nltest /dsgetdc: /force

Table of Contents

Open all sections | Close all sections

Tool Overview

Category

Information Collection

Description

Acquires the Domain Controller used and its IP address.

Example of Presumed Tool Use During an Attack

This tool is used to acquire information on the Domain Controller to which a host belongs.

Tool Operation Overview

Item	Source host	Domain Controller
OS	Windows	Windows Server
Communication Protocol	389/udp	
Belonging to Domain	Not required	
Rights	Standard user	
Service	Workstation	Active Directory Domain Services

Information Acquired from Log

Standard Settings

- Source host
    - Execution history (Prefetch)

Additional Settings

- Source host
    - Execution history (Sysmon, audit policy)

- Evidence That Can Be Confirmed When Execution is Successful

- Source Host: The Event ID 4689 (A process has exited) indicating that nltest.exe was executed and has exited, was recorded in the event log "Security" with the execution result (return value) of "0x0".

- Main Information Recorded at Execution

- Source Host

Event log

#	Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **CommandLine**: Command line of the execution command (nltest /dsgetdc: /force) • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\nltest.exe) • **User**: Execute as user
2	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Exit Status**: Process return value (0x0) • **Subject > Account Name**: Name of the account that executed the tool • **Log Date and Time**: Process terminated date and time (local time) • **Subject > Account Domain**: Domain to which the account belongs • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\nltest.exe) • **Subject > Security ID**: SID of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process

- Details: Source Host

## - Event Log

#	Event Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **LogonGuid/LogonId**: ID of the logon session • **ParentProcessGuid/ParentProcessId**: Process ID of the parent process • **ParentImage**: Executable file of the parent process • **CurrentDirectory**: Work directory • **CommandLine**: Command line of the execution command (nltest /dsgetdc: /force) • **IntegrityLevel**: Privilege level (Medium) • **ParentCommandLine**: Command line of the parent process • **UtcTime**: Process execution date and time (UTC)

				• **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user • **Hashes**: Hash value of the executable file • **Image**: Path to the executable file (C:\Windows\System32\nltest.exe)
	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation (Mandatory Label\Medium Mandatory Level) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Source Process Name**: Path to parent process that created the new process • **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (C:\Windows\System32\nltest.exe) • **Process Information > Token Escalation Type**: Presence of privilege escalation (1) • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process
2	Security	5158	Filtering Platform Connection	The Windows Filtering Platform has permitted a bind to a local port. • **Network Information > Protocol**: Protocol used (17=UDP) • **Network Information > Source Port**: Bind local port • **Application Information > Process ID**: Process ID • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. • **Network Information > Destination Port**: Destination port number (389) • **Network Information > Source Port**: Source port number (high port) • **Network Information > Destination Address**: Destination IP address (Domain Controller) • **Network Information > Protocol**: Protocol used (17=UDP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (outbound) • **Network Information > Source Address**: Source IP address (source host) • **Application Information > Process ID**: Process ID
3	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	Process terminated. • **UtcTime**: Process terminated date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (C:\Windows\System32\nltest.exe)
	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Exit Status**: Process return value (0x0) • **Subject > Account Name**: Name of the account that executed the tool • **Log Date and Time**: Process terminated date and time (local time)

				• **Subject > Account Domain**: Domain to which the account belongs • **Process Information > Process Name**: Path to the executable file (C:\Windows\System32\nltest.exe) • **Subject > Security ID**: SID of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process
4	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\Windows\Prefetch\NLTEST.exe-[RANDOM].pf) • **CreationUtcTime**: File creation date and time (UTC)
	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Object > Object Name**: Target file name (C:\Windows\Prefetch\NLTEST.EXE-[RANDOM].pf) • **Subject > Account Name**: Name of the account that executed the tool ([Host Name]$) • **Subject > Account Domain**: Domain to which the account belongs (domain) • **Process Information > Process Name**: Name of the process that closed the handle • **Subject > Security ID**: SID of the user who executed the tool (SYSTEM) • **Object > Object Type**: Type of the file (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Audit Success**: Success or failure (access successful) • **Object > Object Name**: Target file name (C:\Windows\Prefetch\NLTEST.EXE-[RANDOM].pf) • **Subject > Account Name**: Name of the account that executed the tool ([Host Name]$) • **Subject > Account Domain**: Domain to which the account belongs (domain) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Subject > Security ID**: SID of the user who executed the tool (SYSTEM) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Account Name**: Name of the account that executed the tool ([Host Name]$) • **Subject > Account Domain**: Domain to which the account belongs (domain) • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\svchost.exe)

				- **Subject > Security ID**: SID of the user who executed the tool (SYSTEM) - **Subject > Logon ID**: Session ID of the user who executed the process - **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4656)

- USN Journal

#	File Name	Process	Attribute
1	NLTEST.EXE-[RANDOM].pf	FILE_CREATE	archive+not_indexed
	NLTEST.EXE-[RANDOM].pf	DATA_EXTEND+FILE_CREATE	archive+not_indexed
	NLTEST.EXE-[RANDOM].pf	CLOSE+DATA_EXTEND+FILE_CREATE	archive+not_indexed

- MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Windows\Prefetch\NLTEST.EXE-[RANDOM].pf	FILE	ALLOCATED

- Prefetch

#	Prefetch File	Process Name	Process Path	Information That Can Be Confirmed
1	NLTEST.EXE-[RANDOM].pf	NLTEST.EXE	\VOLUME{[GUID]}\WINDOWS\SYSTEM32\NLTEST.EXE	Last Run Time (last execution date and time)

- Details: Domain Controller

- Event Log

#	Event log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. - **Protocol**: Protocol (udp) - **DestinationIp**: Destination IP address (source host IP address) - **Image**: Path to the executable file (C:\Windows\System32\lsass.exe) - **DestinationHostname**: Destination host name (source host name) - **ProcessGuid/ProcessId**: Process ID - **User**: Execute as user (NT AUTHORITY\SYSTEM) - **DestinationPort**: Destination port number (high port) - **SourcePort**: Source port number (389) - **SourceHostname**: Source host name (Domain Controller host name) - **SourceIp**: Source IP address (Domain Controller IP address)
	Security	5156	Filtering Platform Connection	The Windows Filtering Platform has allowed a connection. - **Network Information > Destination Port**: Destination port number (high port)

				• **Network Information > Source Port**: Source port number (389) • **Network Information > Destination Address**: Destination IP address (source host) • **Network Information > Protocol**: Protocol used (17=UDP) • **Application Information > Application Name**: Execution process (\device\harddiskvolume2\windows\system32\lsass.exe) • **Network Information > Direction**: Communication direction (inbound) • **Network Information > Source Address**: Source IP address (Domain Controller) • **Application Information > Process ID**: Process ID