Site Book - Team Alpha

Joe Abbate, Ryan Schanzenbacher, Vijayavarman Arunasalam Harikrishnan

Team Topology

Visual Topology

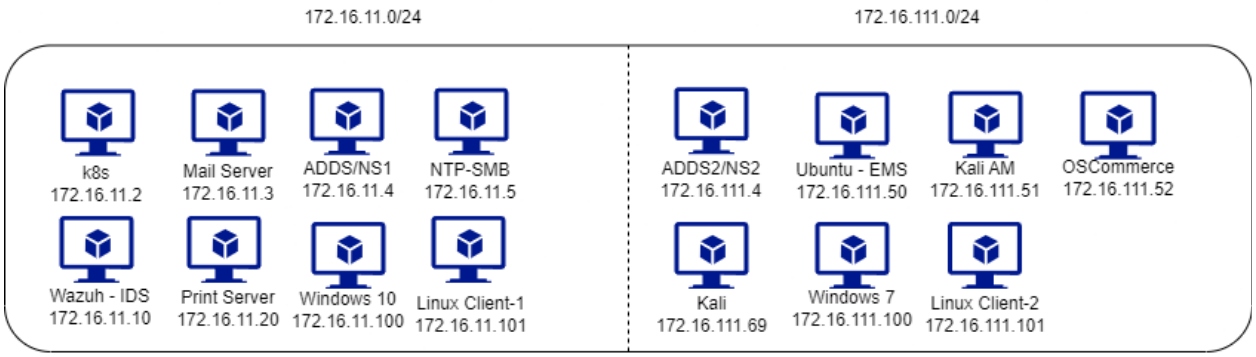


Table of Services

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
172.16.111.20	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)

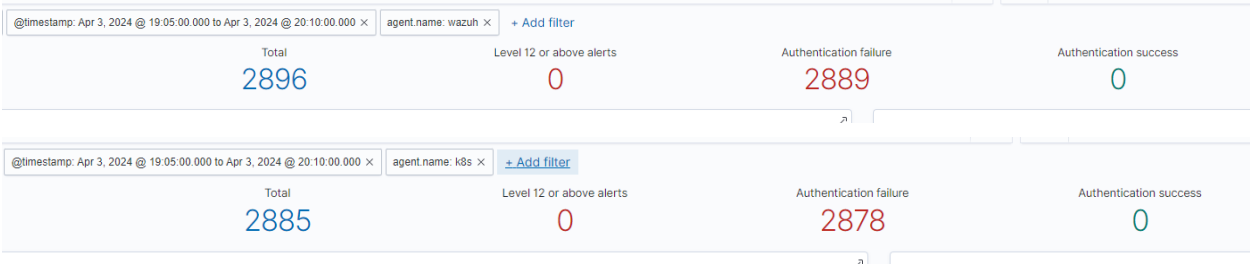
This vulnerability impacted Windows 7's RDP server. By executing the correct steps, one can obtain remote code execution through this server.

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

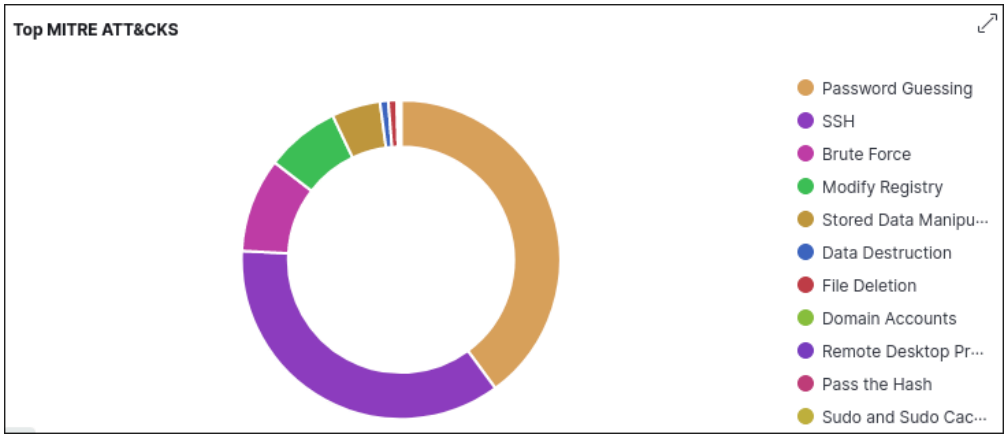
This vulnerability was a standard virtual print server that accepts print jobs without performing any kind of authentication or IP verification

Attack Detections

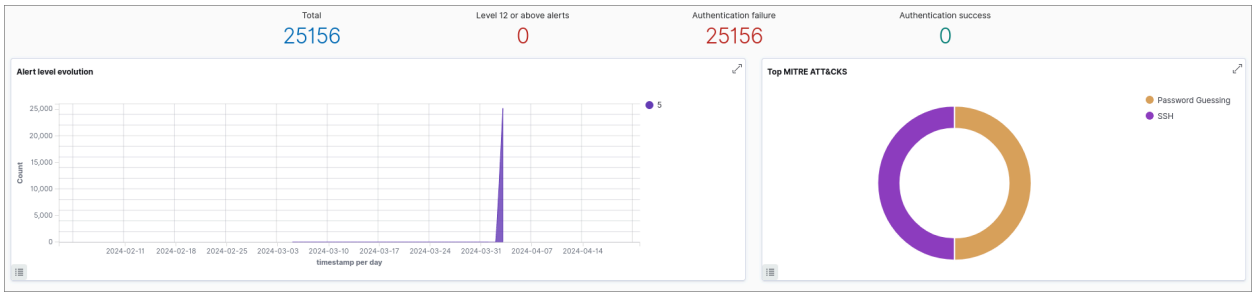
Overall, Wazuh detected no direct infiltration of systems during the event.

