

# HTB Sherlock - Salsa Dance Writeup

## Description:

After gaining elevated privileges on the victim machine, the Incident Response team has been assigned the task of analyzing whether the attacker has carried out any lateral movement or collected confidential data within the network, as unusual activity has been detected related to one of the cloud storage accounts.

## Solution:

After downloading the zip file given, I extract it with the password *hacktheblue* given in the description. Inside the folder are Windows artefacts and Linux artefacts. Let's open up FTK Imager and start to investigate!

### Task 1: What time (UTC) did the threat actor retrieve details about the domain controller using a native Windows tool?

At first, I searched on the web for what native Windows tools can be used to retrieve details about the domain controller, and I found that **nltest.exe** is commonly used for querying information about the domain controller. Specifically, it allows administrators to check domain controller status, trust relationships, and other domain-related information. Given this, it was reasonable to suspect that the threat actor might have used **nltest.exe** for reconnaissance on the compromised system.

#### Nltest.exe

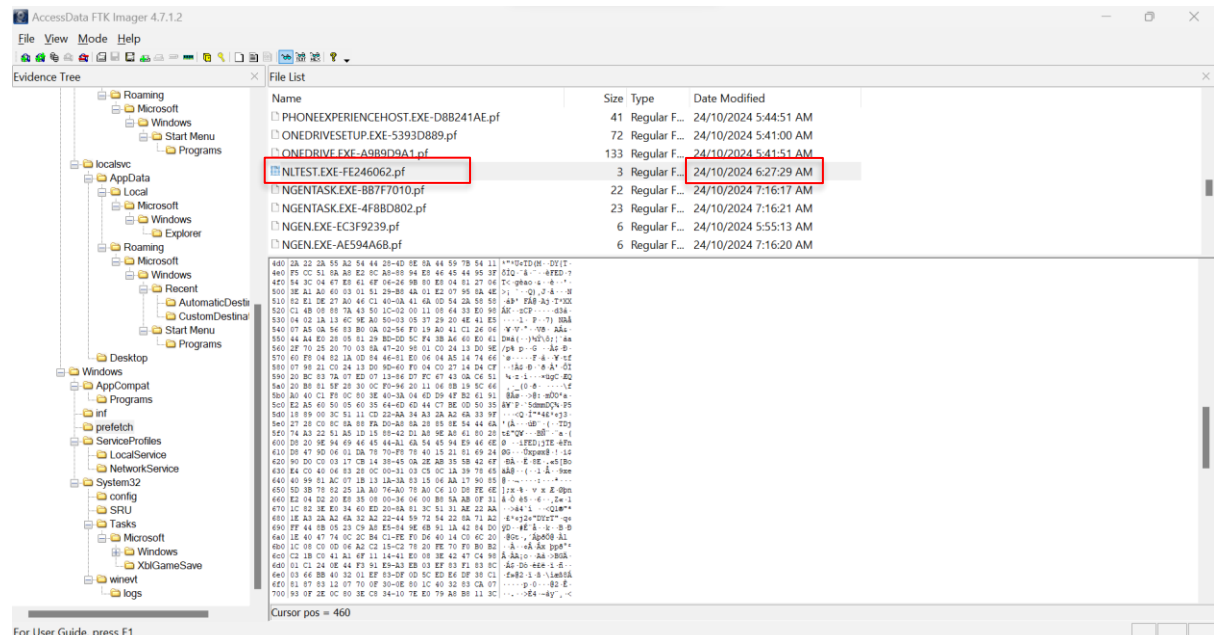
You can use **nltest** to:

- Get a list of domain controllers
- Force a remote shutdown
- Query the status of trust
- Test trust relationships and the state of domain controller replication in a Windows domain
- Force a user-account database to synchronize on Windows NT version 4.0 or earlier domain controllers

**Nltest** can test and reset the secure channel that the NetLogon service establishes between clients and the domain controller that logs them on. Clients using Kerberos authentication cannot use this secure channel.

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731935\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731935(v=ws.11))

To determine when the attacker executed **nltest.exe** on the system, I analyzed the **Prefetch** folder and found **NLTEST.EXE-FE246062.pf**



## Extra Knowledge

**Prefetch** files in Windows are created when applications are executed, and these files store metadata about the execution, including timestamps and the number of times the application has run.

