MWR Labs

++

Privilege Escalation

Nick Jones

20th March 2017

MWR LABS

MWR LABS

++

Who am I?

Nick Jones

+ Security Consultant at MWR InfoSecurity
+ Web Applications and Infrastructure Assessments

Research Topics:

+ Cloud/DevOps
+ Malware Command and Control

MWR LABS

++

Who are MWR InfoSecurity?

A global, research-led cybersecurity consultancy

+ Global – 3 UK offices + US, Singapore, South Africa, Poland
+ Research-led – everyone gets research time, even juniors
+ Cybersecurity consultancy – help clients secure their networks, get paid to hack things

MWR LABS

++

Why are we Awesome?

Lots of good people, fun place to work

+ Multiple Pwn2Own wins, talks at Black Hat, DEF CON etc

HackFu

+ Annual two-day hacking challenge

MWRICON

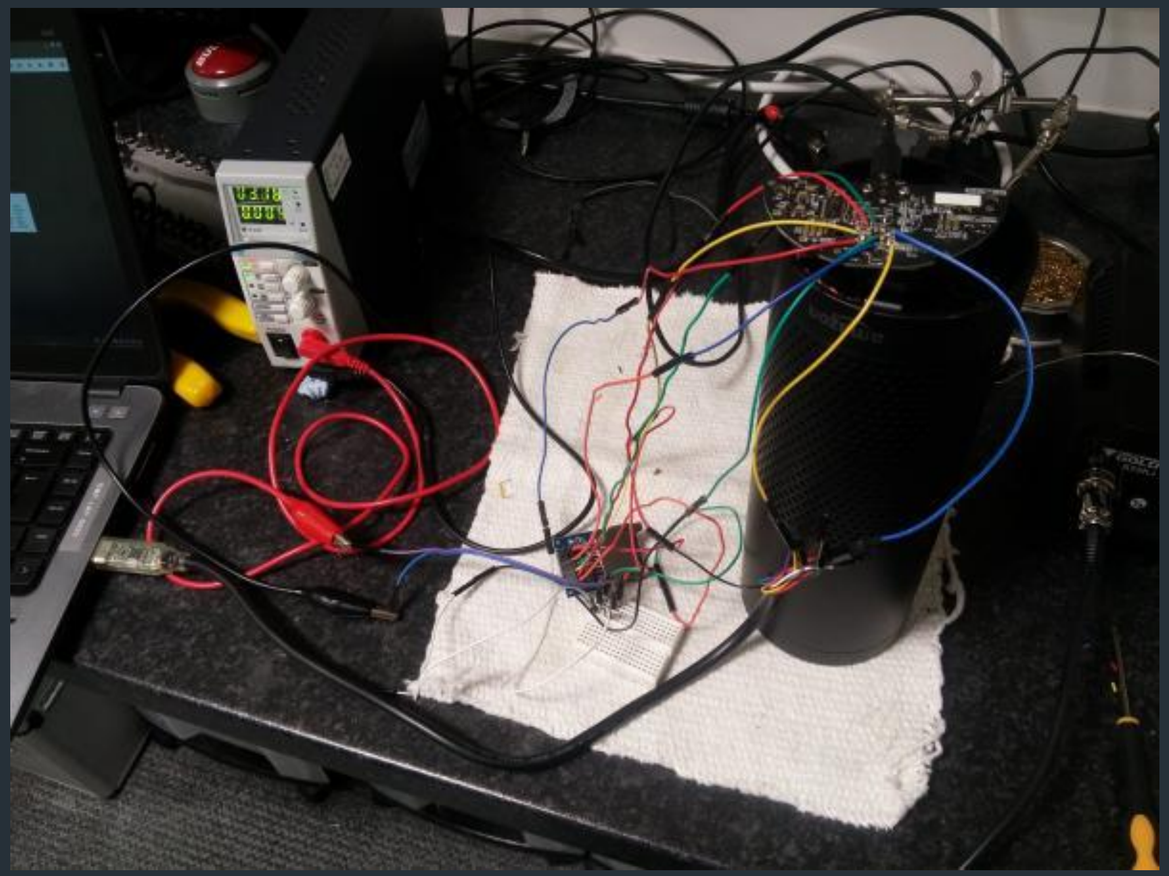
+ Annual internal conference - talks and workshops from our consultants