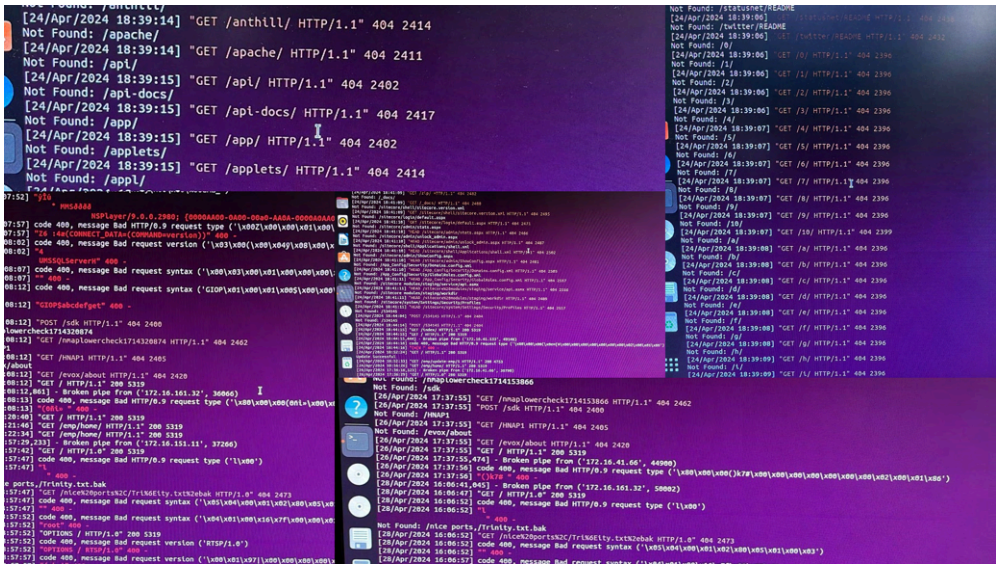


It did detect an attempted brute force attempt against the "wazuh" and "k8s" systems during April 3, 2024 from 7:05p to 8:10p during which ~2900 login attempts were made on both systems. No successful login was made.
Overall, the largest class of attacks detected during the competition was password spraying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

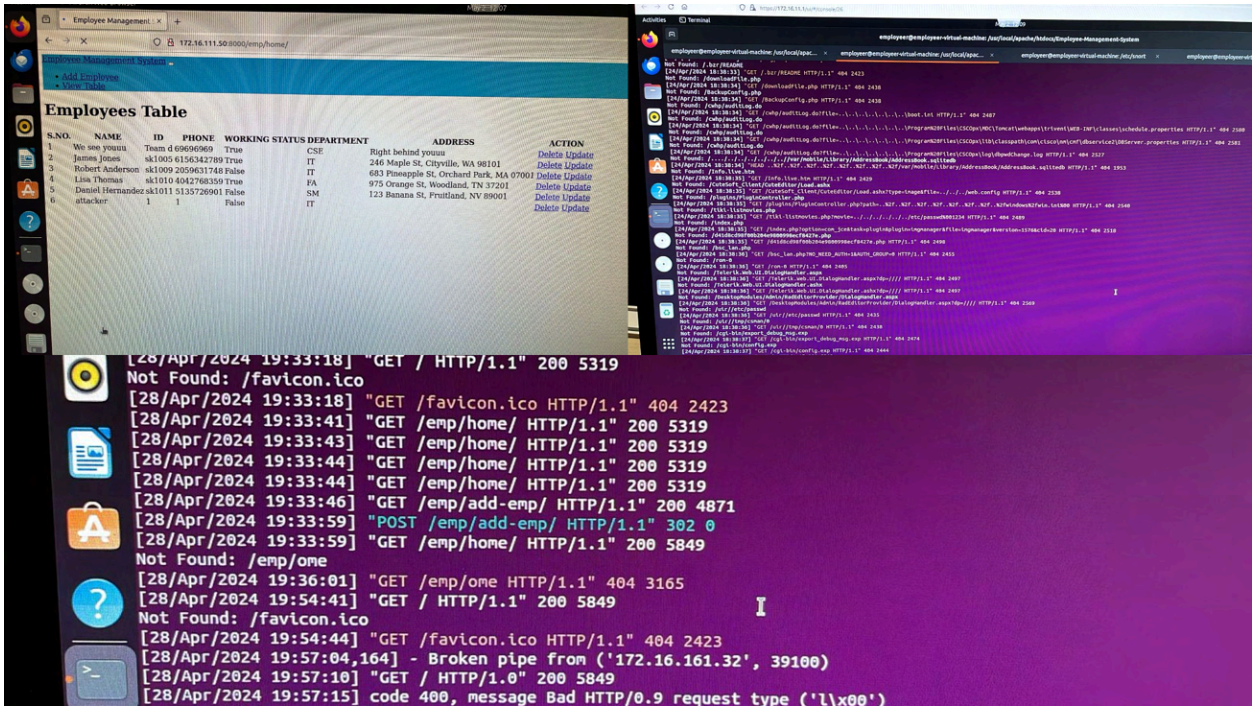


Around 26,000 failed login attempts on all of the systems were made during the event





These entries were logged when teams Delta, Echo and Foxtrot tried to access the Employee Management server. The IP addresses captured were 172.16.41.133 (Delta), 172.16.151.11 (Echo) and 172.16.161.32 (Foxtrot).

