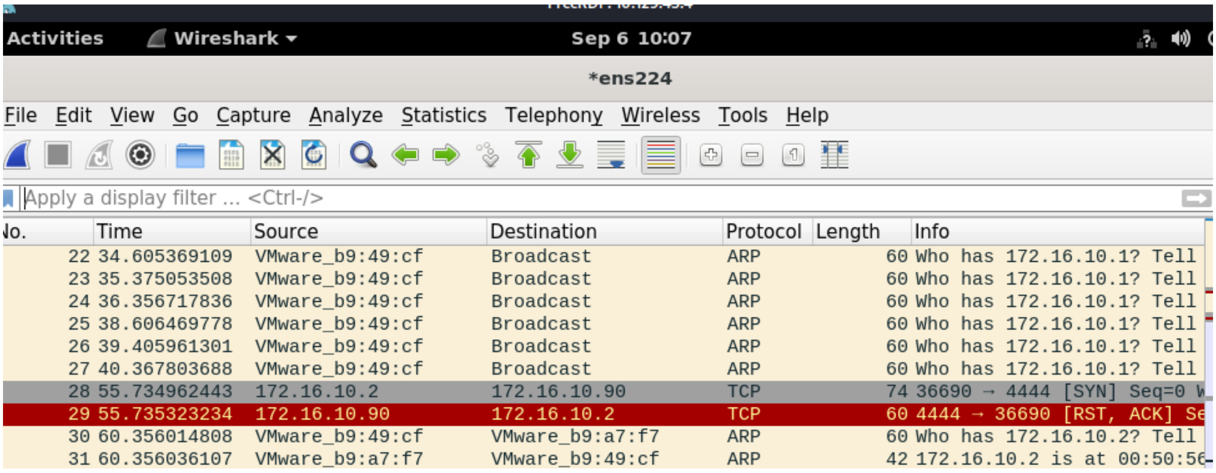
Rami Matouk

Analysis Workflow with Wireshark

One of our fellow admins noticed a weird connection from Bob's host when analyzing the baseline captures we have been gathering. He asked us to check it out and see what we think is happening.

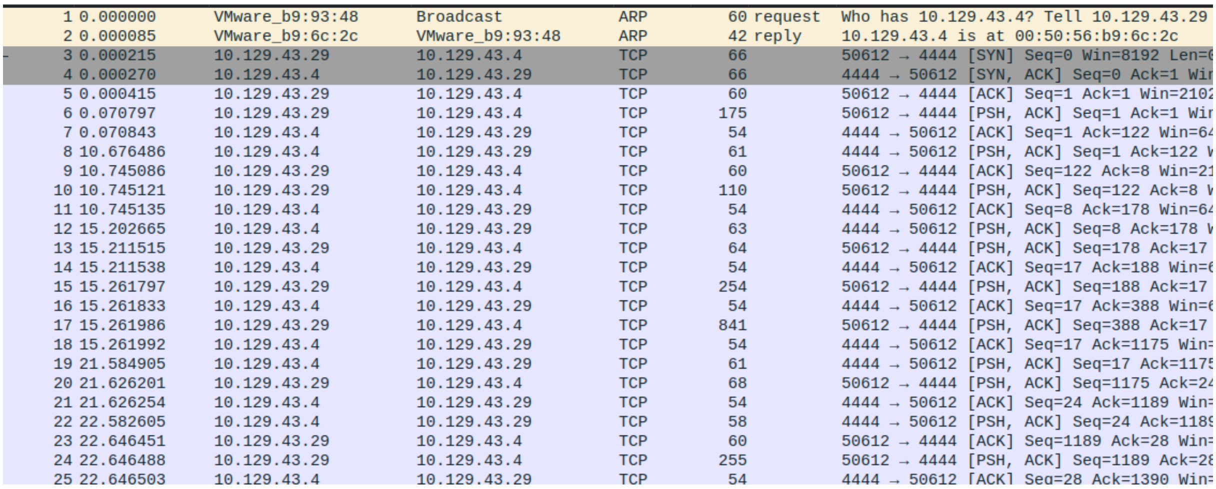
In this project we will practice analysis workflow template. We will follow this template to determine what is happening with the host.

