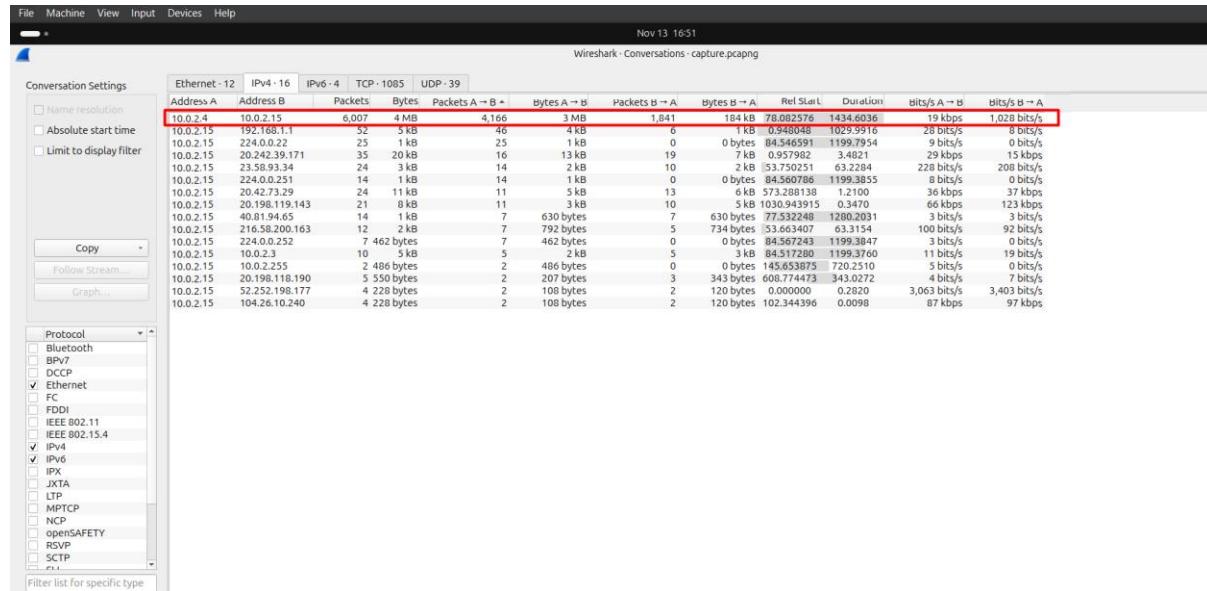


ASPX reverse shell via SMB

In this pcap file, we can see that ASPX reverse shell was planted via SMB protocol.

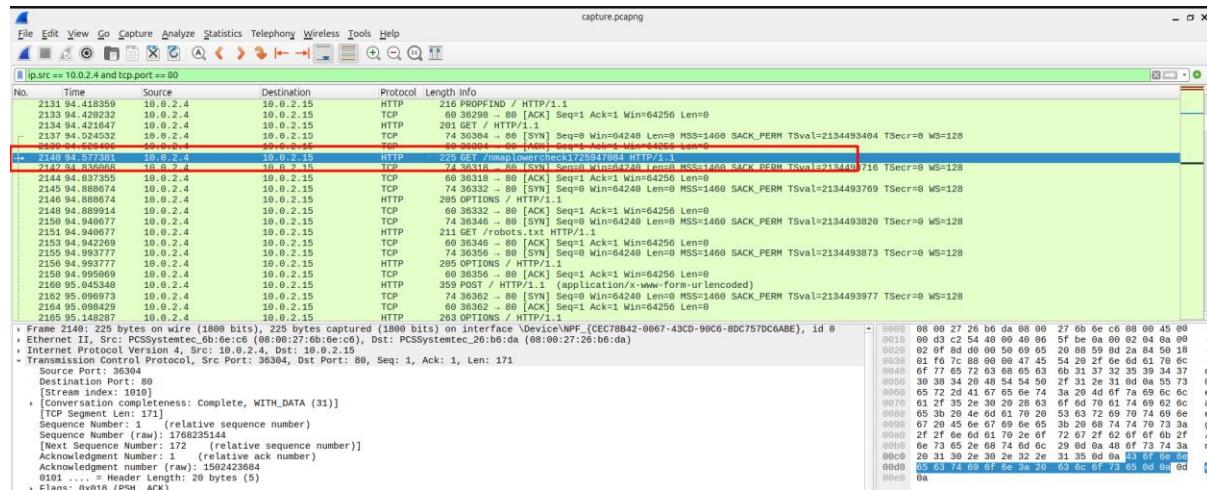
First step of investigating the pcap file, we have filtered the IP addresses in wireshark as:



Lots of conversation is happening between these two IP addresses, so let's search our filter.

Filter: ip.src == 10.0.2.4 and tcp.port == 80

By applying this filter, we can see nmap, which is popular tool for network discovery and security auditing. By this we can see all the open ports in the target host. It finds the open services like SMP, HTTP or reverse shell paths.



