Alpha Team 7

BLUE TEAM RUN BOOK 1

Phishing | Data Exfiltration | C2 Payload | Persistence

Author: Adam Baguley **Version:** 3.0 **Date:** 06-05-2025

INTRODUCTION

This runbook provides instructions for detecting, analyzing, containing, and recovering from a phishing attack that leads to a reverse shell compromise and data exfiltration. It outlines the incident response process using the NIST Incident Response Framework

---

STEP 1: PREPARATION

Endpoint Security and Monitoring
Ensure that all endpoints have updated Windows Defender and Firewalls are active.

Confirm that network monitoring tools are active and that Splunk agents are installed on Vuln 1 while the second Windows VM runs Splunk Enterprise SIEM.

Verify that firewall rules and network segmentation are in place to limit lateral movement.

Access Controls
Ensure all end points are configured with least privilege access.

Baseline and Configuration Management
Document current network configurations, baseline system logs, and maintain an updated incident response plan

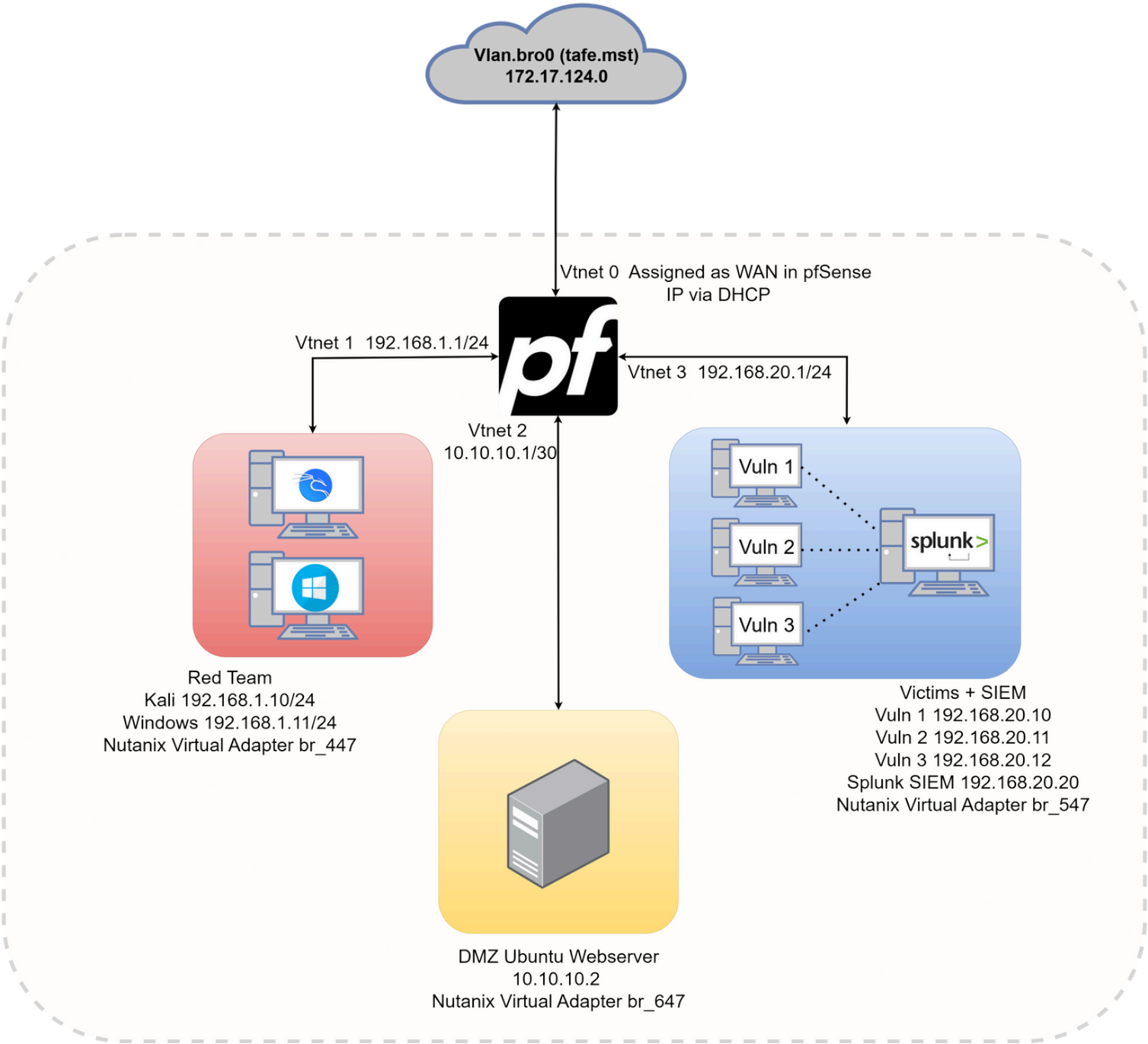
IP addressing

Windows 10 PC With Splunk agent 192.168.20.10/24
Windows 10 PC With Splunk SIEM 192.168.20.20/24

Resources

2 x Virtual Machines
1 x Windows 10 PC Vuln 1
1 x Windows 10 PC Splunk SIEM
Splunk Enterprise installed on Splunk SIEM
Splunk Agent installed on Vuln 1
Wireshark optionally installed on Vuln 1

TOPOLOGY OVERVIEW



STEP 2: DETECTION & ANALYSIS

Install Splunk Agent on Vuln 1

Download the Installer:
Visit the Splunk Downloads page and download the Splunk Universal Forwarder for Windows.
Run the Installer:

Double-click the downloaded installer.
Follow the prompts in the installation wizard.
Accept the license agreement and choose your desired installation folder.

Configure the Forwarder:
During installation, specify the deployment server (if using one) or the Splunk indexer's IP address and management port.
Enter any necessary credentials if prompted.

Complete Installation:
Finish the installation process and allow the installer to configure the forwarder.