1. **what is the issue?**
   a. a brief summary of the issue.
2. **define our scope and the goal (what are we looking for? which time period?)**
   a. **Scope**: We are looking for suspicious traffic activity from Bob's host ip == 10.129.43.4
   b. **when the issue started**: Within 48 hours
   c. **supporting info**: guided-analysis.pcap
3. **define our target(s) (net / host(s) / protocol)**
   a. Target hosts: host with ip == 10.129.43.4 and anyone with connection to it.
4. **capture network traffic / read from previously captured PCAP.**
   We are performing live capture of traffic from suspicious host. Possibly we will catch something in real time.


Activities
Wireshark ▾
Sep 6 10:07
*ens224
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

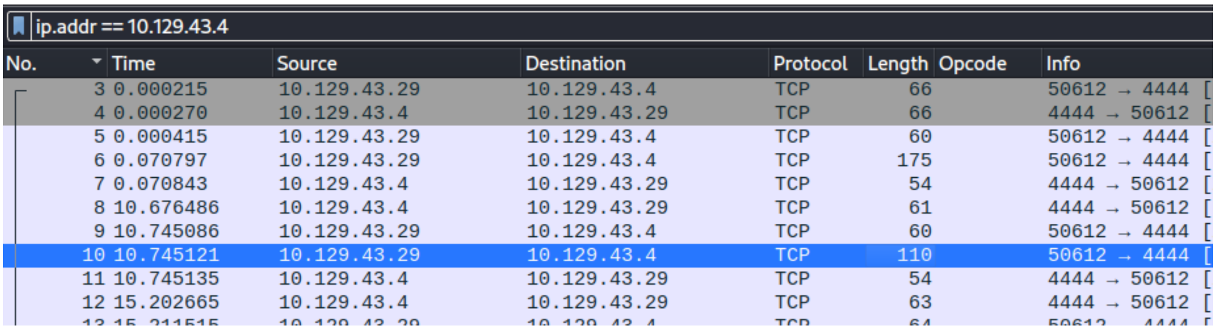
```
lo.  Time          Source            Destination       Protocol Length Info
  22 34.605369109  VMware_b9:49:cf   Broadcast         ARP          60 Who has 172.16.10.1? Tell
  23 35.375053508  VMware_b9:49:cf   Broadcast         ARP          60 Who has 172.16.10.1? Tell
  24 36.356717836  VMware_b9:49:cf   Broadcast         ARP          60 Who has 172.16.10.1? Tell
  25 38.606469778  VMware_b9:49:cf   Broadcast         ARP          60 Who has 172.16.10.1? Tell
  26 39.405961301  VMware_b9:49:cf   Broadcast         ARP          60 Who has 172.16.10.1? Tell
  27 40.367803688  VMware_b9:49:cf   Broadcast         ARP          60 Who has 172.16.10.1? Tell
  28 55.734962443  172.16.10.2       172.16.10.90      TCP          74 36690 → 4444 [SYN] Seq=0 W
  29 55.735323234  172.16.10.90      172.16.10.2       TCP          60 4444 → 36690 [RST, ACK] Se
  30 60.356014808  VMware_b9:49:cf   VMware_b9:a7:f7   ARP          60 Who has 172.16.10.2? Tell
  31 60.356036107  VMware_b9:a7:f7   VMware_b9:49:cf   ARP          42 172.16.10.2 is at 00:50:56
```