By examining the relevant **prefetch** file, I could identify the time when **nltest.exe** was first executed.

The answer for task 1 is: **2024-10-24 06:27:29**

**Task 2: To what directory on the compromised system did the threat actor download the tools used for reconnaissance?**

The task involves determining where a threat actor downloaded their reconnaissance tools on a compromised system. Reconnaissance tools are typically used to gather information about the system or network, such as network scanning, enumeration, or other intelligence-gathering activities.

I started searching for common reconnaissance tools use for windows and I found this article:

## Top active recon tools

- Nmap. Nmap is probably the most well-known tool for active network reconnaissance. ...
- Nessus. Nessus is a commercial vulnerability scanner. ...
- OpenVAS. OpenVAS is a vulnerability scanner that was developed in response to the commercialization of Nessus. ...
- Nikto. ...
- Metasploit.

17 Sept 2019



Infosec

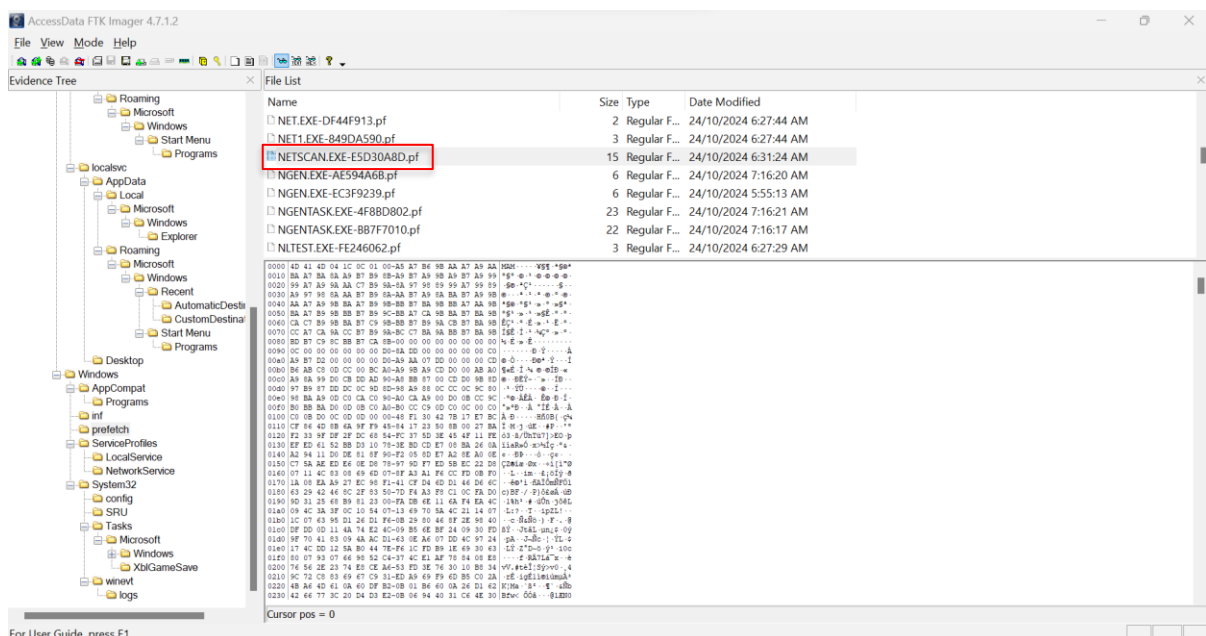
<https://www.infosecinstitute.com> > ... > Hacking

## Top 10 network recon tools - Infosec

? About featured snippets • Feedback

<https://www.infosecinstitute.com/resources/hacking/top-10-network-recon-tools/>

From that article, I can see tools like Nmap, Nessus, OpenVAS ... However, I remember coming across a file named **NMAP.EXE** in the prefetch folder while searching for the NLTEST.EXE file.



Aha! There it is. Now what should I do with it? After searching on the internet, I learned how to use PECmd.exe, an [Eric Zimmerman Tool](#) that will help parse prefetch files.