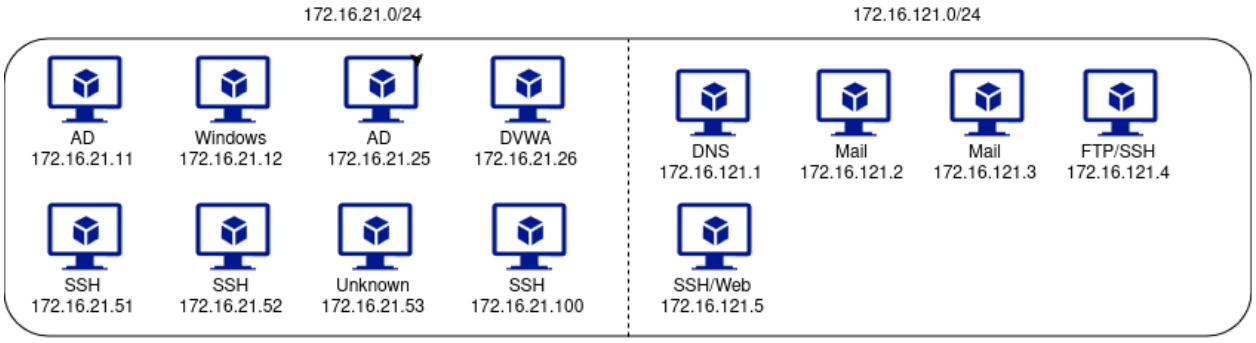


These are logs when teams modified the Employee Database table. Entries 1 and 6 in the Employees table are added by other teams.

Attacks Conducted

Team Bravo

Enumeration

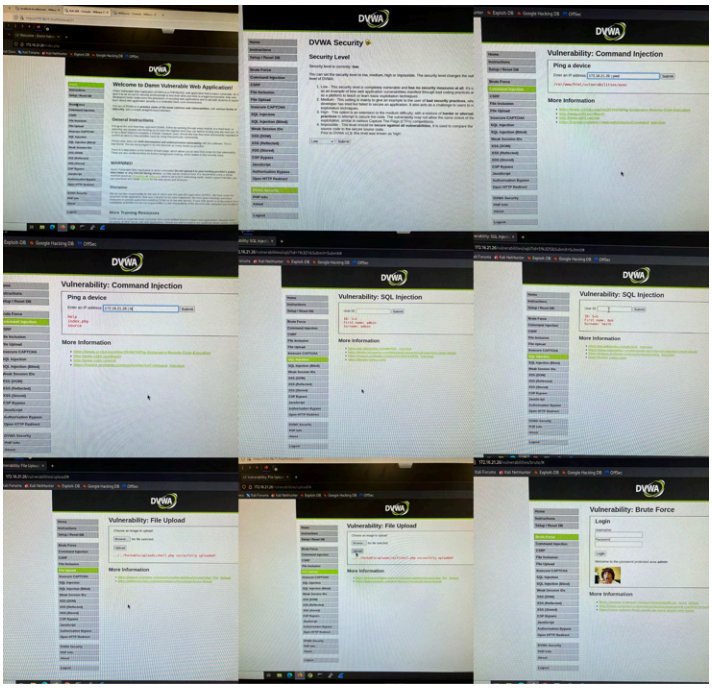


Attacks Conducted

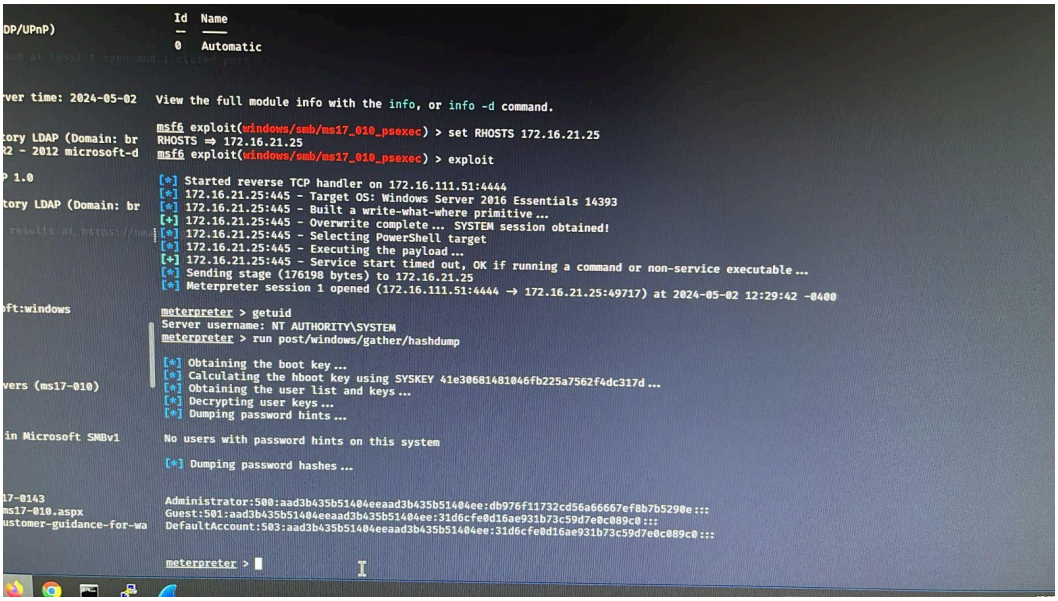
The Domain Controller was vulnerable to the EternalBlue attack. We placed a Realm beacon on the system for persistence. With this, we made a Domain Admin named “skyz”, and used that

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.