And loaded pre-captured pcap file on second machine.



```
 1 0.000000    VMware_b9:93:48  Broadcast        ARP    60 request  Who has 10.129.43.4? Tell 10.129.43.29
 2 0.000085    VMware_b9:6c:2c  VMware_b9:93:48  ARP    42 reply    10.129.43.4 is at 00:50:56:b9:6c:2c
 3 0.000215    10.129.43.29     10.129.43.4      TCP    66          50612 → 4444 [SYN] Seq=0 Win=8192 Len=
 4 0.000270    10.129.43.4      10.129.43.29     TCP    66          4444 → 50612 [SYN, ACK] Seq=0 Ack=1 Wir
 5 0.000415    10.129.43.29     10.129.43.4      TCP    60          50612 → 4444 [ACK] Seq=1 Ack=1 Win=2102
 6 0.070797    10.129.43.29     10.129.43.4      TCP   175          50612 → 4444 [PSH, ACK] Seq=1 Ack=1 Wir
 7 0.070843    10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=1 Ack=122 Win=64
 8 10.676486   10.129.43.4      10.129.43.29     TCP    61          4444 → 50612 [PSH, ACK] Seq=1 Ack=122 W
 9 10.745086   10.129.43.29     10.129.43.4      TCP    60          50612 → 4444 [ACK] Seq=122 Ack=8 Win=21
10 10.745121   10.129.43.29     10.129.43.4      TCP   110          50612 → 4444 [PSH, ACK] Seq=122 Ack=8 W
11 10.745135   10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=8 Ack=178 Win=64
12 15.202665   10.129.43.4      10.129.43.29     TCP    63          4444 → 50612 [PSH, ACK] Seq=8 Ack=178 W
13 15.211515   10.129.43.29     10.129.43.4      TCP    64          50612 → 4444 [PSH, ACK] Seq=178 Ack=17
14 15.211538   10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=17 Ack=188 Win=6
15 15.261797   10.129.43.29     10.129.43.4      TCP   254          50612 → 4444 [PSH, ACK] Seq=188 Ack=17
16 15.261833   10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=17 Ack=388 Win=6
17 15.261986   10.129.43.29     10.129.43.4      TCP   841          50612 → 4444 [PSH, ACK] Seq=388 Ack=17
18 15.261992   10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=17 Ack=1175 Win=
19 21.584905   10.129.43.4      10.129.43.29     TCP    61          4444 → 50612 [PSH, ACK] Seq=17 Ack=1175
20 21.626201   10.129.43.29     10.129.43.4      TCP    68          50612 → 4444 [PSH, ACK] Seq=1175 Ack=24
21 21.626254   10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=24 Ack=1189 Win=
22 22.582605   10.129.43.4      10.129.43.29     TCP    58          4444 → 50612 [PSH, ACK] Seq=24 Ack=1189
23 22.646451   10.129.43.29     10.129.43.4      TCP    60          50612 → 4444 [ACK] Seq=1189 Ack=28 Win=
24 22.646488   10.129.43.29     10.129.43.4      TCP   255          50612 → 4444 [PSH, ACK] Seq=1189 Ack=28
25 22.646503   10.129.43.4      10.129.43.29     TCP    54          4444 → 50612 [ACK] Seq=28 Ack=1390 Win=
```

5. **identification of required network traffic components (filtering)**
   We are interested in traffic related to host 10.129.43.4. So we will filter traffic unrelated to it.



ip.addr == 10.129.43.4

No.	Time	Source	Destination	Protocol	Length	Opcode	Info
3	0.000215	10.129.43.29	10.129.43.4	TCP	66		50612 → 4444 [
4	0.000270	10.129.43.4	10.129.43.29	TCP	66		4444 → 50612 [
5	0.000415	10.129.43.29	10.129.43.4	TCP	60		50612 → 4444 [
6	0.070797	10.129.43.29	10.129.43.4	TCP	175		50612 → 4444 [
7	0.070843	10.129.43.4	10.129.43.29	TCP	54		4444 → 50612 [
8	10.676486	10.129.43.4	10.129.43.29	TCP	61		4444 → 50612 [
9	10.745086	10.129.43.29	10.129.43.4	TCP	60		50612 → 4444 [
10	10.745121	10.129.43.29	10.129.43.4	TCP	110		50612 → 4444 [
11	10.745135	10.129.43.4	10.129.43.29	TCP	54		4444 → 50612 [
12	15.202665	10.129.43.4	10.129.43.29	TCP	63		4444 → 50612 [
13	15.211515	10.129.43.29	10.129.43.4	TCP	64		50612 → 4444 [

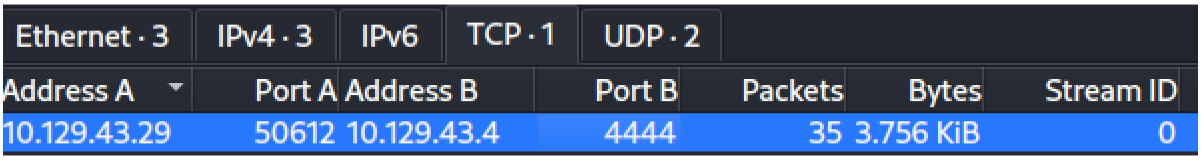
6. **An understanding of captured network traffic**

   Once we have filtered out the noise, it's time to dig for our targets. Start broad and close the circle around our scope.

