|  |  |  |
| --- | --- | --- |
| Course # | James Riley Dorough | Final Penetration Testing Lab Report |
| CSIS 462 | **31MAR22** | **Semester Week 14, Lab 9** |

**Title**

* Discuss and provide content regarding the operations individual red team members have taken throughout the semester
* Consolidate the work of each member in multiple reports to be formatted into one formal final penetration testing document

**Introduction**

During this penetration test, many activities of varying complexity were attempted. Following a structured approach guided by Lockheed Martin’s cyber kill chain. Nearly all red team efforts proved successful. Any time not spent on a live penetration objective was spent learning new tools, generating new TTPs, and testing new custom code. From reconnaissance to malware development to covert C2, the red team has learned and practiced our tradecraft to provide numerous opportunities for the blue team to learn incident response. This document outlines a full catalog of my personal effects during this team penetration test.

**Results**

**Using Shell Code and Shell Code Obfuscation Techniques**

For this objective, I wrote evolving iterations of PowerShell code to collect all local users on a Windows box as objects and add each user to the Administrators group. This allows easy access to systems without the need to pivot for reasons beyond covert lateral movement. My code was the basis for later task scheduler-assisted persistence.

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

**Custom Exploit Development/Deployment**

This objective was to utilize vulnerable software, services, and configurations in target systems to gain access or execute code remotely. My first focus was setting up an SSH tunnel to our red team firing station to provide a NAT’d IP address for file transfers from the red team development network.

**Text

Description automatically generated**

Once this was running, I started Metasploit and used the blue team system and service scans to determine an exploit payload to attempt. I used Metasploit's SMB PSexec payload to acquire Meterpreter sessions on each blue team Windows 10 box.

Text

Description automatically generated with medium confidence

I used my access to stage future attacks and implant flags on blue team Windows 10 boxes.

Graphical user interface

Description automatically generated with medium confidence

In addition to Metasploit, I also utilized the impacket-psexec command to gain a shell on target systems

Text

Description automatically generated

**Custom Covert C2 Platform Development/Deployment**

During this objective, the goal was to obtain and maintain covert persistence within the blue team systems using a command-and-control server with C2 implants running on target systems. This was achieved using previously mentioned exploits and additional backdoors.

**Graphical user interface, text

Description automatically generated**

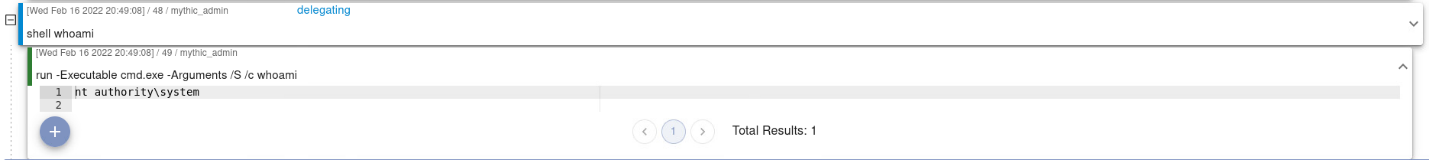
Using NSSM I set my initial C2 payloads as services and ran them on all blue team Windows 10 systems. Using the C2 I installed Admin users which should be recognizable by the blue team as not reasonably named.