Ensure that the Splunk Universal Forwarder service is set to start automatically.

Verify the Installation:
Open a command prompt and navigate to the Splunk forwarder installation directory (usually C:\Program Files\SplunkUniversalForwarder\bin).
Run command: splunk status

Install Splunk Enterprise onto second VM

Download Splunk Enterprise:
Go to the Splunk Enterprise Downloads page and download the appropriate installer for Windows.

Run the Installer:
Double-click the installer.
Follow the on-screen instructions in the installation wizard.
Accept the license agreement and choose your installation folder.

Configure the Installation:
Set the HTTP port (default is 8000) where you will access the Splunk web interface.
Specify the admin username and password.

Complete the Installation:
Click “Install” and wait for the installation to complete.
Once installed, launch Splunk Enterprise either from the Start Menu or by opening a browser and navigating to http://localhost:8000.

IInitial Setup:
Log in with your admin credentials.
Follow any initial setup prompts to configure basic settings.

Configure Data Inputs:
In Splunk Enterprise’s web interface, navigate to Settings > Data Inputs.
Configure the inputs to receive data from the Splunk Universal Forwarder (e.g., via TCP/UDP or by setting up a dedicated Splunk receiver).
Verify that data from the victim machine is being indexed correctly.

Configure Data Receiving on Splunk Enterprise and Forwarding on the Victim Machine

On the Splunk Enterprise (SIEM) Machine:

1. Open the Splunk web interface and navigate to Settings > Data Inputs.
2. Click on Forwarded Data.
3. Enable a TCP receiver by clicking New Receiving Port.
4. Set the port (commonly 9997) and save the configuration.
5. Verify that Splunk Enterprise is listening on the specified port.

On the Victim Machine (Splunk Universal Forwarder):

1. Navigate to the forwarder’s installation directory, usually C:\Program Files\SplunkUniversalForwarder\etc\system\local\.
2. Open (or create if it doesn’t exist) the file named outputs.conf.
3. Add or update the following configuration:

