

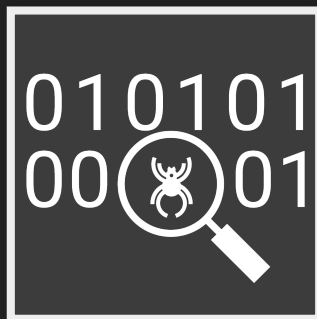
WINDOWS PENTESTING

ANALYZING THE ATTACKERS TOOLBOX

Created by Ben Burkhart and Jim Holcomb

ABOUT EVOLVE SECURITY

- Application Security
- Continuous Penetration 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

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

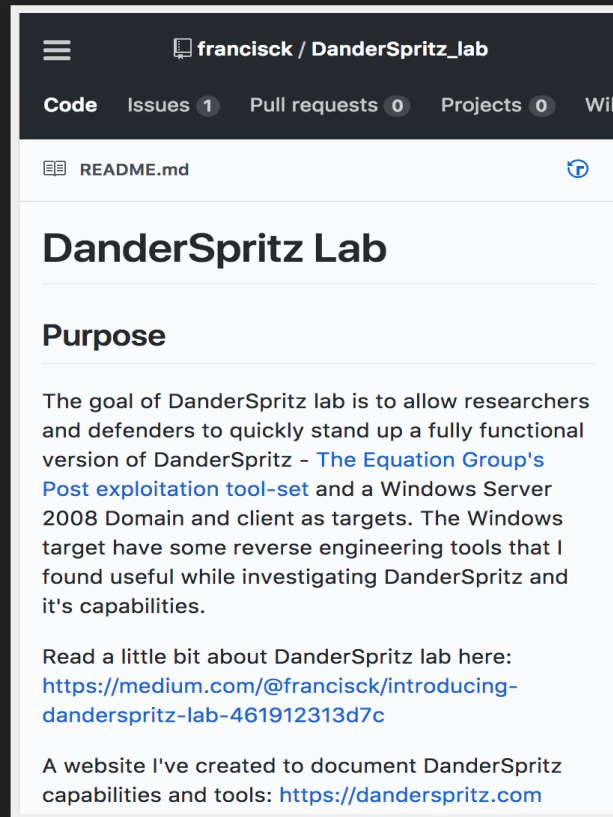
SETTING UP OUR LAB

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

EXAMPLE LABS

- Metasploitable3 ([link](#))
- Danderspritz 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/10240.163
84.150709-1700.TH1_CLIENTENTERPRISEVAL_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/75EC4E
54-5B02-42D6-8879-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

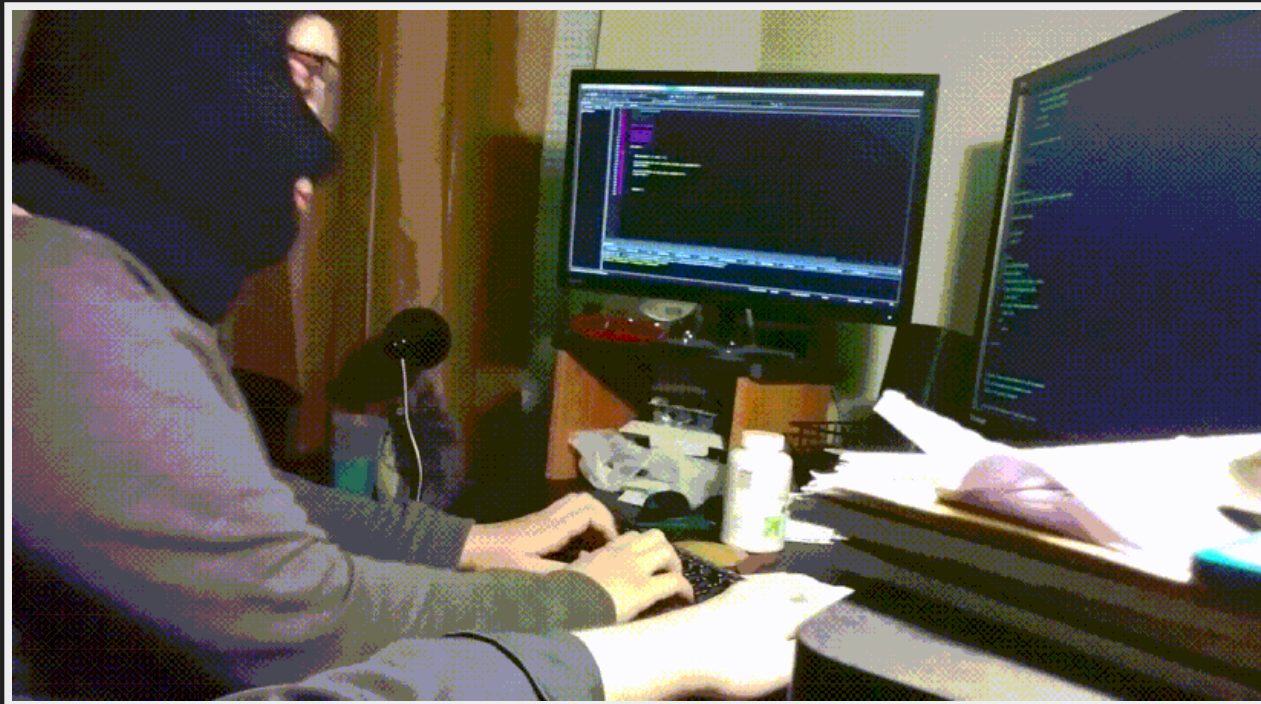
DEPLOYING IMAGES (TERRAFORM / VAGRANT)