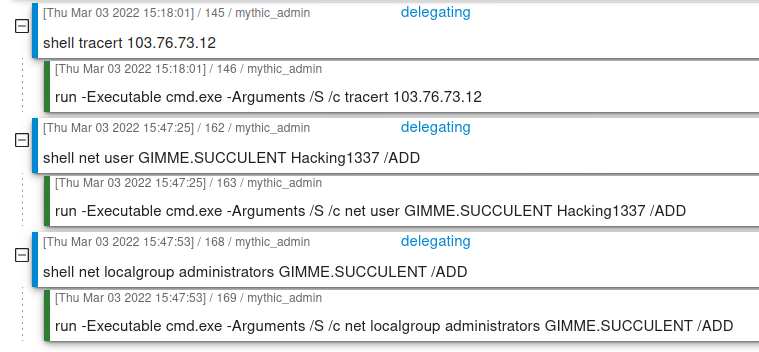
Text

Description automatically generated

Graphical user interface, application, table

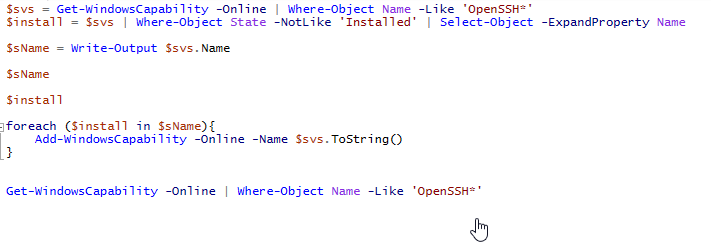
Description automatically generated

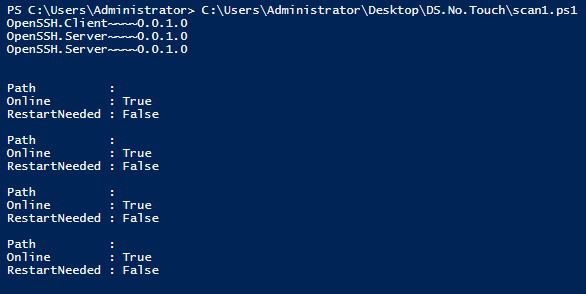




**Scripted Covert Initial Reconnaissance, Scanning, and Enumeration**

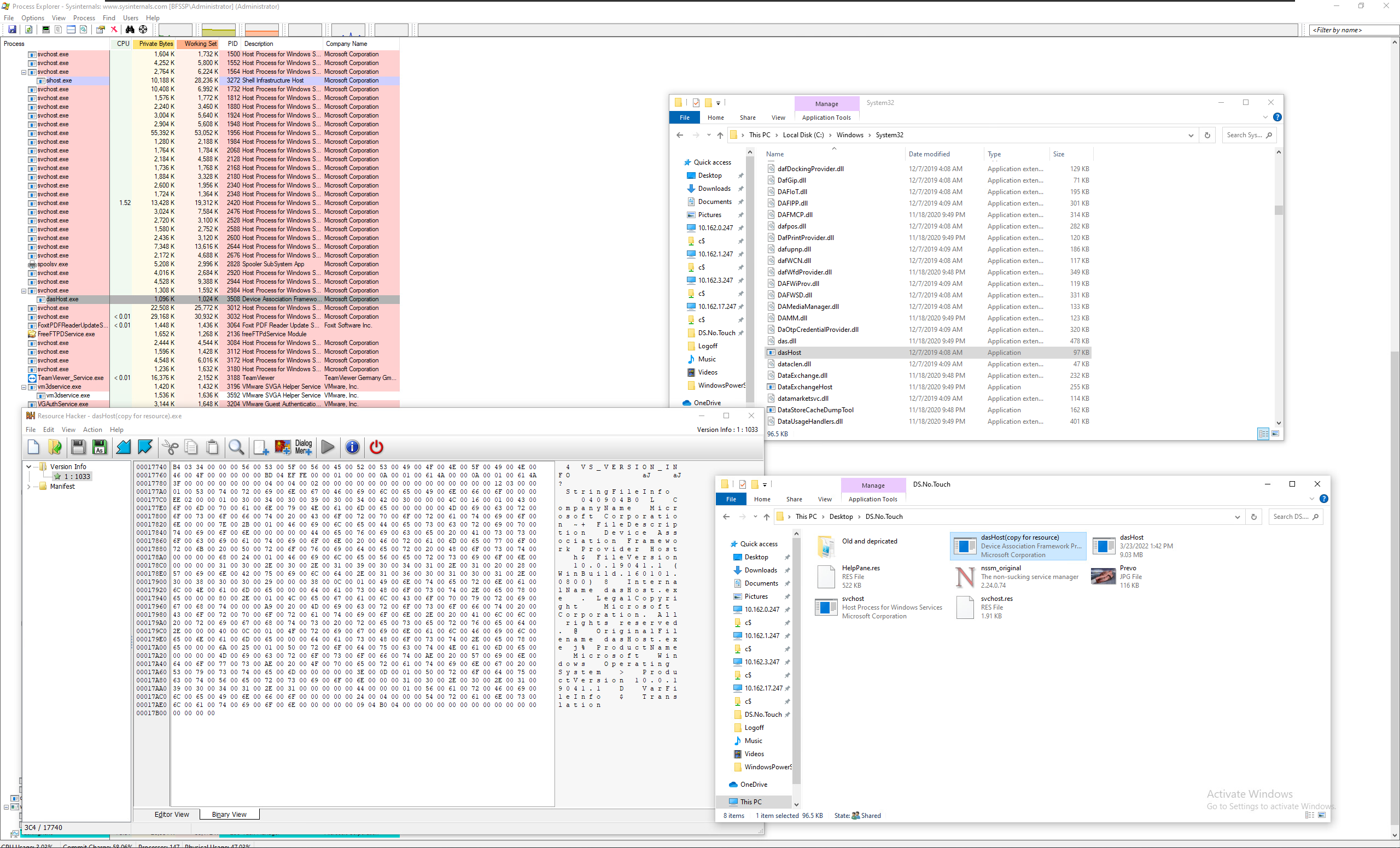
During this lab, I took advantage of PowerShell to write custom code to check the status of SSH services on Windows 10 boxes. The code should install the service as well and return the results to the screen.