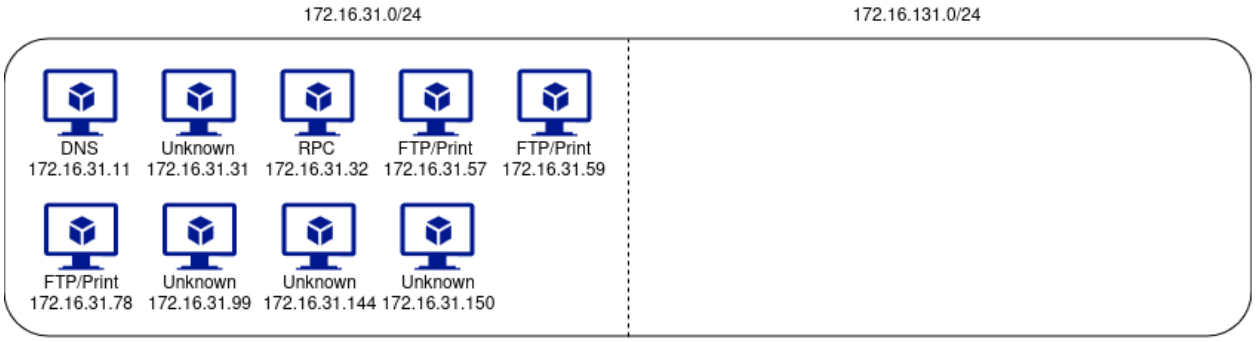


The machine hosted on 172.16.21.25 was vulnerable to EternalBlue. The attack was performed using Metasploit and the hashdump was captured.