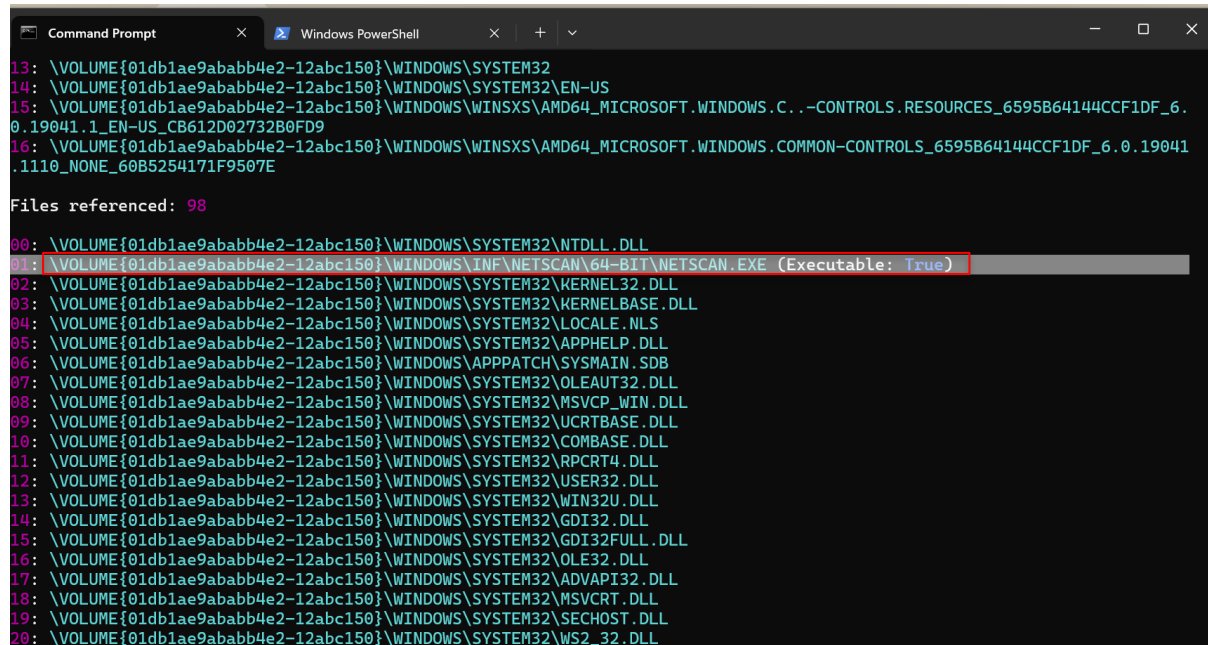
After downloading and unzipping the file, I cd to the directory where PECmd.exe is located and use the command:

**PECmd.exe -d "C:\Path\To\PrefetchFiles"**

OR you can also use this command to output the content in a file:

**PECmd.exe -d "C:\Path\To\PrefetchFiles" -o "C:\Path\To\OutputFolder" -f "NLTEST.EXE"**

I ran the command and found out where NETSCAN.EXE is downloaded.



```
13: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32
14: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\EN-US
15: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\WINSXS\AMD64_MICROSOFT.WINDOWS.C.-CONTROLS.RESOURCES_6595B64144CCF1DF_6.0.19041.1_EN-US_CB612D02732B0FD9
16: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\WINSXS\AMD64_MICROSOFT.WINDOWS.COMMON-CONTROLS_6595B64144CCF1DF_6.0.19041.1110_NONE_60B5254171F9507E

Files referenced: 98

00: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\INF\NETSCAN\64-BIT\NETSCAN.EXE (Executable: True)
02: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\KERNEL32.DLL
03: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\KERNELBASE.DLL
04: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\LOCALE.NLS
05: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\APPHelp.DLL
06: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\APPPATCH\SYSTEMMAIN.SDB
07: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\OLEAUT32.DLL
08: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\MSVCP_WIN.DLL
09: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\UCRTBASE.DLL
10: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\COMBASE.DLL
11: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\RPCRT4.DLL
12: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\USER32.DLL
13: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\WIN32U.DLL
14: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\GDI32.DLL
15: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\GDI32FULL.DLL
16: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\OLE32.DLL
17: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\ADVAPI32.DLL
18: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\MSVCRT.DLL
19: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\SECHOST.DLL
20: \VOLUME{01db1ae9ababb4e2-12abc150}\WINDOWS\SYSTEM32\WS2_32.DLL
```

