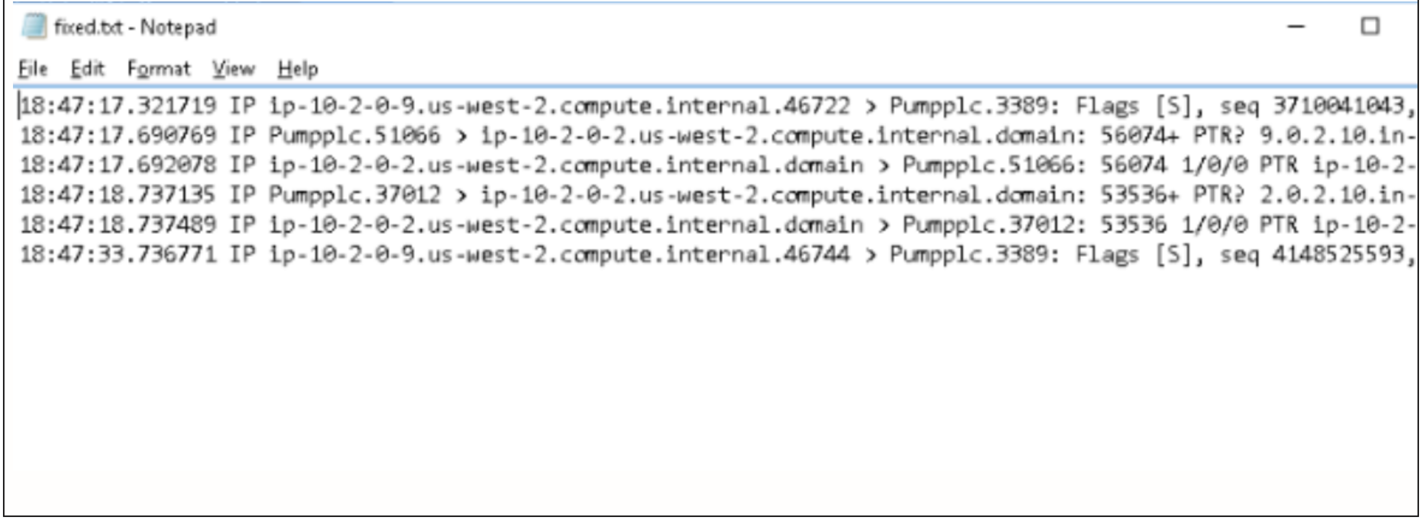
Target: 10.2.0.5

Command: nmap -sU -v 10.2.0.5

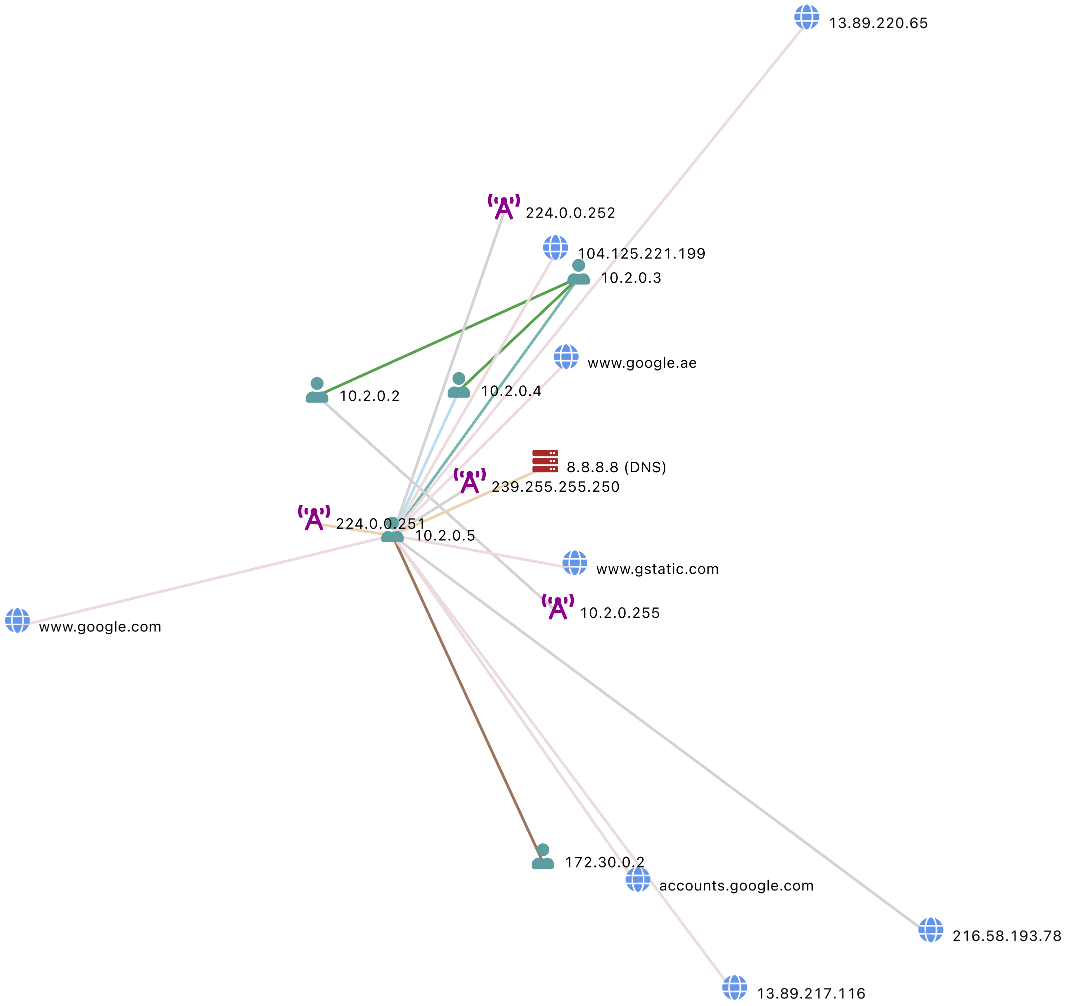
```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-12 10:43 Pacific Standard Time
Initiating ARP Ping Scan at 10:43
Scanning 10.2.0.5 [1 port]
Completed ARP Ping Scan at 10:43, 0.59s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:43
Completed Parallel DNS resolution of 1 host. at 10:43, 0.00s elapsed
Initiating UDP Scan at 10:43
Scanning ip-10-2-0-5.us-west-2.compute.internal (10.2.0.5) [1000 ports]
Completed UDP Scan at 10:43, 22.91s elapsed (1000 total ports)
Nmap scan report for ip-10-2-0-5.us-west-2.compute.internal (10.2.0.5)
Host is up (0.00s latency).
All 1000 scanned ports on ip-10-2-0-5.us-west-2.compute.internal (10.2.0.5) are open|
filtered
MAC Address: 0A:1A:C1:C1:8B:4A (Unknown)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 29.57 seconds
           Raw packets sent: 2001 (57.882KB) | Rcvd: 1 (28B)
```