ASPX reverse shell via SMB

The screenshot shows the MITRE ATT&CK website. The navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and Blog. A search bar is also present. The main content area displays the 'Network Service Discovery' technique under the 'Enterprise' section. The page includes a detailed description of the technique, its sub-techniques (none), platforms (Containers, IaaS, Linux, Network Devices, Windows, macOS), contributors (Aaron Sullivan aka ZerkerEOD, Praetorian), version (3.2), and creation date (31 May 2017). A red box highlights the title 'Network Service Discovery'.

So, the source address 10.0.2.4 is scanning the web server 10.0.2.15. This is attacker is requesting <http://10.0.2.15/nmaplowercheck1725947084> and in response the server is giving 404 Not found.

The screenshot shows a Wireshark capture of an HTTP stream. The request is a GET to 'nmaplowercheck1725947084'. The response is a 404 Not Found from Microsoft-IIS/10.0, indicating that the file or directory was not found. The response body contains an ASPX page with a header and a style block. A red box highlights the 404 response.

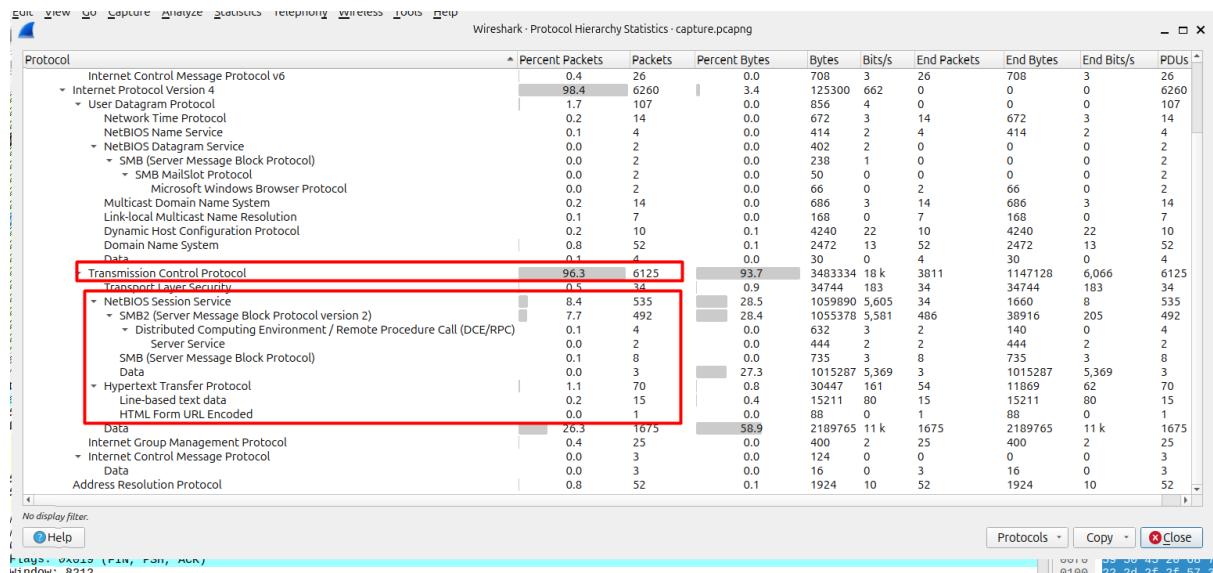
```
GET /nmaplowercheck1725947084 HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
Host: 10.0.2.15
Connection: close

HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Tue, 10 Sep 2024 05:44:49 GMT
Connection: close
Content-Length: 1245

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
```

Exploring the protocol involved.