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.1.5:9997

[tcpout-server://192.168.1.5:9997]
```

Monitor network traffic for abnormal outbound HTTP connections.
Analyse logs from firewalls, proxy servers, and endpoint detection systems for suspicious activity.

Use tasklist, and event logs to identify unknown processes or reverse shell connections.

Investigate file integrity alerts on user Documents and Pictures folders to identify unauthorized file uploads.

Monitor for unusually large files being transferred over HTTP.

Wireshark:
As the exploit is not using a real GitHub API & repository it's running over HTTP, so packets should be recorded for detection and plain text analysis.

Example Splunk alerts for SIEM

Monitor for Unusually Large Files Being Transferred Over HTTP
index=web sourcetype=access_combined
| where bytes > 5000000
| stats count by clientip, uri, bytes

Identify Unknown Process Creation Events
index=windows sourcetype=WinEventLog:Security EventCode=4688
|search NOT New_Process_Name IN ("C:\\Windows\\System32*", "approvedApp.exe")
| stats count by New_Process_Name, Account_Name, Process_Command_Line

Identify when one .exe launches another
index=windows sourcetype=WinEventLog:Security EventCode=4688
| where like(Parent_Process_Name, "%.exe") AND like(New_Process_Name, "%.exe")
| table _time, Account_Name, Parent_Process_Name, New_Process_Name, Process_Command_Line

Identify attempts by .exe to establish persistence using Event Code 4657 (Registry Value Modified)
Enable auditing on the registry path:
Run regedit, navigate to ;
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Right click Permissions - Advanced - Auditing - Add your users/group, check "Set Value"

Splunk SPL:
index=wineventlog sourcetype="XmlWinEventLog:Security" EventCode=4657
| where like(TargetObject, "%Software\\Microsoft\\Windows\\CurrentVersion\\Run%")