- 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)

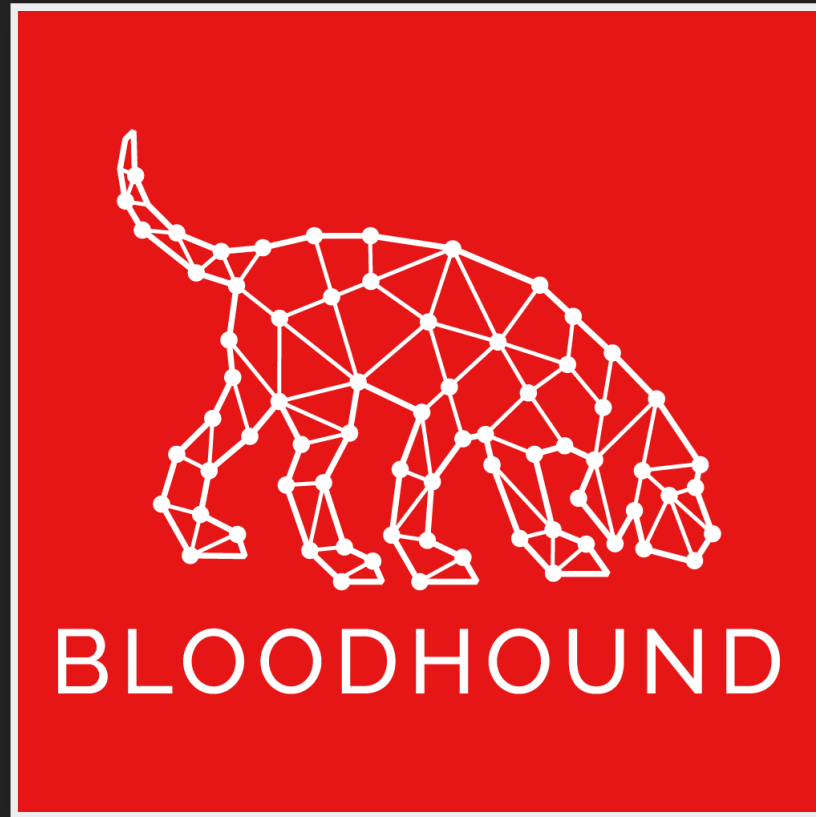
- MS08-067 - RPC Request Buffer Overflow = RCE
- MS12-020 - Remote Desktop Use After Free
- MS17-010 - ETERNALBLUE / Shadow Brokers NSA Leak