++

Research

Amazon Alexa

+ Exposed debug ports + SD card booting = root

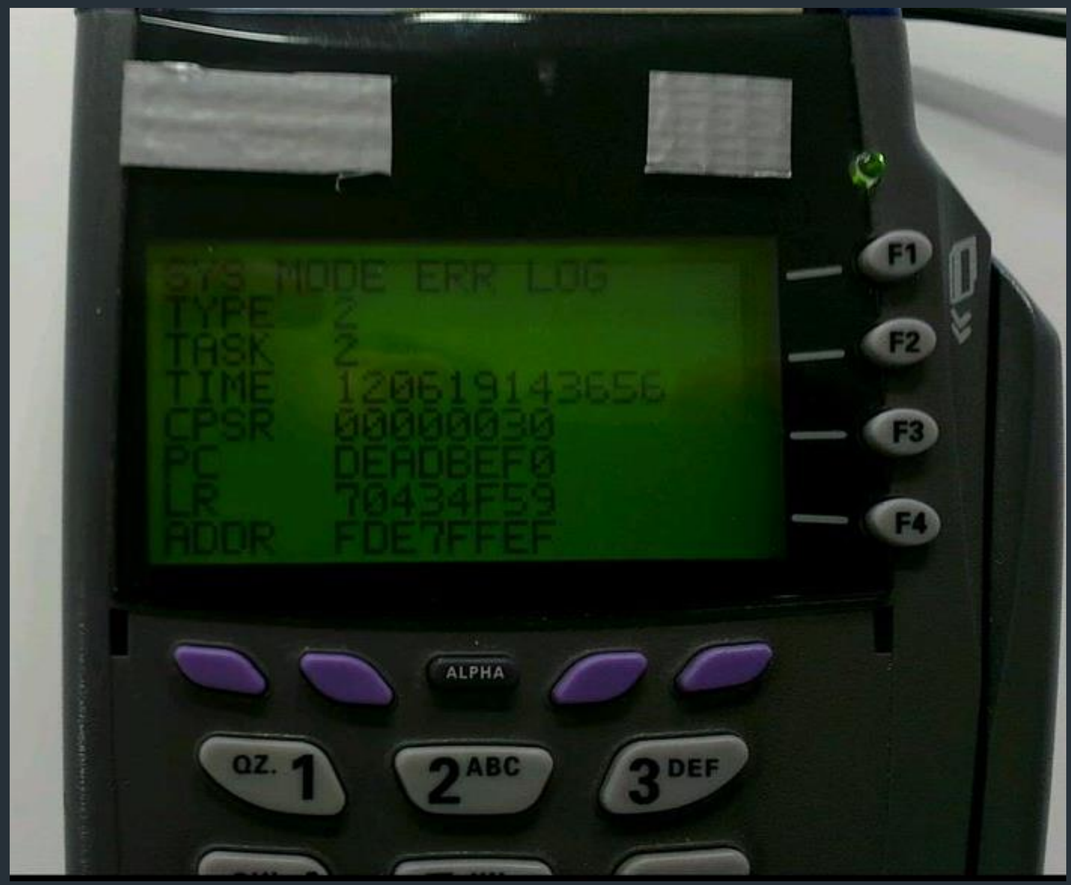


MWR LABS

++

Why are we Awesome?