| table _time, host, user, TargetObject, OldValue, NewValue

Monitor the commands executed by the attacker, assume the commands were executed via HTTPS and not visible within Wireshark.

Enable command line logging:

Open the Registry Editor:

- Press Win+R to open the Run dialog.
- Type regedit and press Enter.

Navigate to the Audit Key

- In the Registry Editor, go to:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit

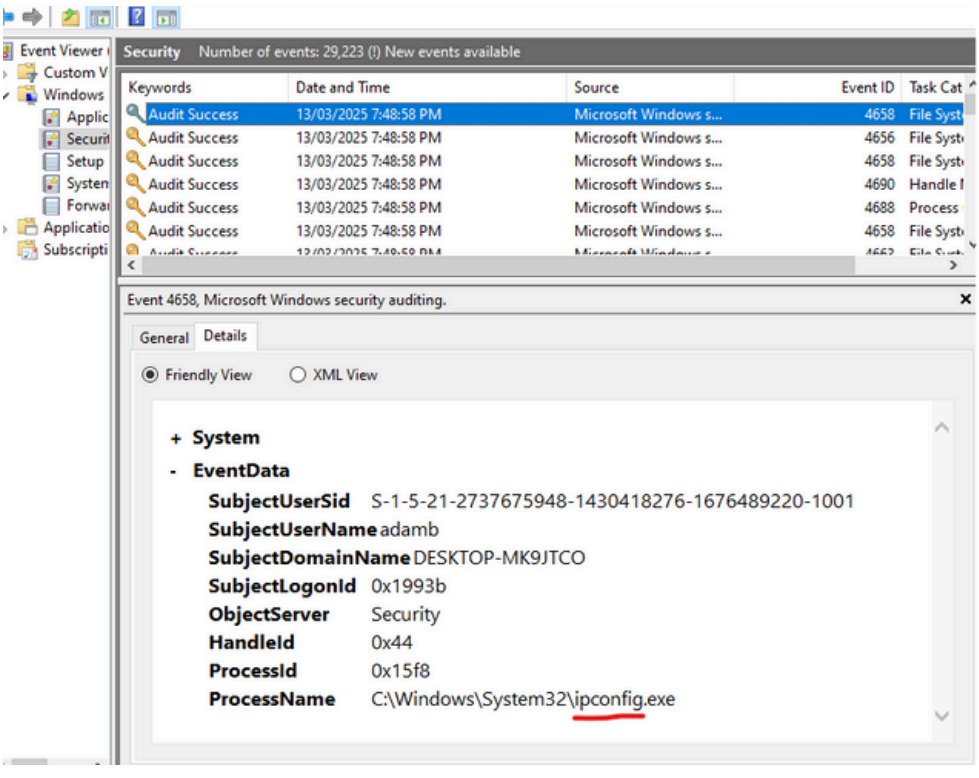
Create or Modify the DWORD Value:

- Right-click in the right pane and select New → DWORD (32-bit) Value.
- Name the new value: ProcessCreationIncludeCmdLine_Enabled.
- Double-click on ProcessCreationIncludeCmdLine_Enabled and set its Value data to 1.

Apply the Changes:

Close the Registry Editor.
Reboot the system to apply the changes.
Monitor commands using Event ID: 4688

Example: Attacker runs command “ipconfig”



STEP 3: CONTAINMENT ERADICATION & RECOVERY

Containment
Immediately isolate any suspected compromised systems from the network.

Block malicious IP addresses, URLs, and domains at the firewall.

Perform forensic analysis on the affected endpoints to determine the extent of the compromise.

Eradication and Recovery

Remove the malicious payload (reverse shell executable) and any related artifacts.

Conduct a thorough forensic analysis of affected endpoints using collected Splunk logs and PCAP data from Wireshark.

As the attack will have occurred using HTTP for this simulation defenders may be able to examine all captured packets and follow the trail of commands that were executed.

This would be beneficial in assessing the damage and checking for any other lateral movement attempts or backdoors installed.

Reimage or restore affected systems if necessary, and ensure all security patches are applied.

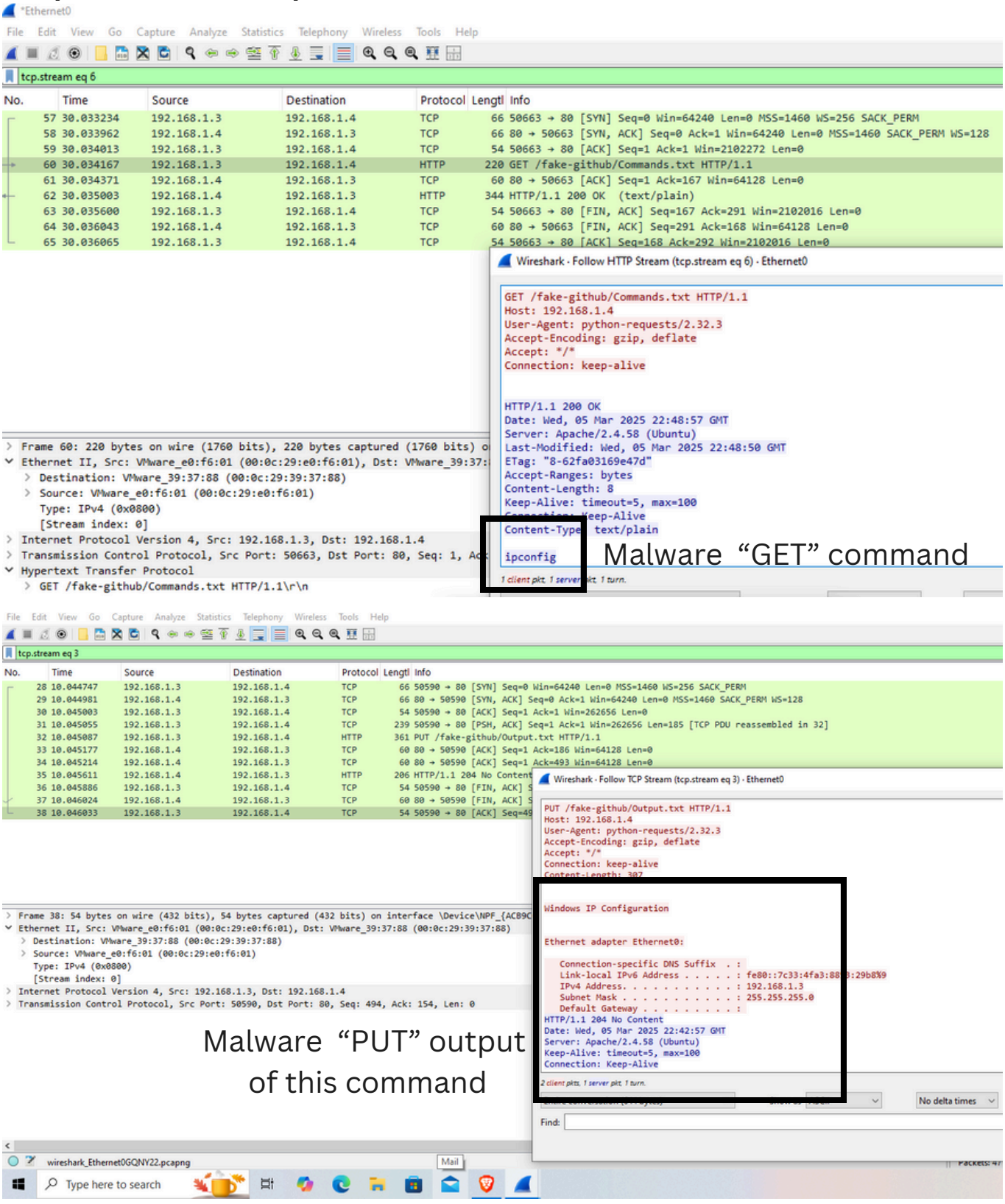
