### **Network Analysis — Web Shell**

This is a walkthrough of the Network Analysis — Web Shell challenge in Blue Team Labs Online platform.

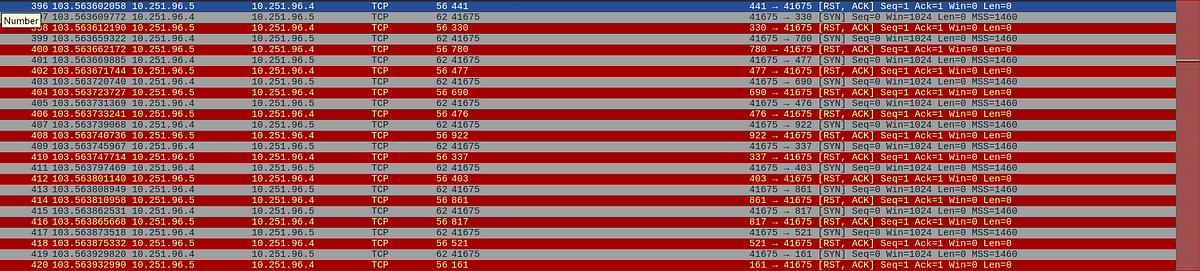
**Scenario:** The SOC received an alert in their SIEM for ‘Local to Local Port Scanning’ where an internal private IP began scanning another internal system.

**Investigation file:** BTLOPortscan.pcap

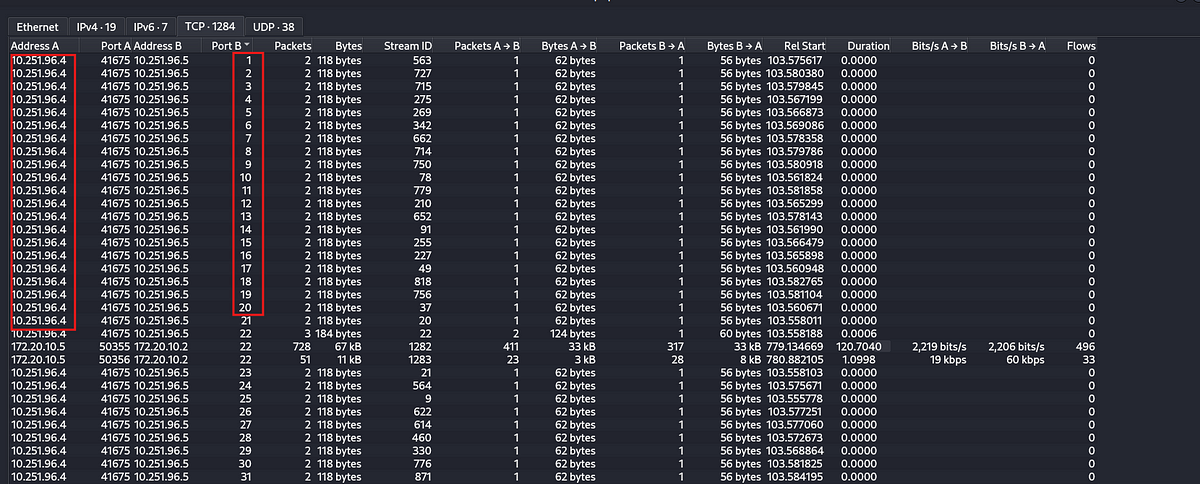
#### **Tasks:**

**1.What is the IP responsible for conducting the port scan activity?**

This we can check for the typical behavior of a port scan where the attacker sends a SYN packet to the victims computer and the victim computer sends a [SYN, ACK] packet to the attacker if it is open and ready to accept the connection. If the port is closed then the victims computer sends a [RST, ACK] response. We can look for multiple SYN requests followed by multiple [RST, ACK] responses to find out the answer.

