



Windows API Exploitation Recipes for Red – Blue Teams

Vivek Ramachandran
Chief Trainer, Pentester Academy
<http://PentesterAcademy.com>

Process Token Dumper: Part 1

The Basics

What will you learn?

```
C:\Users\vivek\Documents\Visual Studio 2017\Projects\DumpProcessToken\Debug>DumpProcessToken.exe 788
[+] SeDebugPrivilege available for enabling![+] Enabled SeDebugPrivilege
Dumping token information for PID: 788
```

```
*****Dumping Privileges*****
```

#	Status	Privilege-Name
1.	Enabled	SeCreateTokenPrivilege [+]
2.	Disabled	SeAssignPrimaryTokenPrivilege [-]
3.	Enabled	SeLockMemoryPrivilege [+]
4.	Disabled	SeIncreaseQuotaPrivilege [-]
5.	Enabled	SeTcbPrivilege [+]
6.	Disabled	SeSecurityPrivilege [-]
7.	Disabled	SeTakeOwnershipPrivilege [-]
8.	Disabled	SeLoadDriverPrivilege [-]
9.	Enabled	SeSystemProfilePrivilege [+]
10.	Disabled	SeSystemtimePrivilege [-]
11.	Enabled	SeProfileSingleProcessPrivilege [+]
12.	Enabled	SeIncreaseBasePriorityPrivilege [+]
13.	Enabled	SeCreatePagefilePrivilege [+]
14.	Enabled	SeCreatePermanentPrivilege [+]
15.	Disabled	SeBackupPrivilege [-]
16.	Disabled	SeRestorePrivilege [-]
17.	Disabled	SeShutdownPrivilege [-]
18.	Enabled	SeDebugPrivilege [+]
19.	Enabled	SeAuditPrivilege [+]
20.	Disabled	SeSystemEnvironmentPrivilege [-]
21.	Enabled	SeChangeNotifyPrivilege [+]
22.	Disabled	SeUndockPrivilege [-]
23.	Disabled	SeManageVolumePrivilege [-]
24.	Enabled	SeImpersonatePrivilege [+]
25.	Enabled	SeCreateGlobalPrivilege [+]
26.	Disabled	SeTrustedCredManAccessPrivilege [-]
27.	Disabled	SeRelabelPrivilege [-]
28.	Enabled	SeIncreaseWorkingSetPrivilege [+]
29.	Enabled	SeTimeZonePrivilege [+]
30.	Enabled	SeCreateSymbolicLinkPrivilege [+]
31.	Enabled	SeDelegateSessionUserImpersonatePrivilege [+]

```
*****
```

```
C:\Users\vivek\Documents\Visual Studio 2017\Projects\DumpProcessToken\Debug>
```