The answer for task 2 is: **C:\Windows\INF**

**Task 3: Which legitimate Windows program did the threat actor use to download the initial file?**

For this task, I further analysed the prefetch folder and identified some legitimate Windows programs for example:

1. BITSADMIN.EXE
2. EXPLORER.EXE
3. CMD.EXE
4. NOTEPAD.EXE
5. WINWORD.EXE
6. OUTLOOK.EXE
7. REGEDIT.EXE
8. MSIEXEC.EXE
9. TASKMGR.EXE
10. RUNDLL32.EXE
11. CONHOST.EXE
12. WMPLAYER.EXE

- 13. SERVICES.EXE
- 14. SVCHOST.EXE
- 15. EXPLORER.EXE
- 16. CONTROL.EXE

However, it is worth noting that some of these legitimate programs, such as **BITSADMIN.EXE** and **RUNDLL32.EXE**, are commonly abused by threat actors.

Since this task specifically asks about the downloading of files, **BITSADMIN.EXE** would be a more relevant answer compared to **RUNDLL32.EXE**, as it is commonly used for transferring files, including malicious ones, while **RUNDLL32.EXE** is more associated with executing payloads rather than downloading them.

#### Extra Knowledge

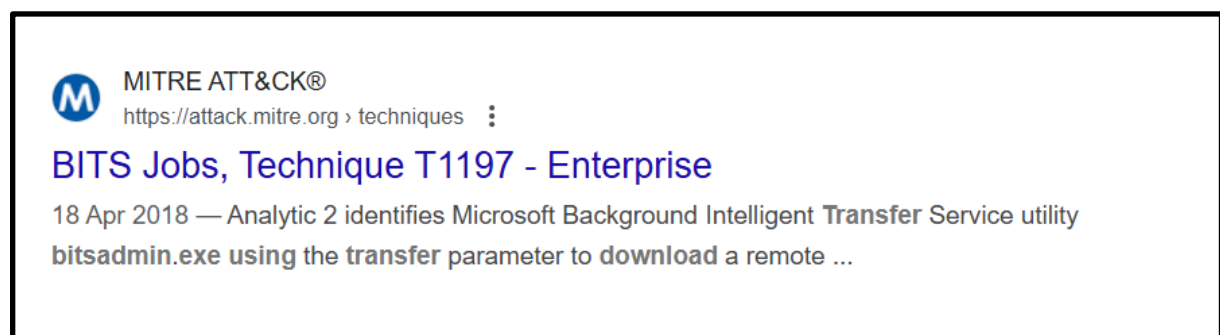
What is **bitsadmin.exe**?

**bitsadmin.exe** is a legitimate command-line tool that facilitates the transfer of files using the Background Intelligent Transfer Service (BITS). Though originally designed for Windows Update and other administrative tasks, **bitsadmin.exe** is commonly abused by attackers to download malicious files from remote servers onto compromised systems.

The answer for task 3 is: **bitsadmin.exe**

**Task 4: What is the MITRE ATT&CK Technique ID associated with the method used by the threat actor in Question #3?**

For this task, we just have to search for “What is the MITRE ATT&CK Technique ID associated with using bitsadmin.exe to download files?” and we will get the answer:




<https://attack.mitre.org/techniques/T1197/>

The answer for task 4 is: **T1197**


**Task 5: The threat actor used a program to identify the credentials stored on the victim machine. What was the original filename of this program before it was renamed?**

Ok so here's a twist, I took a few day's break because I was busy with something else and when I came back to this box ...

< Retired Sherlock

 **OpSalwarKameez24-4: Salsa-Dance** ★★★★☆  
Medium 4.3 3 Reviews

Play Sherlock Sherlock Info Reviews

 **Upgrade to play this Sherlock**  
Unlock 800+ exclusive labs, from beginner to advanced levels, and train at your own pace with official write-ups and walkthroughs to boost your learning! **UPGRADE FROM \$11.25/MO**

What is the MITRE ATT&CK Technique ID associated with the method used by the threat actor in Question #3?

T1197 ✓

Task 5 Task 6 Task 7 Task 8

It has become a retired box and I have to become premium to continue solving it :( Since I'm not premium, so I guess this is the end of this writeup ...