Also on PumpPLC, we re-ran tcpdump to show there’s no network traffic on PumpMonitor (10.2.0.6) or PumpPLC (10.2.0.5). This confirms that PumpPLC is no longer under attack from UDP traffic, and PumpMonitor is not scanning any host.



```
18:47:17.321719 IP ip-10-2-0-9.us-west-2.compute.internal.46722 > Pumpplc.3389: Flags [S], seq 3710041043,
18:47:17.690769 IP Pumpplc.51066 > ip-10-2-0-2.us-west-2.compute.internal.domain: 56074+ PTR? 9.0.2.10.in-
18:47:17.692078 IP ip-10-2-0-2.us-west-2.compute.internal.domain > Pumpplc.51066: 56074 1/0/0 PTR ip-10-2-
18:47:18.737135 IP Pumpplc.37012 > ip-10-2-0-2.us-west-2.compute.internal.domain: 53536+ PTR? 2.0.2.10.in-
18:47:18.737489 IP ip-10-2-0-2.us-west-2.compute.internal.domain > Pumpplc.37012: 53536 1/0/0 PTR ip-10-2-
18:47:33.736771 IP ip-10-2-0-9.us-west-2.compute.internal.46744 > Pumpplc.3389: Flags [S], seq 4148525593,
```


13.89.220.65
224.0.0.252
104.125.221.199
10.2.0.3
www.google.ae
10.2.0.2
10.2.0.4
8.8.8.8 (DNS)
239.255.255.250
224.0.0.251
10.2.0.5
www.gstatic.com
10.2.0.255
www.google.com
172.30.0.2
accounts.google.com
216.58.193.78
13.89.217.116