+ Buffer overflow on credit card reader led to…

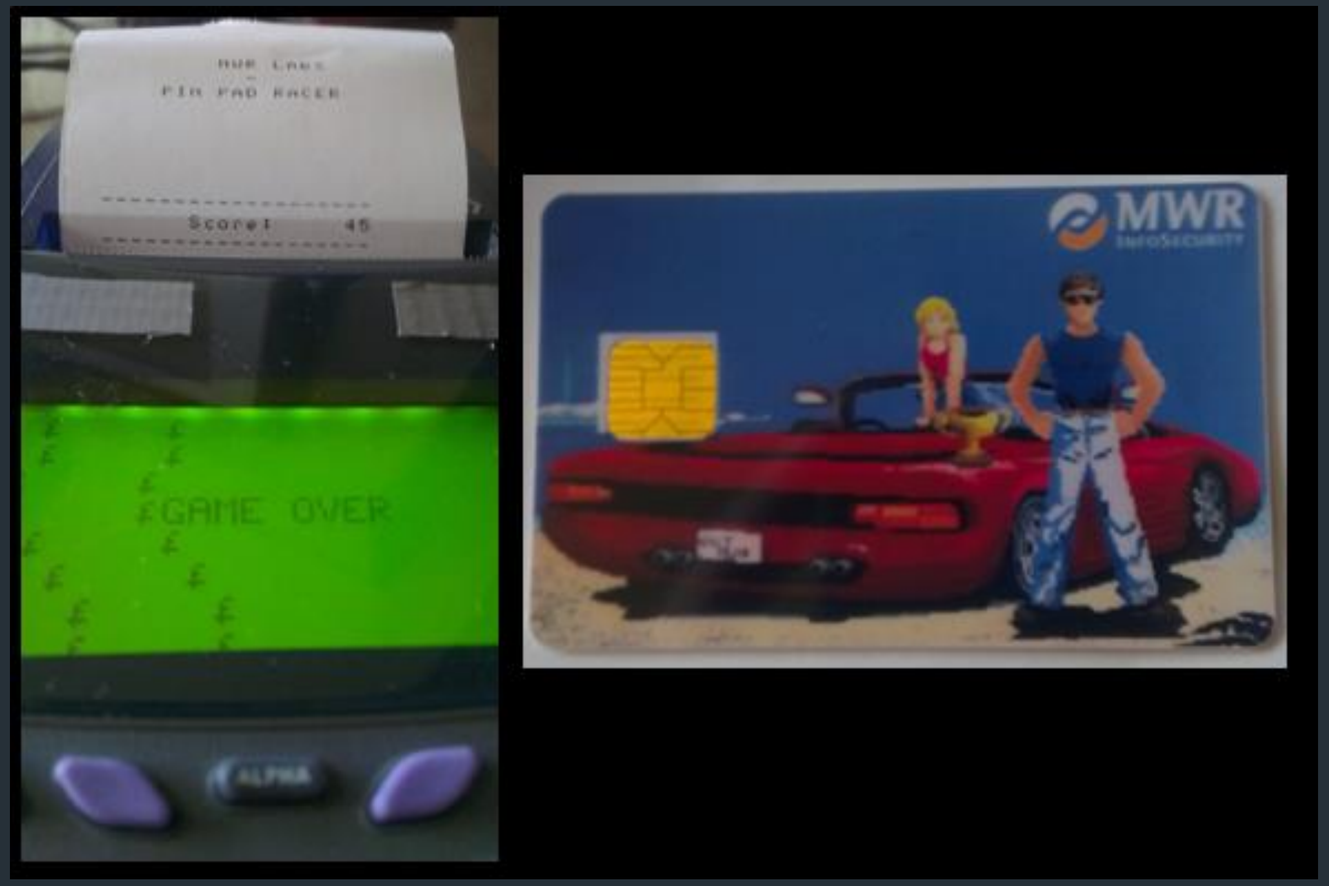


MWR LABS

++

Why are we Awesome?

+ Flappy Bird!
+ Game loads off malicious chip & pin card
+ Insert card, play game



MWR LABS

++

What is Privilege?

The level of access that a user or application has

+ The files or data they can read/write
+ The programs they can run
+ The hardware they can interface with

MWR LABS

++

Why Escalate it?

Perform actions we're not supposed to

+ Read/write files we currently can't access
+ Execute programs we currently can't run
+ Access devices we can't currently communicate with