ASPX reverse shell via SMB



In the protocol hierarchy. SMB2 is there so, filtering with SMB2

ip.src == 10.0.2.4 && smb2

No.	Time	Source	Destination	Protocol	Length Info
2388	137.932590	10.0.2.4	10.0.2.15	SMB2	238 Negotiate Protocol Request
2397	138.041167	10.0.2.4	10.0.2.15	SMB2	238 Negotiate Protocol Request
2618	239.339908	10.0.2.4	10.0.2.15	SMB2	284 Negotiate Protocol Request
2622	240.674813	10.0.2.4	10.0.2.15	SMB2	220 Session Setup Request, NTLMSP_NEGOTIATE
2626	240.674817	10.0.2.4	10.0.2.15	SMB2	162 Tree Connect Request Tree: \\10.0.2.15\IPC\$
2629	240.778552	10.0.2.4	10.0.2.15	SMB2	162 Tree Connect Request Tree: \\10.0.2.15\IPC\$
2631	240.788624	10.0.2.4	10.0.2.15	SMB2	162 Tree Connect Request Tree: \\10.0.2.15\IPC\$
2633	240.821279	10.0.2.4	10.0.2.15	DCERPC	250 Bind: call_id: 1, Fragment: Single, 1 context items: SRVSVC V3.0 (32bit NDR)
2636	240.874425	10.0.2.4	10.0.2.15	SRVSVC	270 NetShareEnumAll request
2639	240.882214	10.0.2.4	10.0.2.15	SMB2	146 Close Request File: srvsvc
2641	240.885198	10.0.2.4	10.0.2.15	SMB2	126 Tree Disconnect Request
2666	263.287025	10.0.2.4	10.0.2.15	SMB2	284 Negotiate Protocol Request
2668	263.293534	10.0.2.4	10.0.2.15	SMB2	220 Session Setup Request, NTLMSP_NEGOTIATE
2670	263.297878	10.0.2.4	10.0.2.15	SMB2	580 Session Setup Request, NTLMSP_AUTH, User: WORKGROUP\root
2672	263.304625	10.0.2.4	10.0.2.15	SMB2	162 Tree Connect Request Tree: \\10.0.2.15\IPC\$
2674	263.304627	10.0.2.4	10.0.2.15	SMB2	222 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\10.0.2.15\Documents
2676	263.308940	10.0.2.4	10.0.2.15	SMB2	172 Tree Connect Request Tree: \\10.0.2.15\Documents
2678	263.312045	10.0.2.4	10.0.2.15	SMB2	172 Tree Connect Request Tree: \\10.0.2.15\Documents
2681	263.449229	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
2684	265.805134	10.0.2.4	10.0.2.15	SMB2	179 Create Request File:
2687	265.897184	10.0.2.4	10.0.2.15	SMB2	156 Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
2689	265.810289	10.0.2.4	10.0.2.15	SMB2	156 Find Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
2691	265.815482	10.0.2.4	10.0.2.15	SMB2	146 Close Request File:
2693	265.817348	10.0.2.4	10.0.2.15	SMB2	179 Create Request File:
2695	265.822787	10.0.2.4	10.0.2.15	SMB2	163 GetInfo Request FS_INFO/FileFsSizeInformation File:
2697	265.826204	10.0.2.4	10.0.2.15	SMB2	146 Close Request File:
2701	267.26747856	10.0.2.4	10.0.2.15	SMB2	126 Keepalive Request
2702	272.389369	10.0.2.4	10.0.2.15	SMB2	179 Create Request File:
2707	272.394643	10.0.2.4	10.0.2.15	SMB2	162 KeepAlive Request
2709	272.402711	10.0.2.4	10.0.2.15	SMB2	146 Close Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
2711	272.415608	10.0.2.4	10.0.2.15	SMB2	146 Close Request File: SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
2714	272.932287	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
2768	327.835747	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
2773	339.894727	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
2778	337.991332	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
2783	342.482279	10.0.2.4	10.0.2.15	SMB2	198 Create Request File: shell.aspx
3505	342.611215	10.0.2.4	10.0.2.15	SMB2	494 Write Request Len:1015024 Off:0 File: shell.aspx
3509	342.614219	10.0.2.4	10.0.2.15	SMB2	146 Close Request File: shell.aspx
3514	342.919228	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
3517	347.804043	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
3523	352.846514	10.0.2.4	10.0.2.15	SMB2	126 Keepalive Request
3526	357.907498	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
3531	362.872570	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request
3534	367.918896	10.0.2.4	10.0.2.15	SMB2	126 KeepAlive Request

Establishment of tree connect request

- When a windows client wants to access a share on a remote machine via SMB, it first sends a tree request to specify the share it want to access.
- \\\10.0.2.15\IPC\$ → the **administrative IPC share**, often used for remote management and named pipes.

ASPX reverse shell via SMB

- \\10.0.2.15\Documents → a **regular document share**, where the attacker is trying to store the malicious file.

Along with that, there is a create / write request.

Once connected to the share:

- **Create Request** → tells the SMB server:

"I want to create a new file named shell.aspx."

- **Write Request** → actually **writes the content** of the file (your malicious ASPX shell) into the newly created file on the server.

After the write, the malicious file now exists on the server: Documents\shell.aspx.

Port used:

ip.src == 10.0.2.15 && ip.dst == 10.0.2.4 && tcp.flags.syn == 1 && tcp.flags.ack == 0

SYN flag is set to 1 → this packet is **trying to start a new TCP connection**

ACK flag is 0 → the packet is **not a reply**; it's the first packet in the handshake. This is the **very first message from the server to the attacker** when opening the connection.

ip.src == 10.0.2.15 && ip.dst == 10.0.2.4 && tcp.flags.syn == 1 && tcp.flags.ack == 0						
No.	Time	Source	Destination	Protocol	Length	Info
3585	401.496667	10.0.2.15	10.0.2.4	TCP	66	49688 → 4443 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

443 listening port number is used by attacker for the reverse shell.

Execution:

Once the malicious shell.aspx is on the server:

- The attacker can access it via HTTP on the webserver (or IIS) by navigating to <http://10.0.2.15/Documents/shell.aspx>.
- When visited, the shell executes code on the server —, it sets up a **reverse shell**.

ASPX reverse shell via SMB

- Then the server initiates an **outbound TCP connection** to the attacker, connecting to the attacker's listening port.

Inside of shell.aspx

Certainly, this is a malicious shell execution code

Steps Involved:

1. SMB Access: Tree Connect Request → connects to Documents share
 2. Planting Shell: Create Request + Write Request → uploads shell.aspx
 3. Triggering Shell: HTTP request to shell.aspx → executes malicious code
 4. Reverse Shell Connections: Server (10.0.2.15) initiates TCP connection → attacker (10.0.2.4) listening port.