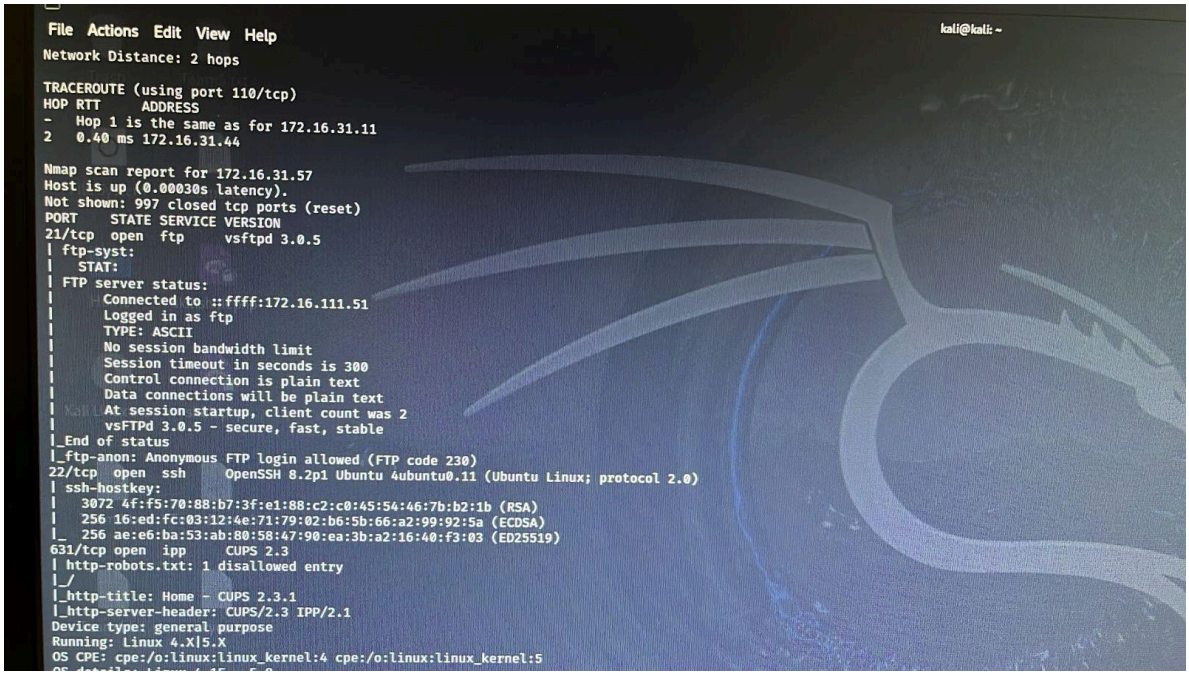
Team Charlie

Enumeration

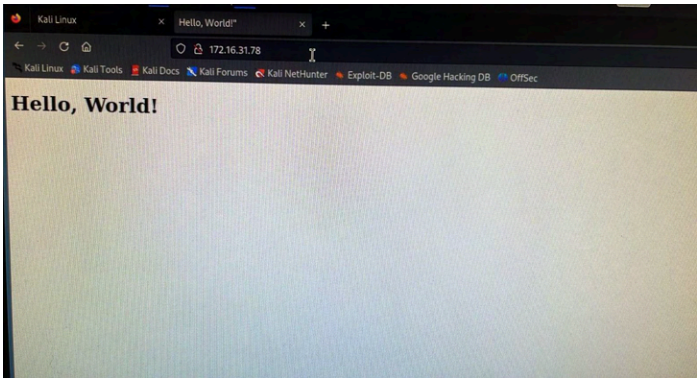


Attacks Conducted

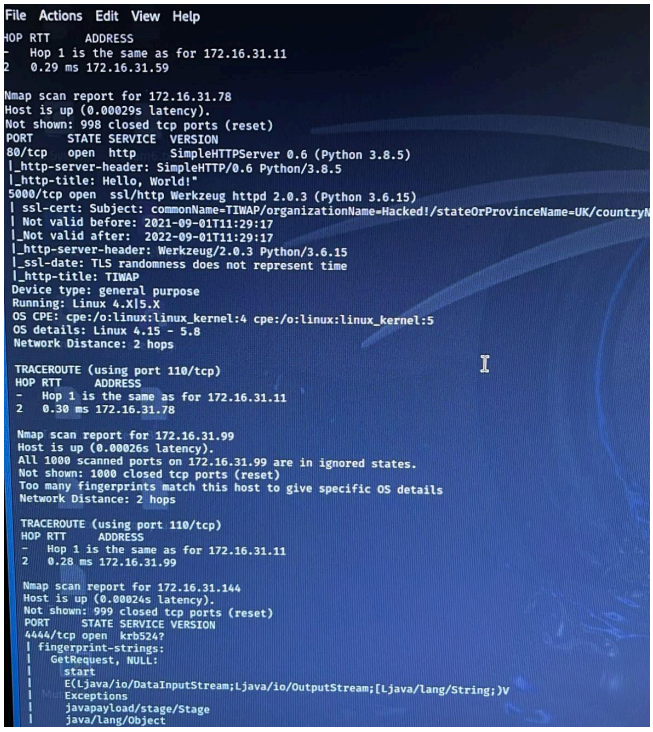
FTP Anonymous login was enabled on 172.16.31.57



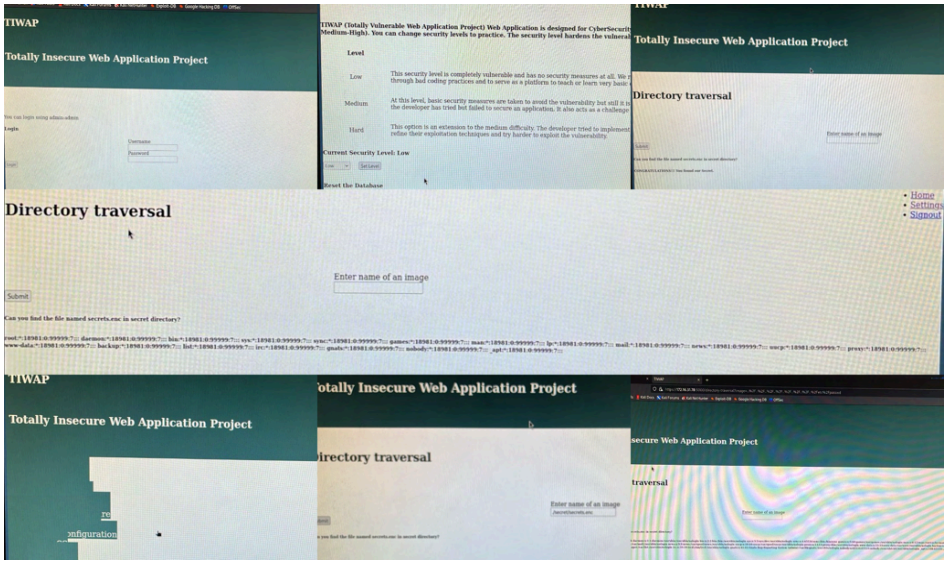
A Simple python web server was hosted on port 80 of 172.16.31.78.



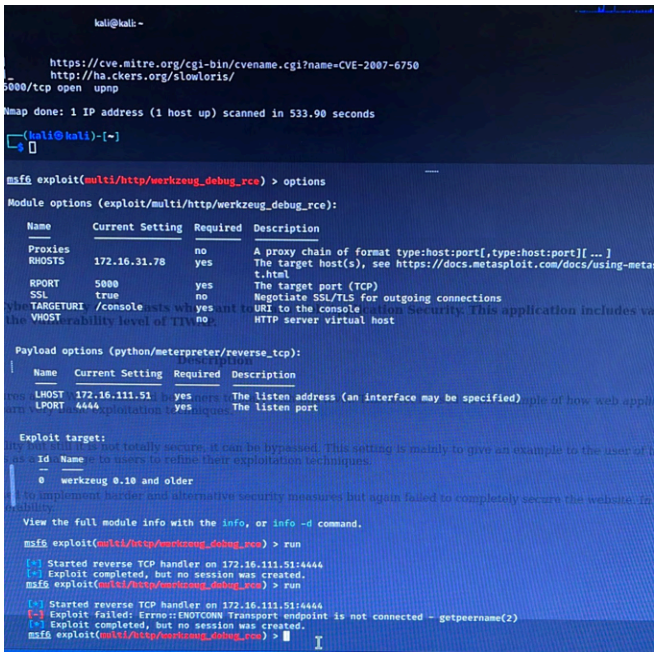
But NMAP scans also revealed that port 5000 was running Werkzeug hosting TIWAP. It is an intentionally vulnerable web server with its code available in github.