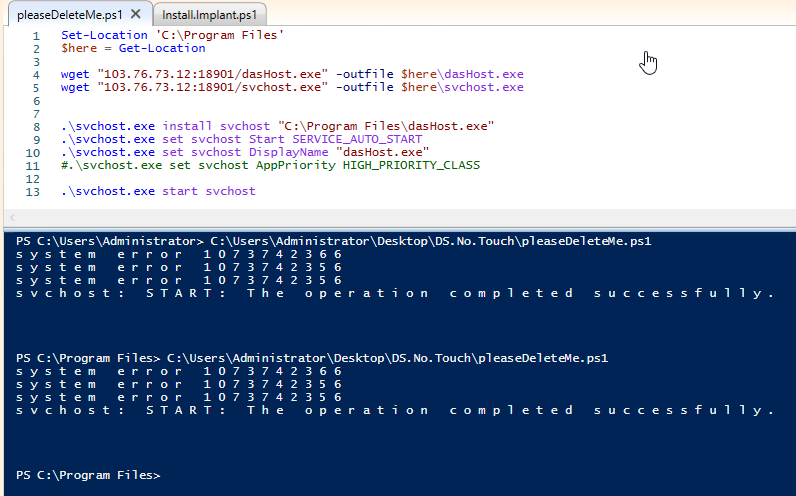


**Covert Persistence**

This was one of the most extensive objectives I have completed to improve persistence. I overhauled my initial Apollo C2 payload by replacing it with the Merlin payload. I had stripped legit Windows 10 processes and copied its recourses to my malicious binary and service manager.



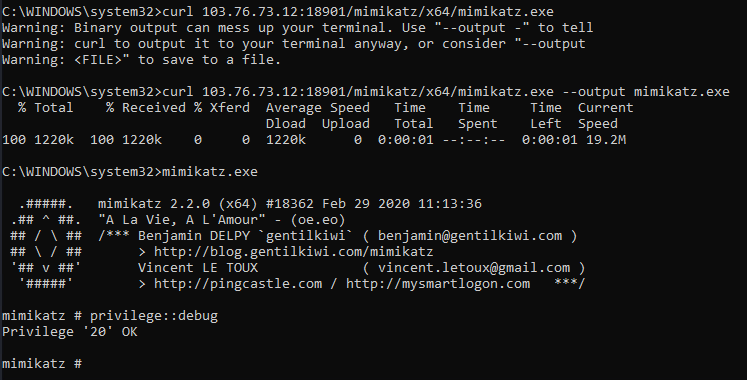
After replacing my binaries’ attributes with the legit Windows service attributes, I needed to install the malware on target systems. I wrote PowerShell scripts to download and install my malware on the blue team systems.

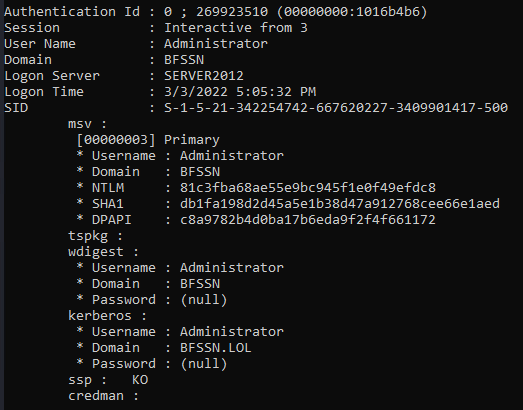


Once this was finalized, I implanted the code on the target systems and boosted my level of persistence.