COMMON MISCONFIGURATIONS

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

GAINING ACCESS: DEMO

ENUMERATING WITH BLOODHOUND



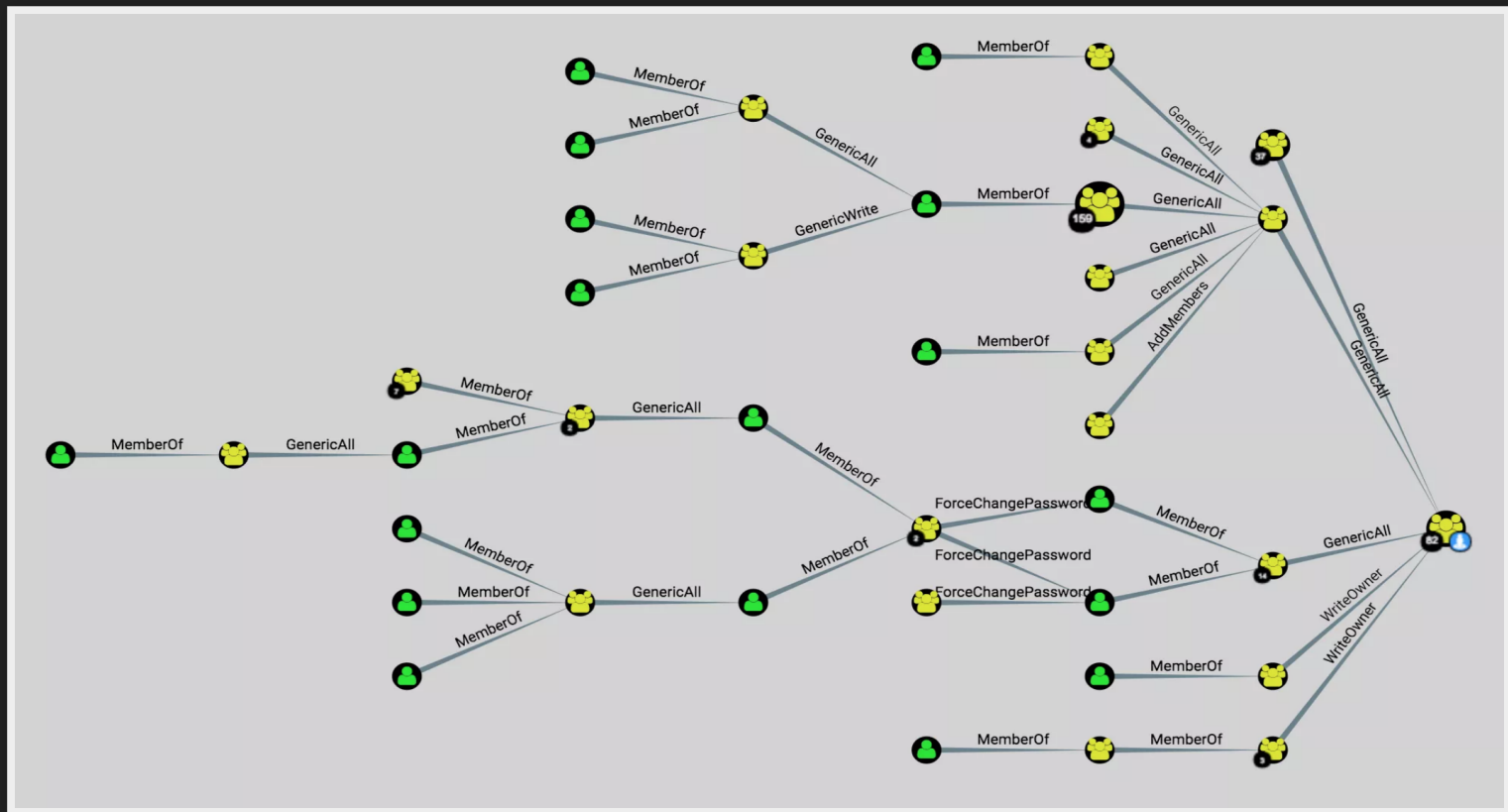
ENUMERATING WITH BLOODHOUND

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

- 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

ENUMERATION DEMO: BLOODHOUND

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

DEMO: POWERSPLOIT

ESTABLISHING PERSISTENCE: EMPIRE

```

      .-:./+
    -+sydmNNNNNNNNNN
  . /ymmNNNNNNNNNNNN
 -ymmNNNNNNNNNNNNNN
ommmNNNNNNNNNNNNNN
 .ydmNNNNNNNNNNNNNN
odmmNNNNNNNNNNNNNN
 /hmmNNNNNNNNNNNNNN
 +hmmNNNNNNNNNNNNMM
 .ymmNNNNNNNNNNNNNN
 .+so+//:---.----:!--
 .-:./+
 -/osy+///:---.---dNNNN
 :sdyyydy` `:mNNNNM
 -hmdhdmm:` `+hNNNNNNM
odNNmdmmNN` `:yNNNNNNNNN
-sNNNNmdh/dNNhhNNNNNNNNNNNN
-hNNNNmNo:mNNNNNNNNNNNNNNNN
-hNNmdNo--/dNNNNNNNNNNNNNNNN
:dNmdmd-:+NNNNNNNNNNNNNNNm
/hNNmdmd+mNNNNNNNNNNNNds++o
/dNNNNNNmmmmmmNNNNNNNNNNmdoosydd
sNNNNdydNNNNmmmmmmNNNNmYoymNNNNN
:NNmmmdso++dNNNNmmNNNNdhymNNNNNNN
-NmdmmNNdsyohNNNNmmNNNNNNNNNNNNNN
sdhmmNNNNdyhdNNNNNNNNNNNNNNNNNN
 /yhmNNmmNNNNNNNNNNNNNNNNNNmmh
 +ymmmNNNNNNNNNNNNNNNNNNmmh+:
 . /dmmmmNNNNNNNNNNNNNNmmmd.
ommmmmNNNNNNNNmmNNNNmmmd:
 :dmmmmNNNNNmh. /oyhhhy:
 `sdmmmmNNNNmmh/++-.+oh.
 `dmmmmmmmdo-:/ossd:
 /ohhdmmmmmddddmh/
  -/osyhdddddhyo:
    .-:./+

```

Welcome to the 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

- 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 without 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 user logs in
- Establishes a new connection to remote Empire C2 server

ESTABLISHING PERSISTENCE: DEMO

DATA EXFILTRATION: DEMO

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