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

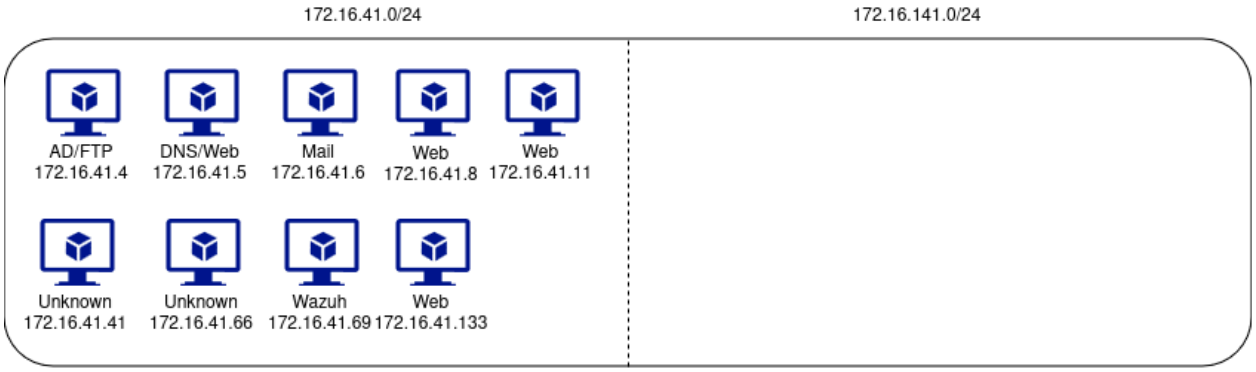


Werkzeug also had a metasploit module that can perform RCE. Unfortunately it couldn't create a session back.



Team Delta

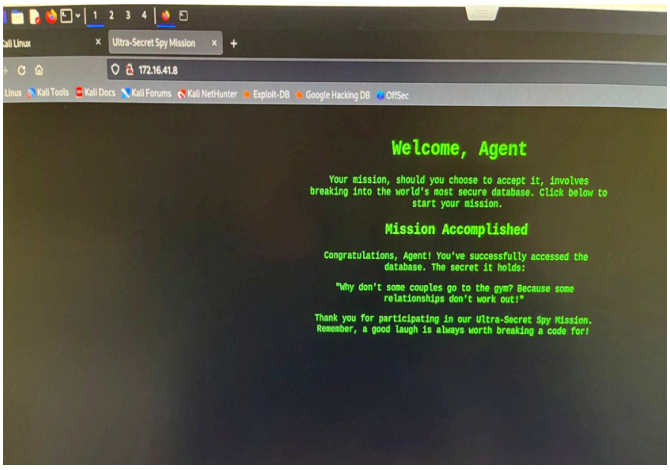
Enumeration



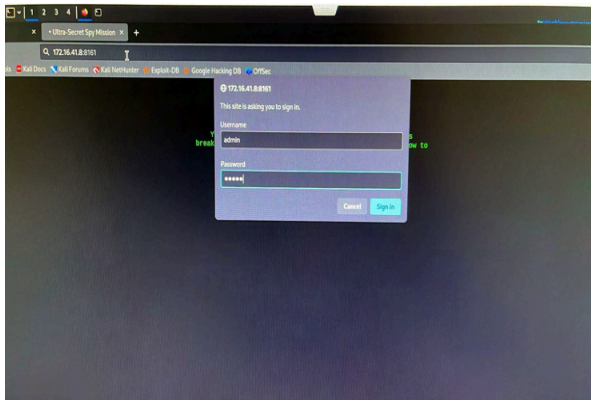
Attacks Conducted

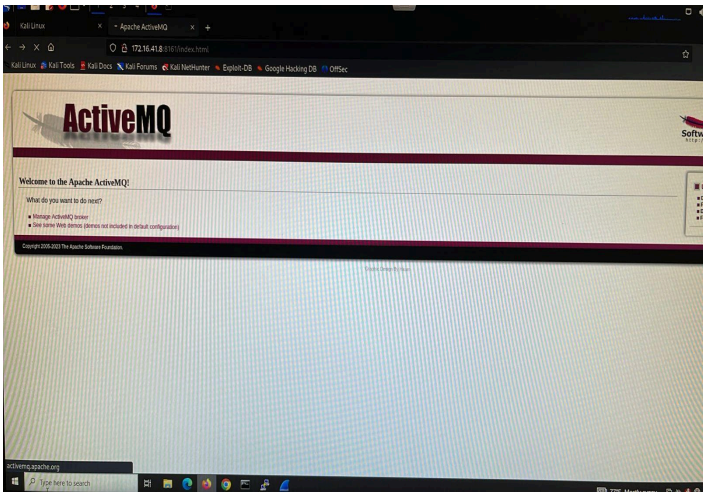
Remote Code Execution was found in the ML Python server. The code was edited to add a backdoor shell at the path “/lol”.

The machine running on 172.16.41.8 had an interesting website.