7. **note taking / mind mapping of the found results.**

   Most noticable is vast amount of traffic related to port 4444 and port 50612

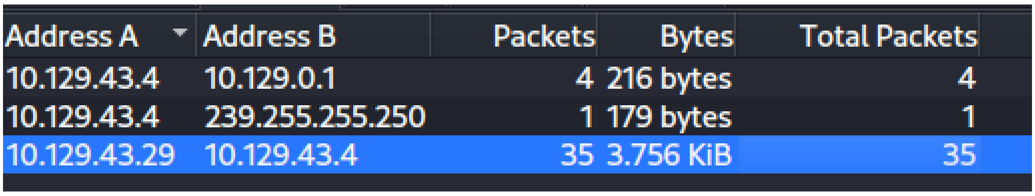
   This is conversations tab from Wireshark.



Ethernet · 3 | IPv4 · 3 | IPv6 | TCP · 1 | UDP · 2

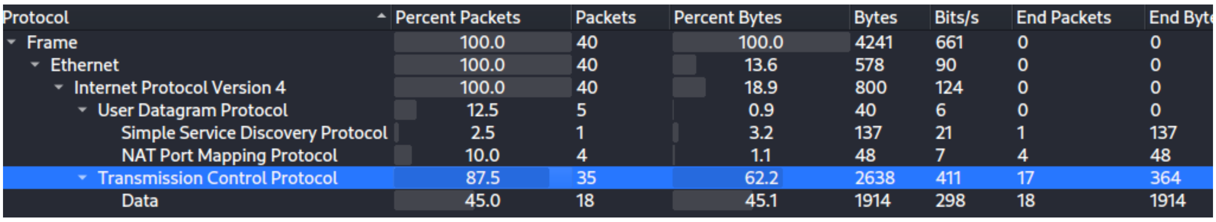
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID
10.129.43.29	50612	10.129.43.4	4444	35	3.756 KiB	0

In total we can notice 3 captured conversations with our target host.



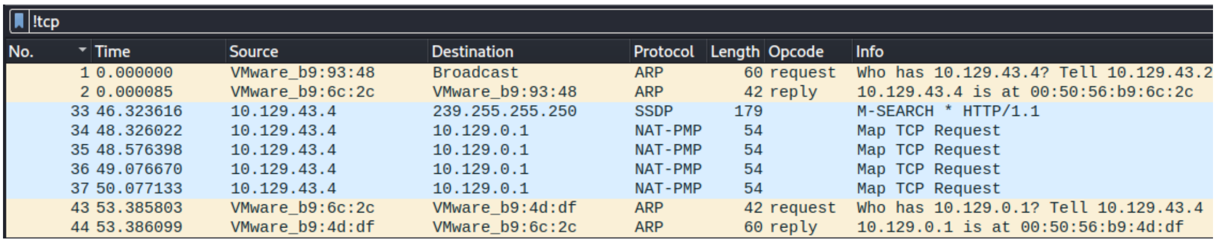
Address A	Address B	Packets	Bytes	Total Packets
10.129.43.4	10.129.0.1	4	216 bytes	4
10.129.43.4	239.255.255.250	1	179 bytes	1
10.129.43.29	10.129.43.4	35	3.756 KiB	35

This is protocol hierarchy statistics. We can see here that this PCAP is mostly TCP traffic, with a bit of UDP traffic.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Byt
Frame	100.0	40	100.0	4241	661	0	0
Ethernet	100.0	40	13.6	578	90	0	0
Internet Protocol Version 4	100.0	40	18.9	800	124	0	0
User Datagram Protocol	12.5	5	0.9	40	6	0	0
Simple Service Discovery Protocol	2.5	1	3.2	137	21	1	137
NAT Port Mapping Protocol	10.0	4	1.1	48	7	4	48
Transmission Control Protocol	87.5	35	62.2	2638	411	17	364
Data	45.0	18	45.1	1914	298	18	1914

Still this little amount of UDP communication is worth investigating first.