pcap showing the port scan activity

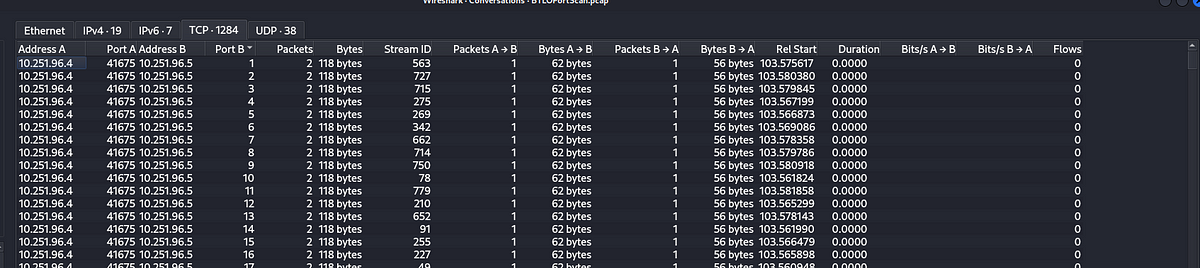
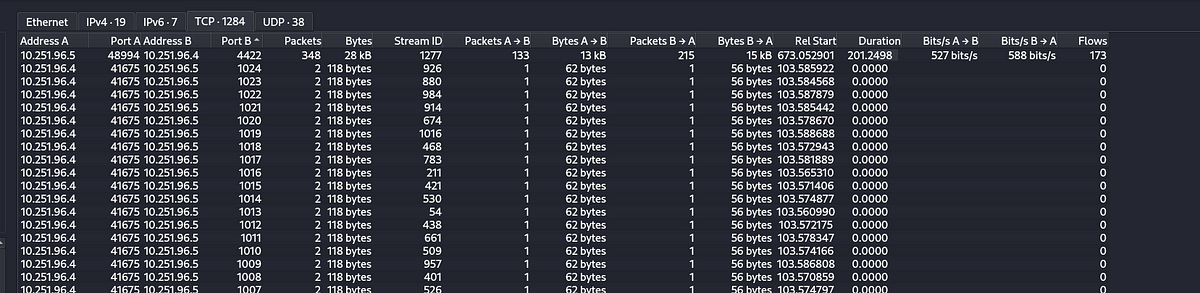
Alternatively we can find this in wireshark->statistics->conversations->TCP

TCP conversations showing port scan activity.

**Answer:** 10.251.96.4

**2.What is the port range scanned by the suspicious host?**

For this we can sort the conversations based on the destination port in ascending to see the first port scanned by the attacker and in descending to see the last port scanned by the attacker.

TCP conversations showing the starting port.TCP conversations showing the ending port.

**Answer:** 1–1024

**3.What is the type of port scan conducted?**

As explained in the question 1 this is a SYN scan as the attacker sends TCP SYN packets to multiple ports of the victim.

**Answer:** TCP SYN

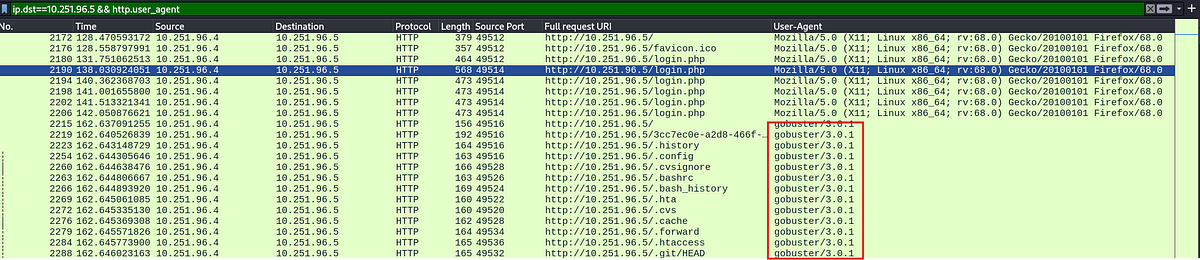
**4.Two more tools were used to perform reconnaissance against open ports, what were they?**

To answer this we can check for the user agent string in packets. An user agent string is a line of text that a client software such as a tool or browser sends to the web server when making a request.

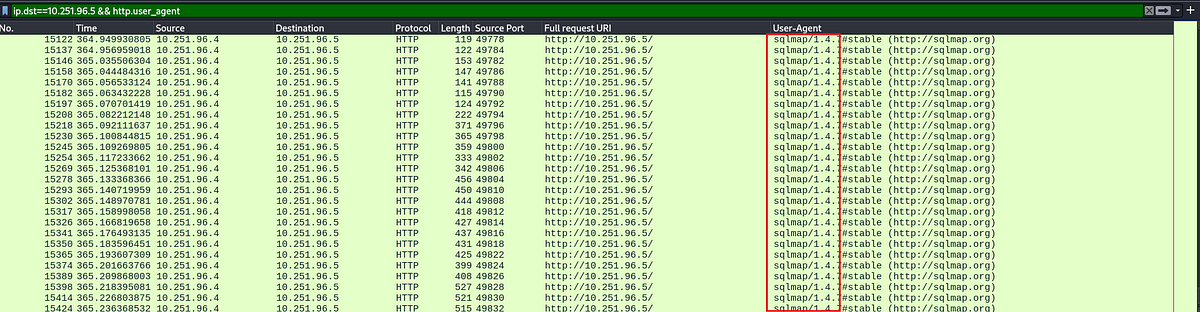
So in this scenario I filtered the packets that have the destination as the victims IP which is 10.251.96.5 and search for packets which had the user agent string.

Filter: ip.dst==10.251.96.5 && http.user\_agent

Immediately I can see a tool called gobuster which is a directory enumeration tool used for web reconnaissance to find out the subdomains in a website.

filtered packets indicating gobuster usage.