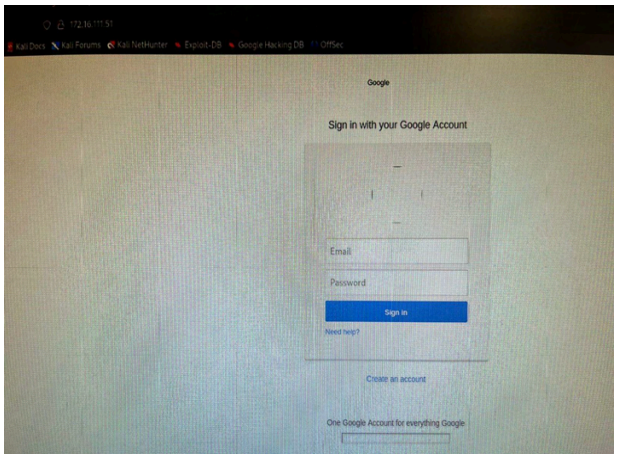


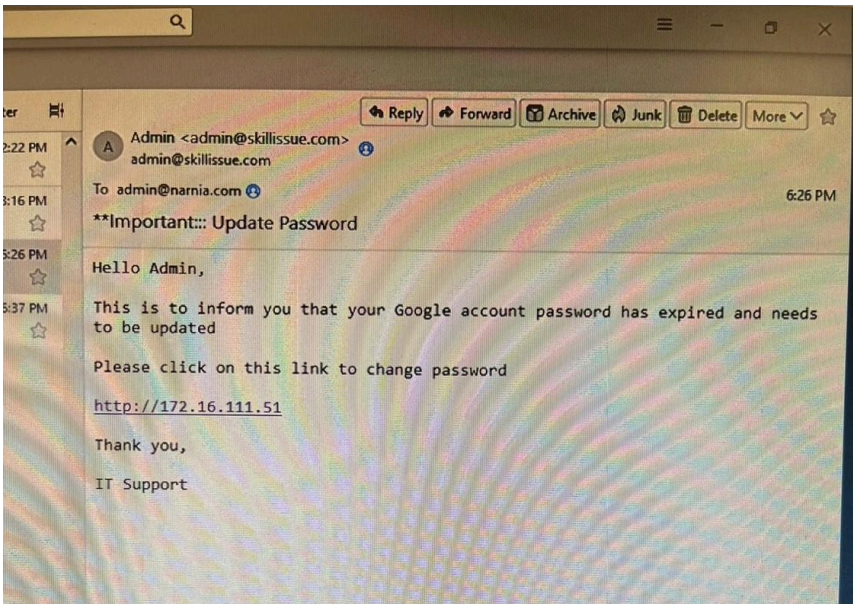
But it also was running ActiveMQ on port 8161. The default login of admin:admin worked.





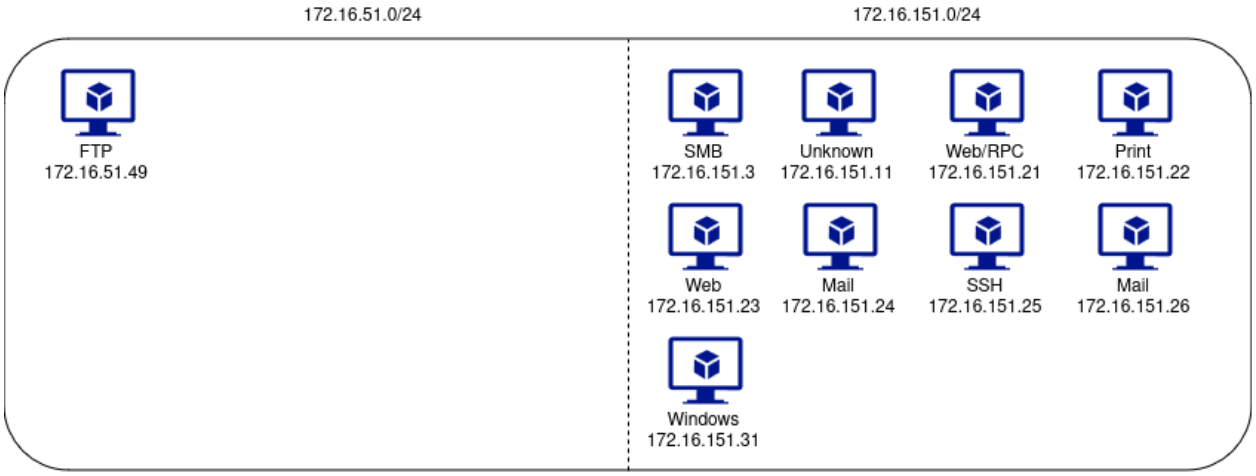
We also tried a very basic phishing attempt by hosting a website in our Kali machine. We sent out the phishing email with the URL of the malicious website attached in the email.