MWR LABS

++

Types of Escalation

Vertical

+ Extra privileges
+ Normal user -> admin/root

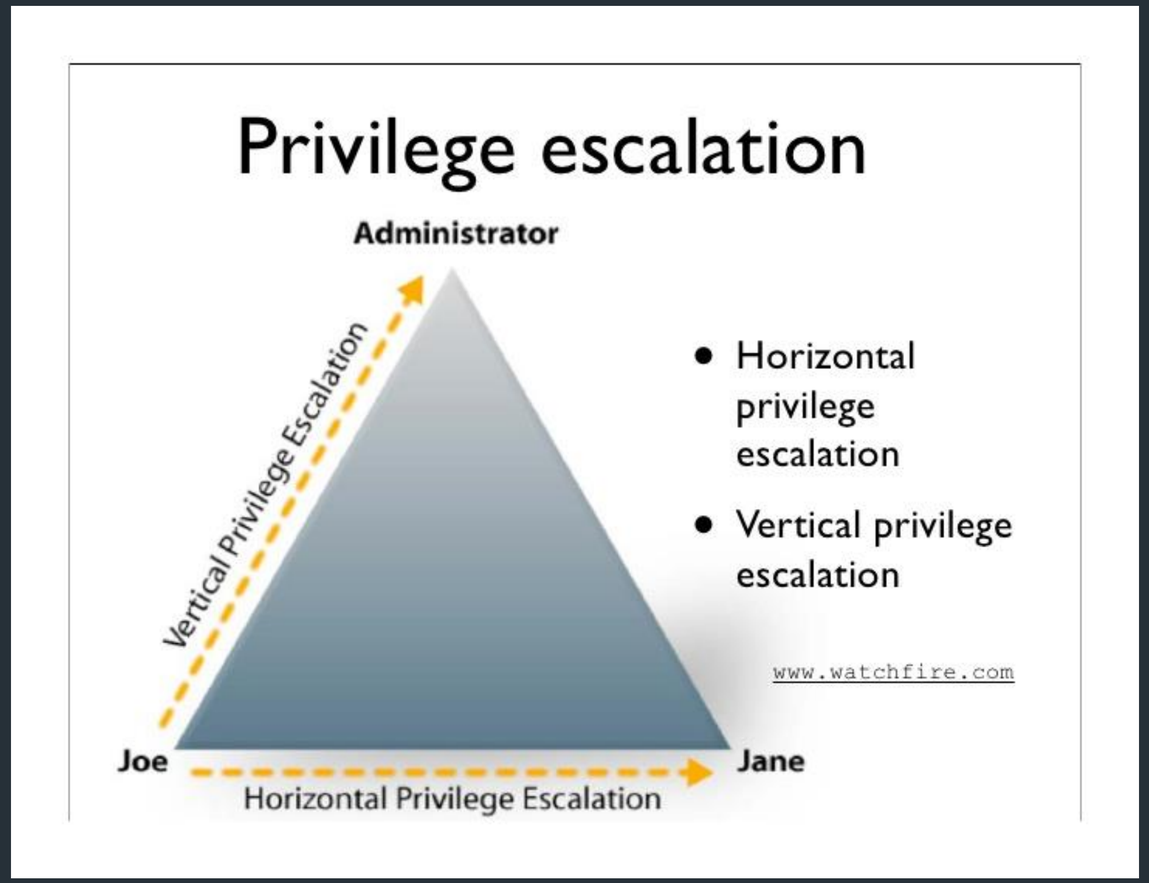
Horizontal

+ Access rights of a different user the same level

MWR LABS

++

Horizontal vs Vertical



MWR LABS

++

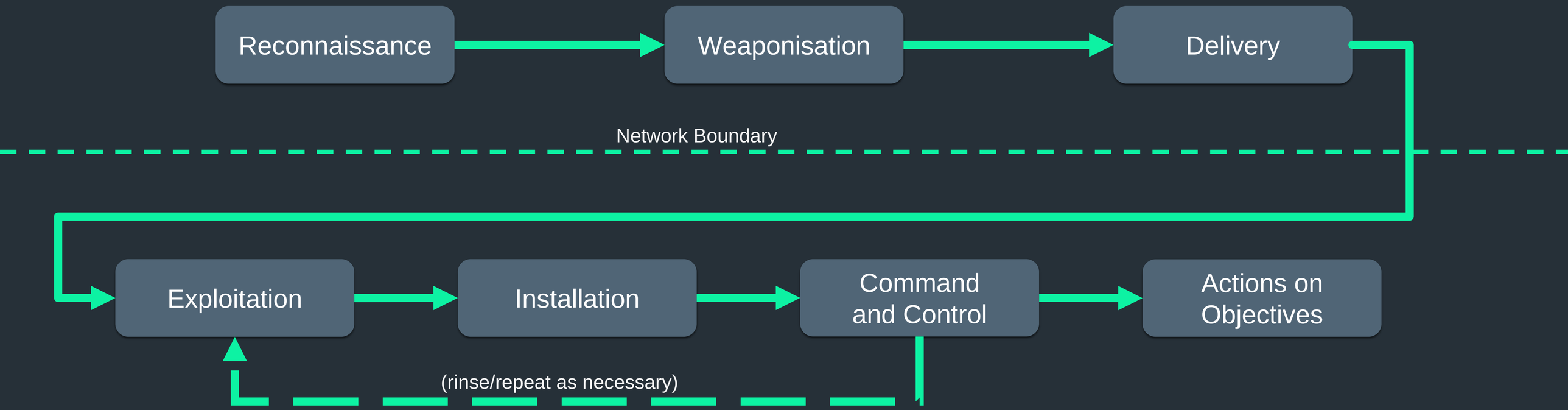
Why Escalate Horizontally?

+ Amazon – purchase on someone else's card
+ Online Banking – move money around from someone else's account
+ Student Management Systems – view someone else's grades

More generally, they may have files, emails, etc. containing passwords, or other useful info