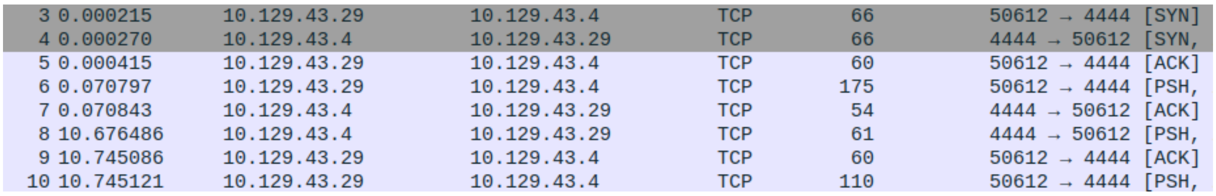


!tcp

No.	Time	Source	Destination	Protocol	Length	Opcode	Info
1	0.000000	VMware_b9:93:48	Broadcast	ARP	60	request	Who has 10.129.43.4? Tell 10.129.43.2
2	0.000085	VMware_b9:6c:2c	VMware_b9:93:48	ARP	42	reply	10.129.43.4 is at 00:50:56:b9:6c:2c
33	46.323616	10.129.43.4	239.255.255.250	SSDP	179		M-SEARCH * HTTP/1.1
34	48.326022	10.129.43.4	10.129.0.1	NAT-PMP	54		Map TCP Request
35	48.576398	10.129.43.4	10.129.0.1	NAT-PMP	54		Map TCP Request
36	49.076670	10.129.43.4	10.129.0.1	NAT-PMP	54		Map TCP Request
37	50.077133	10.129.43.4	10.129.0.1	NAT-PMP	54		Map TCP Request
43	53.385803	VMware_b9:6c:2c	VMware_b9:4d:df	ARP	42	request	Who has 10.129.0.1? Tell 10.129.43.4
44	53.386099	VMware_b9:4d:df	VMware_b9:6c:2c	ARP	60	reply	10.129.0.1 is at 00:50:56:b9:4d:df

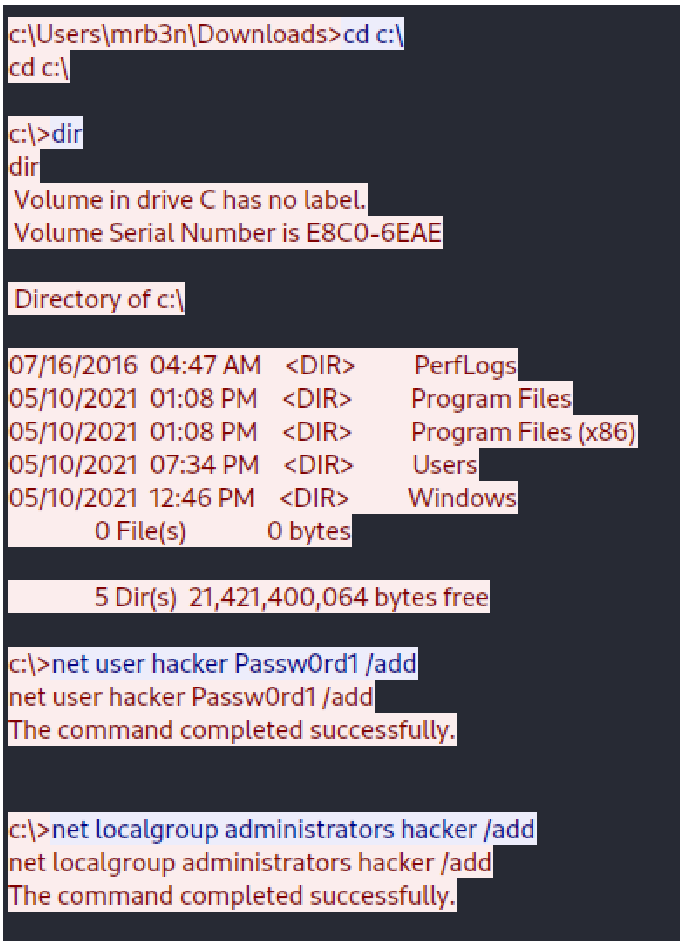
4 ARP packets, 4 NAT and 1 SSDP. This is normal traffic. Nothing abnormal.