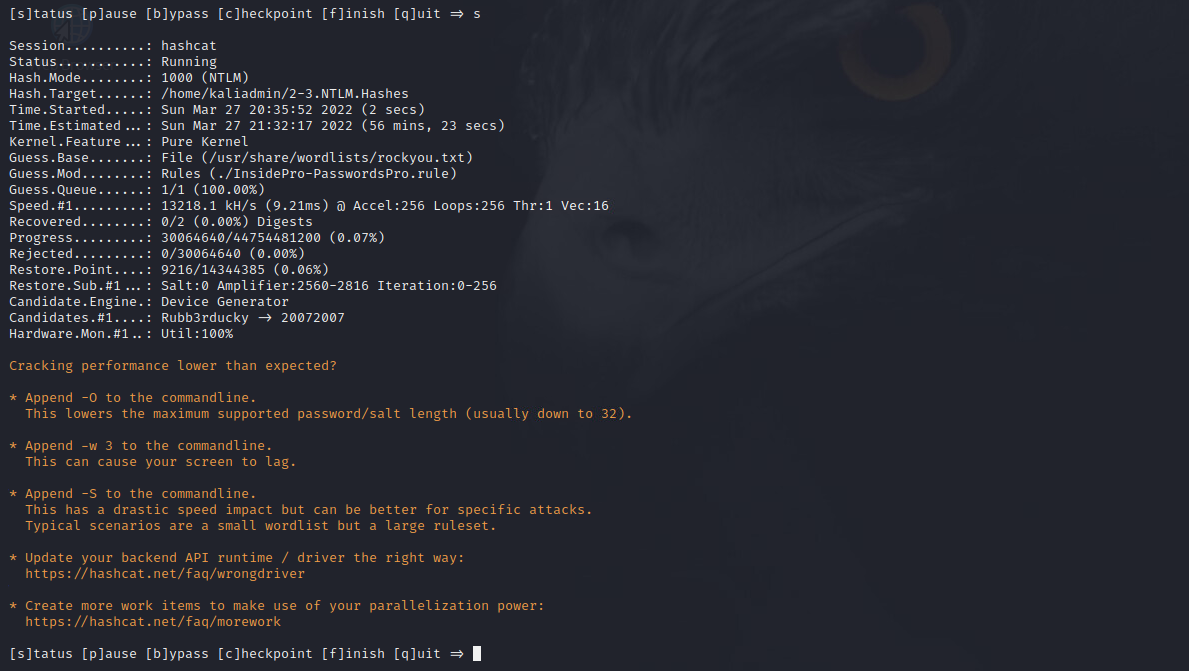
**Covertly Capturing and Using Hashes**

During this objective, I utilized Mimikatz to collect hashes from target systems and exfiltrate them to my red team devices. After recovering the hashes I utilized the NTLM hashes for hash cracking operations.





Using Hashcat I used dictionary and hybrid attacks to attempt to crack various blue team hashes





**Discussion**

**Reconnaissance**

This stage includes scanning and enumeration of services, service versions, open ports, available users, and exploitable applications. This stage was accomplished through initial Nmap scans. After orientation, the effort was directed at gaining initial access to begin internal scanning. Reconnaissance was made quicker and more streamlined due to the red team having a development copy of existing target boxes.

**Weaponization**

Metasploit was the main method used to accomplish the weaponization stage. Using the psexec payload allowed direct meterpreter and System Administrator access to Windows 10 systems. Pre-delivered account credentials provided SSH access as a viable option until blue teams lockdown SSH services.

**Delivery**

Running a simple HTTP server on my local network and SSH tunneling through a firing station running hide NATing was all that was necessary to deliver malware to target systems.

**Exploitation**

The impacket-psexec allows Administrator access to target Windows 10 systems given SMB is online and network-accessible shares are available. Additionally, Mimikats was used to exploit Windows internals to recover blue team NTLM hashes. This coupled with Hashcat to break the hashes returned blue team passwords. This was simply a proof of concept.

**Installation**

NSSM and PowerShell were relied on to install services delivered through web requests to the HTTP server. Scripted installation binaries were written using NSSM to install malicious additional binaries to the target systems.

**Command & Control**

Using two sets of C2 payloads Apollo and Merlin allowed for covert persistence. The Apollo payload was highly noisy and worked for teams not paying close attention to their running services frequently. The Merlin payload was obfuscated and masked as legit Windows services. It utilized such low CPU usage that it blends in well with other legit services in blue team systems.

**Actions on Objectives**

Primality the intentional actions taken on target systems were to provide learning opportunities for blue team members. Among these actions on target were file modification, configuration changes, mild log alteration to promote blue team research, installation of malware, adding users and modifying permissions, and in some cases, wallpaper changes for teams who need some inspiration.

**Conclusion**

This document outlined, in an abstracted informational overview, the operations taken during this penetration test. All events were organized into the Lockheed Martin cyber kill chain format. From initial recon to final actions on target, progress was consistently made to prepare and improve covert persistence on target networks. All objectives were accomplished on a step-by-step basis to provide learning opportunities for both blue and red team members.