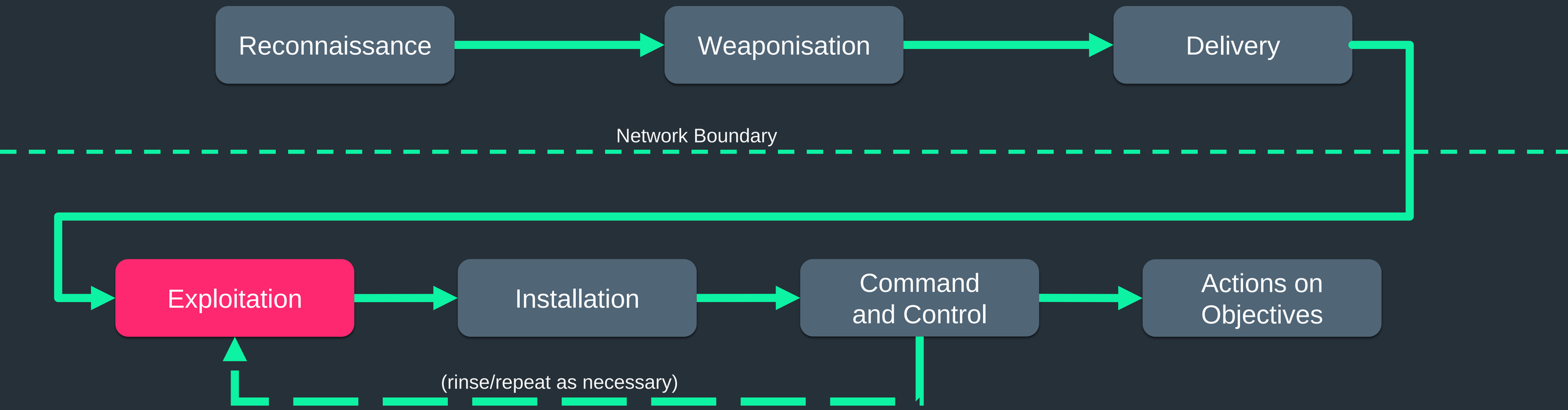
++

Attack Paths – The Cyber Killchain



++

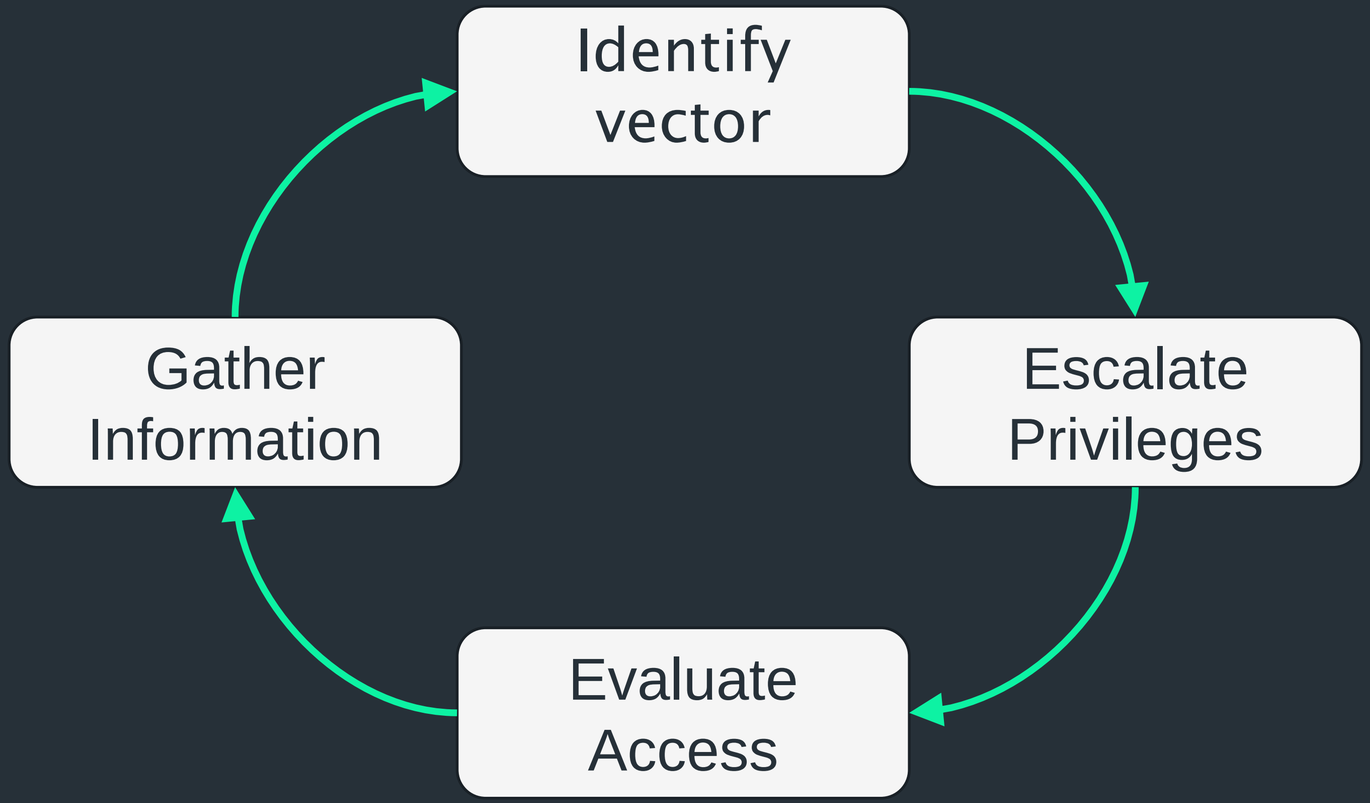
Attack Paths – The Cyber Killchain



MWR LABS

++

What is the Process?



MWR LABS

++

What is the Process?

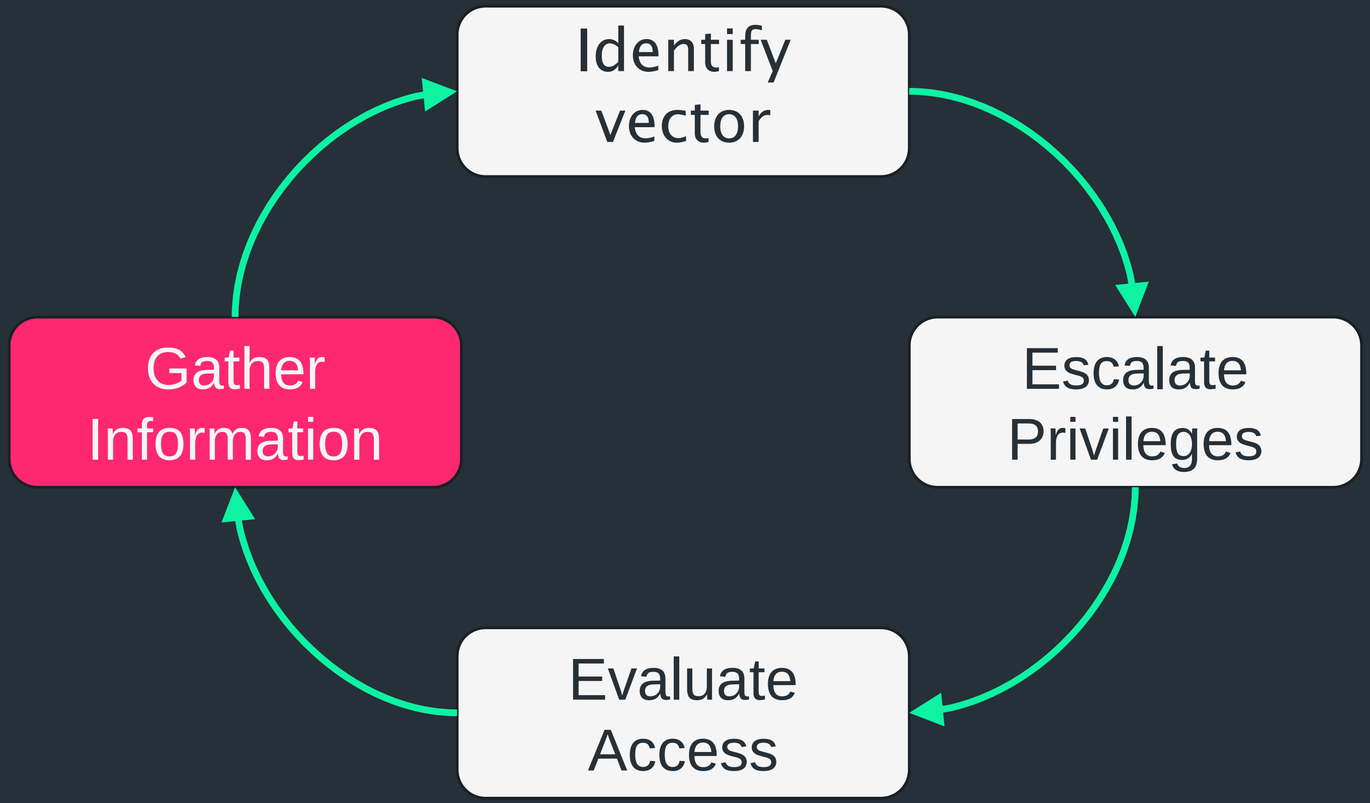
You may need to repeat this process multiple times.