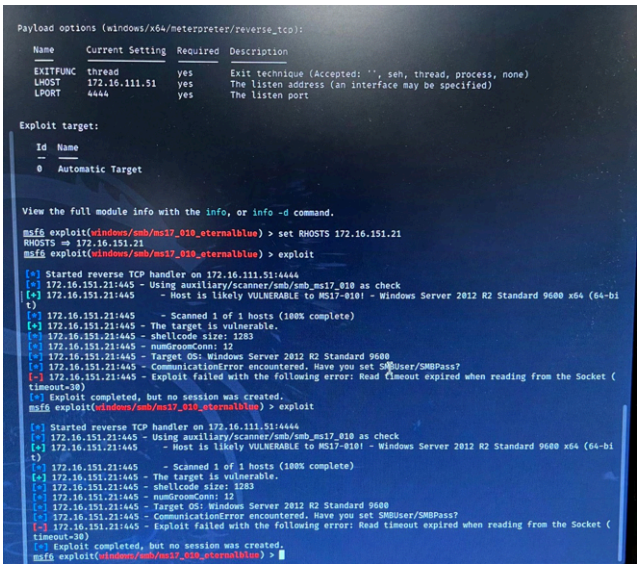
Team Echo

Enumeration

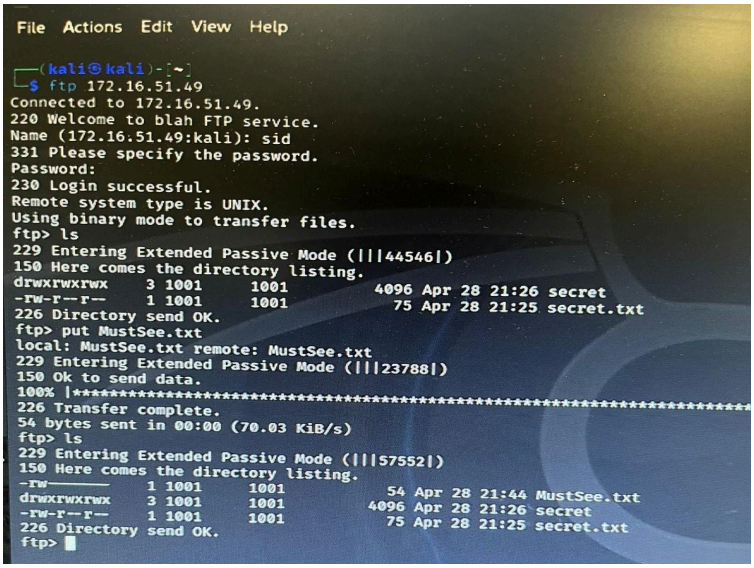


Attacks Conducted

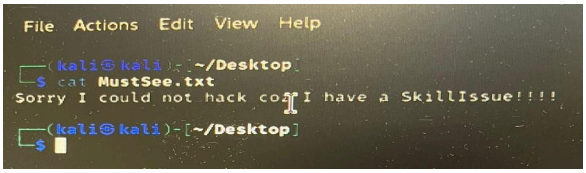
The DNS server was found to be vulnerable to EternalBlue. This was used to get in and place a Realm beacon. We searched this host for other routes around the network, but did not find other credentials available.



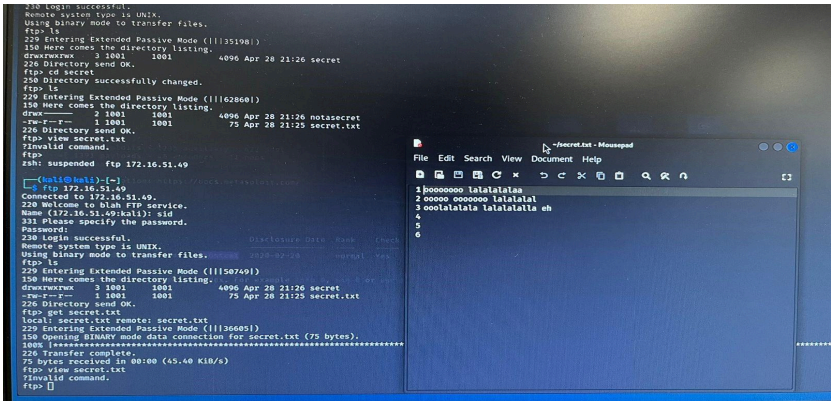
The machine on 172.16.51.49 had Anonymous FTP login enabled. Apart from that, a user account with root privileges had a weak password which was identified by simple password guessing.



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

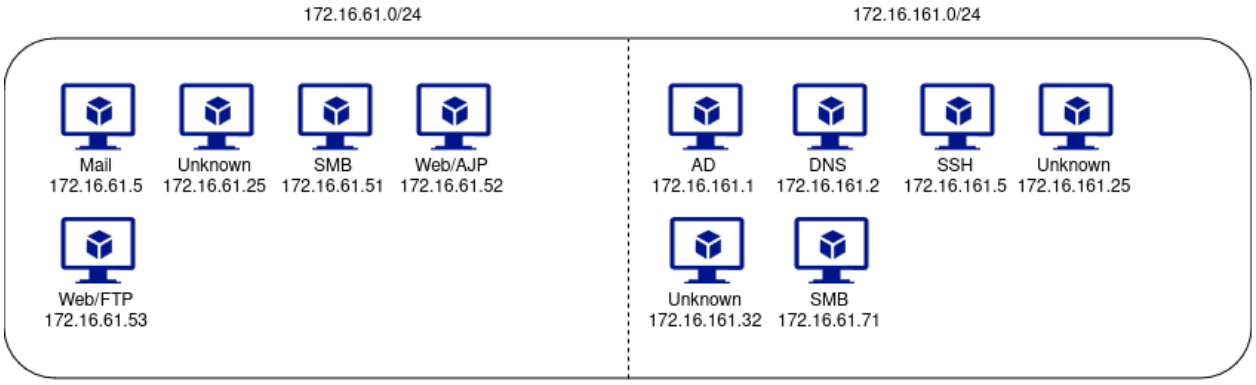


The server also had a file named “secret.txt”. We were able to download it and view the secret message.



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.