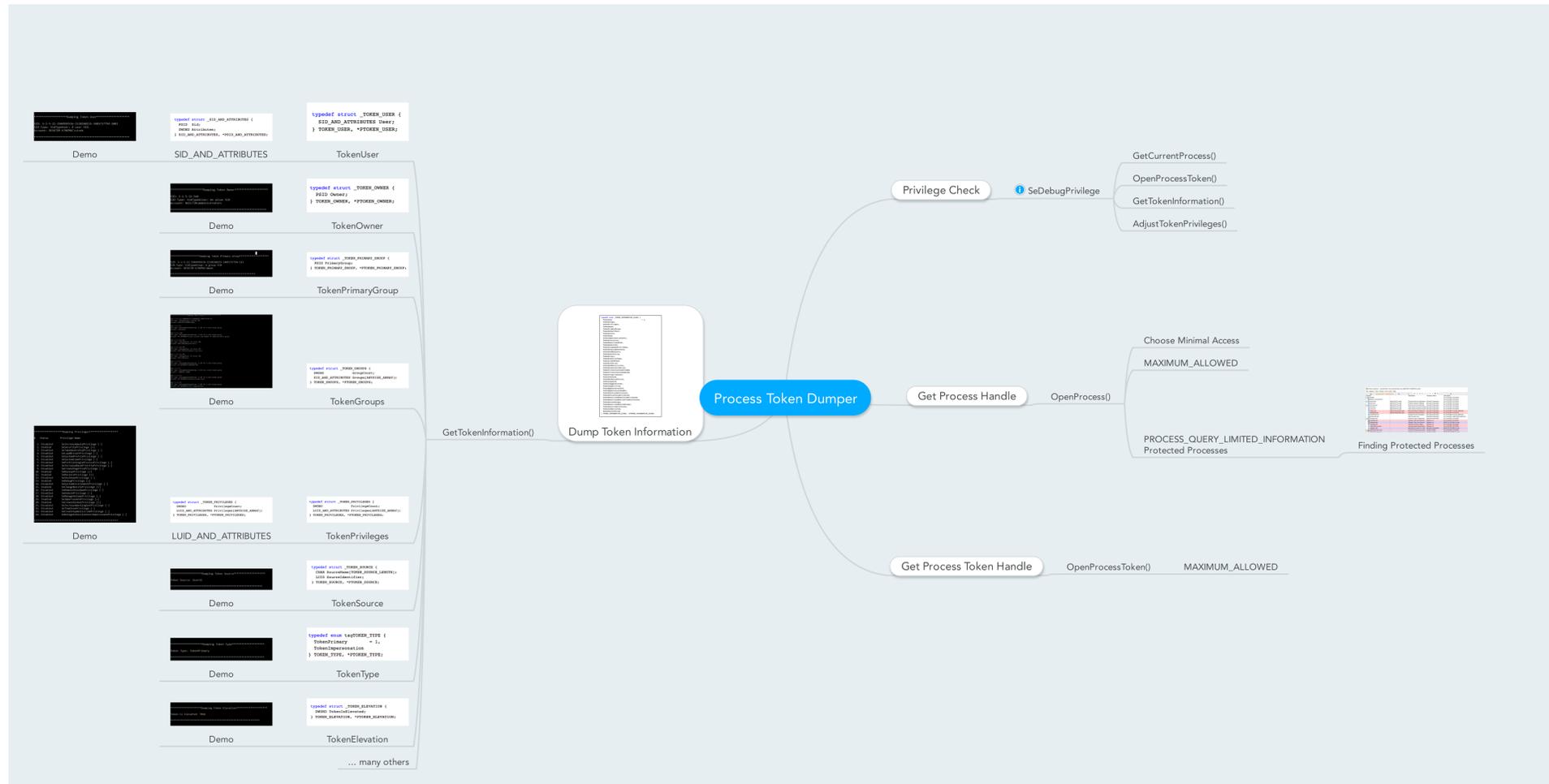
What will you learn?

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-K70EMVC\vivek]

File Options View Process Find Users Help

Process	Description	Company Name
System		
Memory Compression		
wininit.exe	SignerWinTcb-Light	Windows Start-Up Application Microsoft Corporation
smss.exe	SignerWinTcb-Light	Windows Session Manager Microsoft Corporation
services.exe	SignerWinTcb-Light	Services and Controller app Microsoft Corporation
csrss.exe	SignerWinTcb-Light	Client Server Runtime Process Microsoft Corporation
csrss.exe	SignerWinTcb-Light	Client Server Runtime Process Microsoft Corporation
NisSrv.exe	SignerAntimalware-Light	Microsoft Network Realtime I... Microsoft Corporation
MsMpEng.exe	SignerAntimalware-Light	Antimalware Service Execut... Microsoft Corporation
WUDFHost.exe		Windows Driver Foundation -... Microsoft Corporation
WmiPrvSE.exe		WMI Provider Host Microsoft Corporation
winlogon.exe		Windows Log-on Application Microsoft Corporation
vmtoolsd.exe		VMware Tools Core Service VMware, Inc.
vmtoolsd.exe		VMware Tools Core Service VMware, Inc.
vmacthlp.exe		VMware Activation Helper VMware, Inc.
VGAAuthService.exe		VMware Guest Authenticatio... VMware, Inc.

Token Dumper MindMap



Thank You!

PentesterAcademy

a SecurityTube.net initiative

Follow @SecurityTube 89.6K followers

Recommend Share 311K