+ Web app: normal user -> app administrator -> root
+ Windows: Low integrity -> local user -> SYSTEM
+ Linux: user -> root -> root on another box

MWR LABS

++

What is the Process?



MWR LABS

++

Gather Information

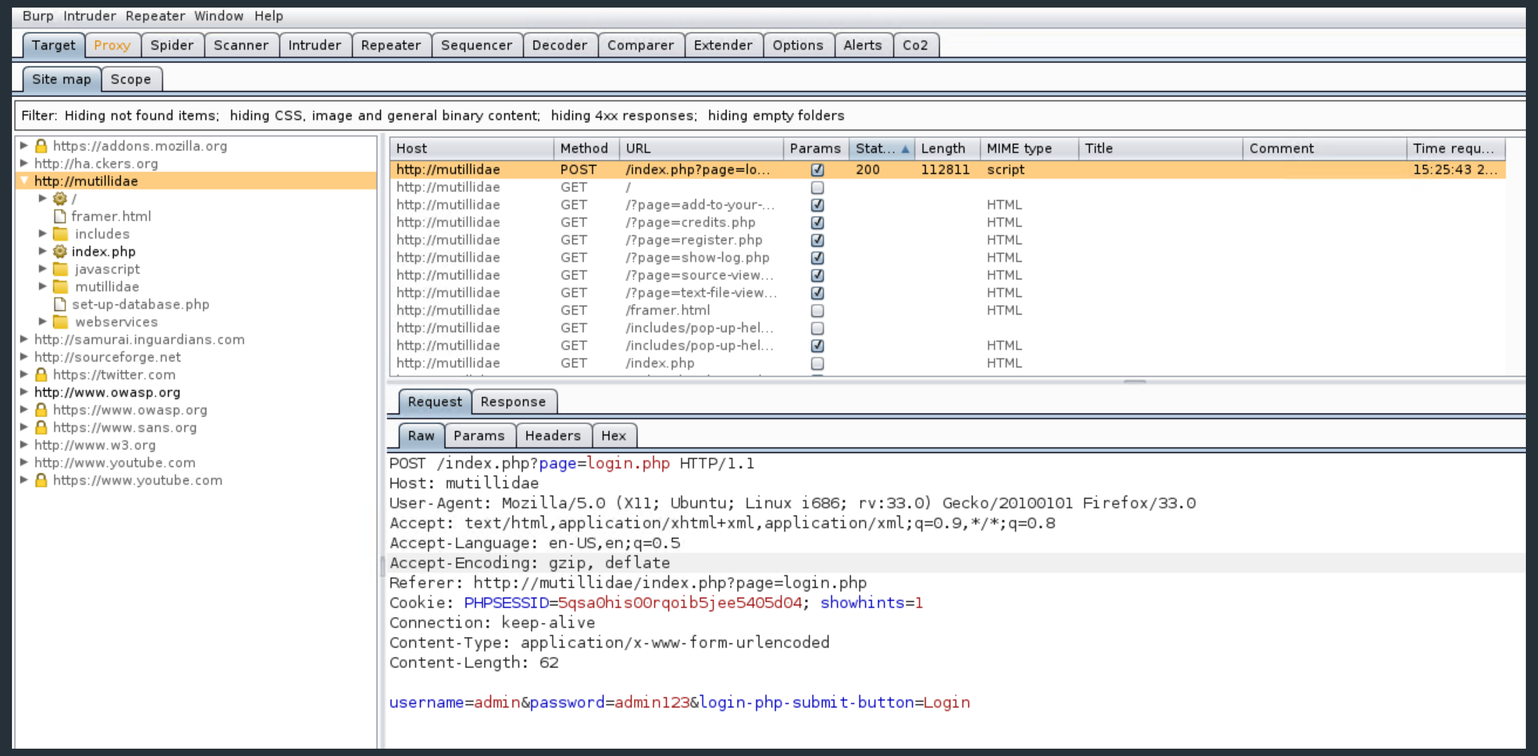
+ Otherwise known as reconnaissance, or enumeration
+ Details of the system, software, users, network…
+ More information -> better chance of finding an escalation vector
+ What information is useful?