Validate that systems are clean and fully operational before reconnecting them to the network.

Analyse Wireshark Pcap files

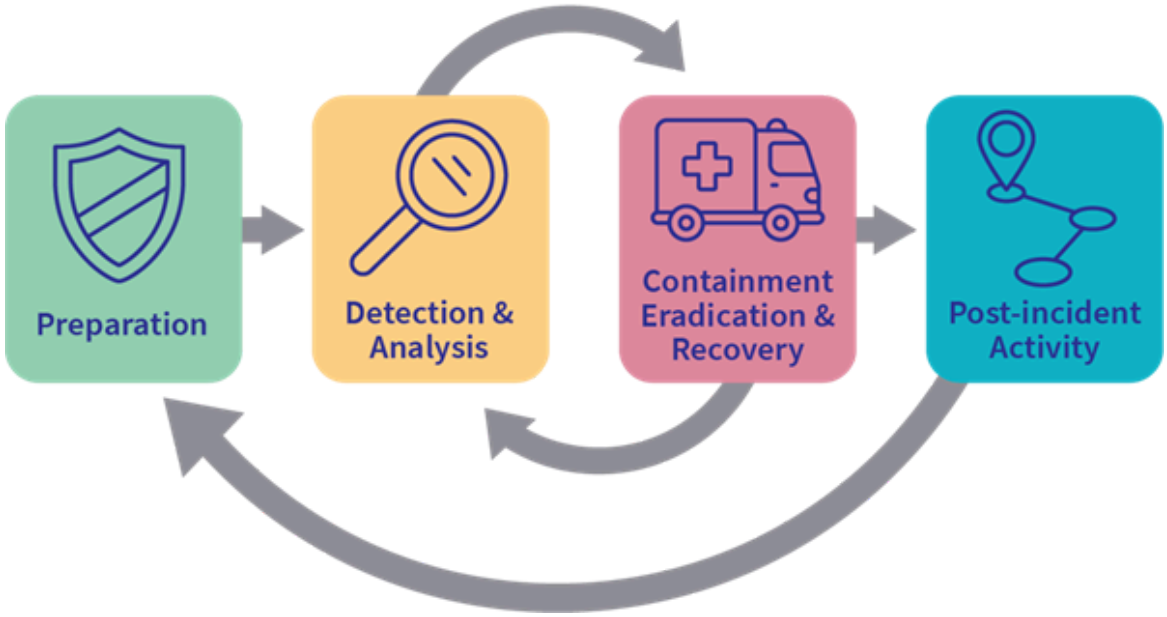
Further inspection of any pcap files should provide further information on the actions taken by the attacking team and the responses sent by the victim machine.

This information should be used to further understand the TTP's of this type of attack and be useful in determining the success and damage of the attack and developing defence measures.

Example of Wireshark captures



STEP 4: POST INCIDENT ACTIVITY



Following The NIST Incident Response Framework;

Debrief and Document
Document all findings, including timelines, attack vectors, and indicators of compromise (IoCs).

Using Splunk and PCAP files refine detection rules and update firewall policies and intrusion prevention measures.

Analyses of the Wireshark (PCAP) captures provides the Blue Team with visibility into the exact commands sent and received during the red team's activities.

By inspecting the plaintext GET and PUT requests, the Blue Team could identify key vulnerabilities or misconfigurations, such as a lack of encrypted communication (use of plain-text HTTP), unmonitored web activity, or weak network segmentation that allows lateral movement.

Lessons Learned and Process Improvement
Conduct a joint debrief with the Blue Team and Purple Team coordinator to analyse the incident response process.

Discuss the attack technique by viewing the python script logic provided by the Purple team lead, use the script logic to identify any gaps in detection and response.

Update the incident response plan and runbook based on the lessons learned, and schedule follow-up training and simulations to ensure continuous improvement.

Re run the simulation to test new improved response measures.