If we scroll down we can see another tool called sqlmap. sqlmap is a tool used in detecting and exploiting sql injection, a common vulnerability found in web applications.

filtered packets indicating sqlmap usage.

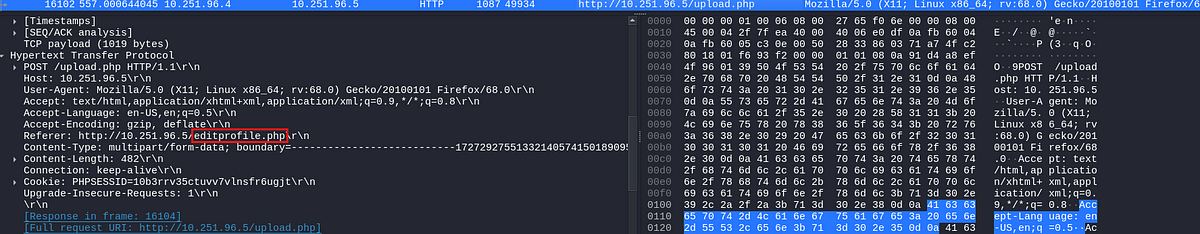
**Answer:** Gobuster 3.0.1, sqlmap 1.4.7

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

For this we can filter for the http post request made from the attacker machine to the victims machine.

Filter: (ip.src==10.251.96.4 && ip.dst==10.251.96.5) && http.request.method==POST

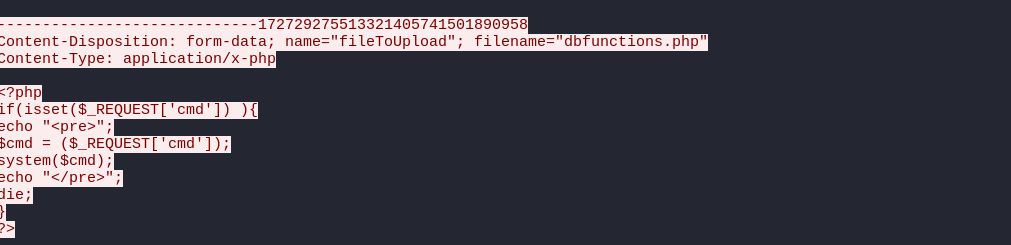
If we scroll down we can see a request to “upload.php”, if we look at the contents of the packet we can find the name of the file uploaded.

file upload

**Answer:** editprofile.php

**6.What is the name of the web shell that the attacker uploaded?**

To answer this question we can select the above packet and follow the TCP stream, which will let us view the entire conversation between the hosts.

user upload file.

In the above screenshot we can see that the user uploaded a file called dbfunctions.php which lets the user execute commands in a shell.

**Answer:** dbfunctions.php

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

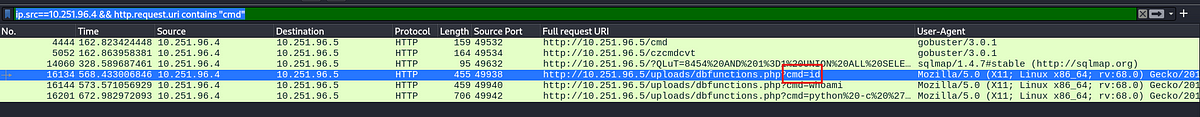
This is evident from the above screenshot. The code checks if the cmd parameter is set in the incoming request and if the parameter is set then it uses <pre> to preserve the formatting of the request. Then it retrieves the command and executes with system.

**Answer:** cmd

**8.What is the first command executed by the attacker?**

Now that we know that the attacker is using cmd parameter to send commands to the victim we can filter on the http request uri and the source or destination ip address.

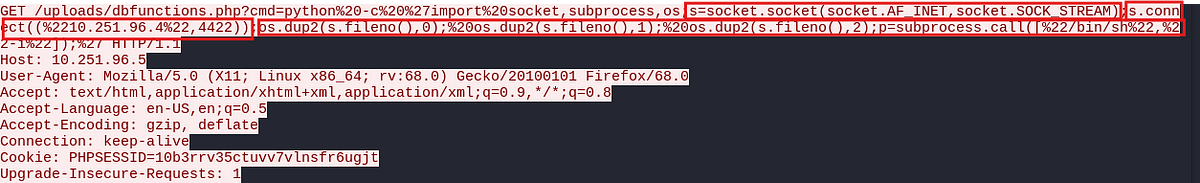
**Filter:** ip.src==10.251.96.4 && http.request.uri contains “cmd”

http request containing cmd

**Answer:** id

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

we can see the other commands executed by the attacker to figure this out. there is a python script being passed, by looking at the python script it is creating a reverse shell to the attackers machine on port 4422.

reverse shell code uploaded by the attacker

**Answer:** Reverse

**10.What is the port he uses for the shell connection?**

This can be seen in the above screenshot

**Answer:** 4422

This is the end of the investigation.