MWR LABS

++

What information is useful – Web Apps

A site map



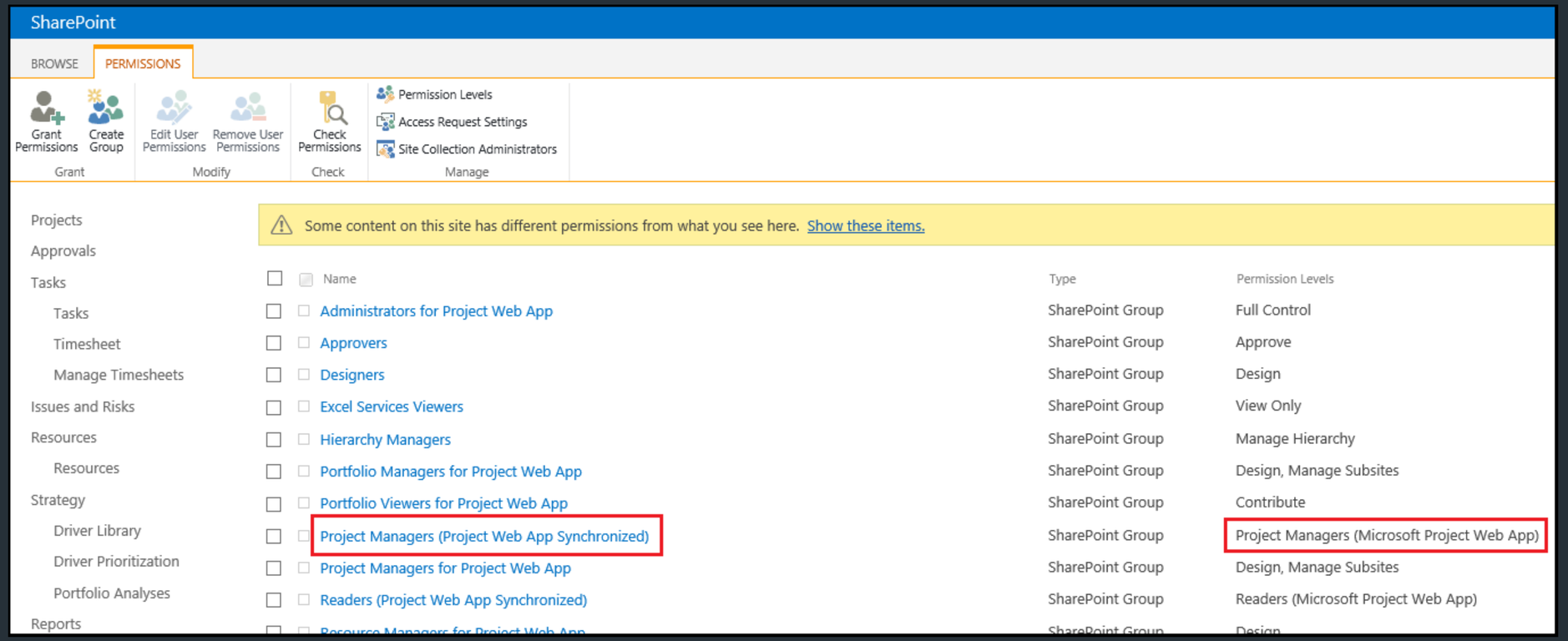
https://azeemnow.wordpress.com/2016/02/17/samuraiwtf-and-burp/

MWR LABS

++

What information is useful – Web Apps

Permissions models



http://www.mpug.com/articles/managing-project-web-app-site-permissions-project-online-project-server-2013/

MWR LABS

++

What information is useful – Web Apps

Technical information

+ What language is it built in?
+ What frameworks have they used?
+ What databases does it communicate with?
+ Are there any perimeter defences (firewalls, WAFs etc)?

MWR LABS

++

What information is useful? - Windows/Linux

+ Which version of the OS is this?
+ What users are on the system? Who am I currently?
+ Installed software and devices
+ Network information, routing tables, firewall rules etc
+ Services/daemons and their permissions
+ Scheduled Tasks/cron etc.

MWR LABS

++

Web app reconnaissance tools

+ A web browser
+ Application help pages
+ An intercepting proxy - Burp Suite/ZAP/Fiddler
+ Nmap
+ Nikto/Arachni/Netsparker/{insert app scanner here}

MWR LABS

++

Windows reconnaissance tools

+ Native windows commands/GUI components - systeminfo, net, netstat, tasklist, services.msc...
+ WMIC
+ PowerSploit's PowerUp modules
+ Metasploit's Windows Post-Exploitation Modules
+ Sysinternals Suite
+ Windows-exploit-suggester / windows-privesc-check