Let’s investigate further TCP communication.

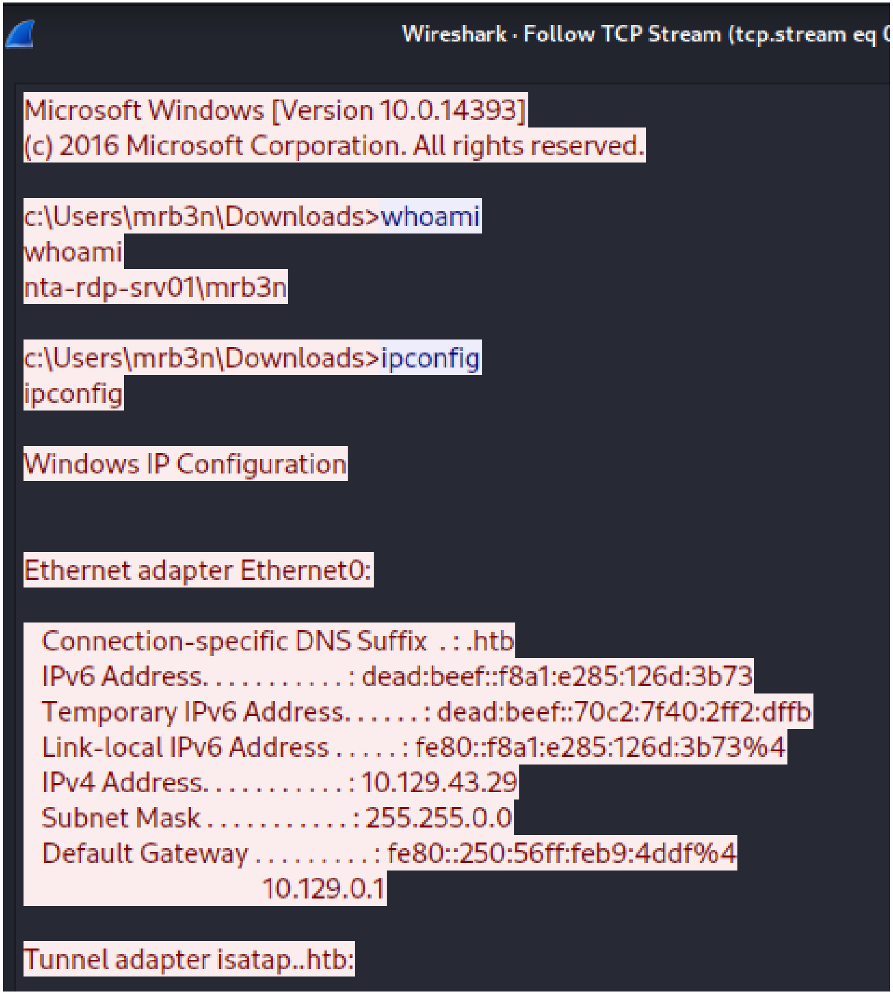


3	0.000215	10.129.43.29	10.129.43.4	TCP	66	50612 → 4444 [SYN]
4	0.000270	10.129.43.4	10.129.43.29	TCP	66	4444 → 50612 [SYN,
5	0.000415	10.129.43.29	10.129.43.4	TCP	60	50612 → 4444 [ACK]
6	0.070797	10.129.43.29	10.129.43.4	TCP	175	50612 → 4444 [PSH,
7	0.070843	10.129.43.4	10.129.43.29	TCP	54	4444 → 50612 [ACK]
8	10.676486	10.129.43.4	10.129.43.29	TCP	61	4444 → 50612 [PSH,
9	10.745086	10.129.43.29	10.129.43.4	TCP	60	50612 → 4444 [ACK]
10	10.745121	10.129.43.29	10.129.43.4	TCP	110	50612 → 4444 [PSH,

TCP Port 4444 is a default listener port for Metasploit which may suggest that we are dealing with shell communication. Lets follow TCP stream.



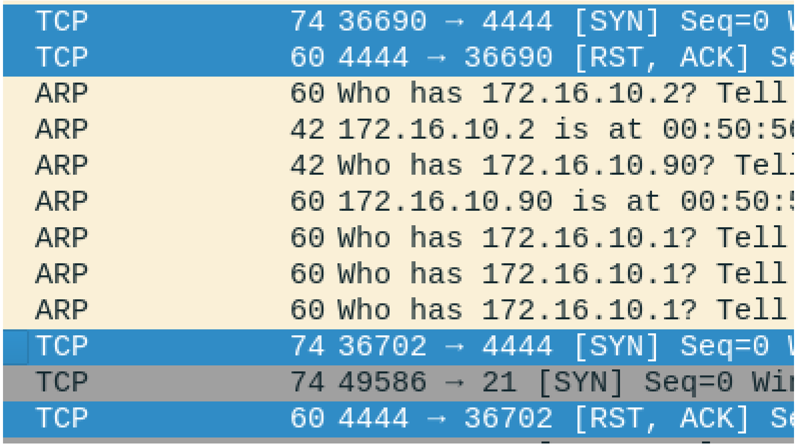
```
c:\Users\mrb3n\Downloads>cd c:\
cd c:\

c:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E8C0-6EAE

 Directory of c:\

07/16/2016  04:47 AM    <DIR>          PerfLogs
05/10/2021  01:08 PM    <DIR>          Program Files
05/10/2021  01:08 PM    <DIR>          Program Files (x86)
05/10/2021  07:34 PM    <DIR>          Users
05/10/2021  12:46 PM    <DIR>          Windows
               0 File(s)              0 bytes

               5 Dir(s)  21,421,400,064 bytes free

c:\>net user hacker Passw0rd1 /add
net user hacker Passw0rd1 /add
The command completed successfully.


c:\>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.
```



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\Users\mrb3n\Downloads>whoami
whoami
nta-rdp-srv01\mrb3n

c:\Users\mrb3n\Downloads>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::f8a1:e285:126d:3b73
   Temporary IPv6 Address. . . . . . : dead:beef::70c2:7f40:2ff2:dffb
   Link-local IPv6 Address . . . . . : fe80::f8a1:e285:126d:3b73%4
   IPv4 Address. . . . . . . . . . . : 10.129.43.29
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:4ddf%4
                                       10.129.0.1

Tunnel adapter isatap..htb:
```

1. We can notice that someone was doing basic recon. Using whoami, and ipconfig commands he could determine his privileges and position in network.
2. Then he moved through system and discovered files and directories contained in device.
3. Biggest alarm bell is creation of new administrator account called **Hacker**.

Let’s return to real time capture. We can notice another communication via port 4444. We can’t be sure that this is another malicious communication but considering that pre-captured pcap had malicious TCP communication via port 4444 we can be suspicious of this attempt.



```
TCP        74 36690 → 4444 [SYN] Seq=0 W
TCP        60 4444 → 36690 [RST, ACK] Se
ARP        60 Who has 172.16.10.2? Tell
ARP        42 172.16.10.2 is at 00:50:5
ARP        42 Who has 172.16.10.90? Tel
ARP        60 172.16.10.90 is at 00:50:
ARP        60 Who has 172.16.10.1? Tell
ARP        60 Who has 172.16.10.1? Tell
ARP        60 Who has 172.16.10.1? Tell
TCP        74 36702 → 4444 [SYN] Seq=0 W
TCP        74 49586 → 21 [SYN] Seq=0 Wi
TCP        60 4444 → 36702 [RST, ACK] Se
```

8. **summary of the analysis (what did we find?)**

Our analysis determined that host 10.129.43.29 communicated with host 10.129.43.4 that included executing of commands. Host performed recon operations and then proceeded to create new account with privileges of administrator called **hacker** via net commands. It looks like someone used Bob’s device to perform these actions. Live capture suggest another attempts to communicate via port 4444 that was used in previously mentioned communication

It is our opinion to complete Incident Response procedure to ensure that threat is stopped from spreading further.

This concludes this lab exercises. Thanks for reading and I hope you found the information here useful.

Source: https://academy.hackthebox.com/module/81/section/962