MWR LABS

++

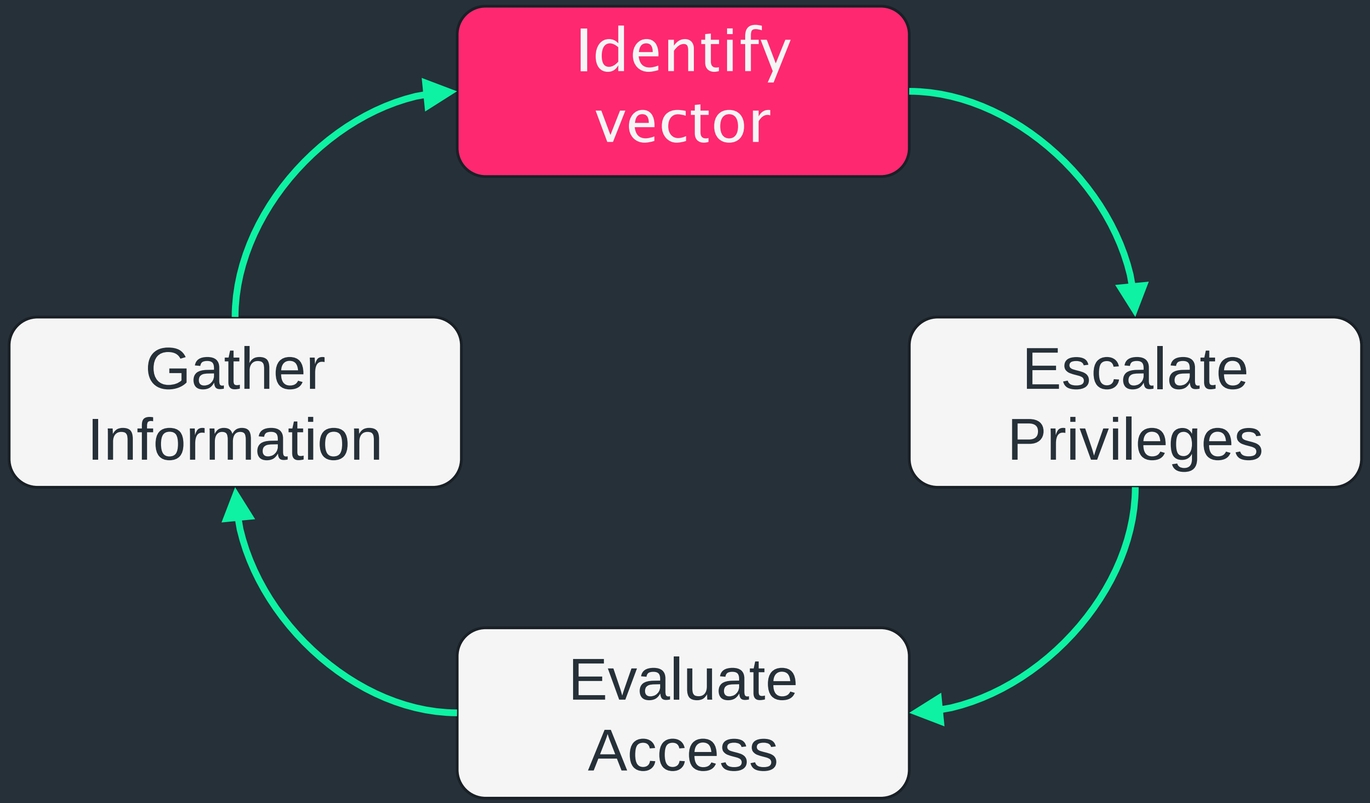
Linux reconnaissance tools

+ Native Linux commands – service/init.d, ps, netstat…
+ Digging through log/config files - /etc/passwd, .bash_history, service config…
+ Metasploit's Linux Post-Exploitation Modules
+ Linuxprivchecker.py
+ LinEnum
+ Unix-privesc-check

MWR LABS

++

What is the Process?



MWR LABS

++

Identify escalation vector

Review gathered information, identify your options

Pick a vector based on your requirements

+ Test Environment? Pick the easiest
+ Production environment? Pick one that won't break things
+ Need to be stealthy? Pick something that'll blend in

MWR LABS

++

Examples of Escalation Vectors

+ Authorisation bypasses
+ Poor passwords / password reuse
+ Misconfiguration
+ Exploits
+ Design flaws

MWR LABS

++

Authorisation bypasses

Escalate by accessing privileged content, without the necessary rights

+ Direct object referencing
+ Admin:true in a web cookie
+ Interacting with Android app IPC endpoints that should be locked down

MWR LABS

++

Poor Passwords/Password Reuse

Guess or crack an account's passwords, try passwords you've found elsewhere

+ Pa55w0rd on a windows domain admin account
+ Use XSS to Keylog someone's credentials, password also used on their email account
+ Password spraying – try a known or common user/password on other systems
+ Brute-force – guess until you find it, last resort

MWR LABS

++

Misconfiguration

Someone's misconfigured a service, file permissions, server hardening features…

+ Windows: No software restriction policies, unquoted service paths, permissive service configuations…

+ Linux: suid files, writeable authorized_keys files, readable private keys, cron jobs with world writeable scripts…

MWR LABS

++

Exploits

Poorly written code -> privilege escalation

+ Not just in apps, check OS, libraries in use, etc.
+ Jailbreaks are a form of exploit-related privilege escalation
+ Be careful here – exploits often unstable, may crash apps/systems

MWR LABS

++

Design Flaws

Flaws in the design of applications and protocols

+ Hard to patch
+ Usually low-risk

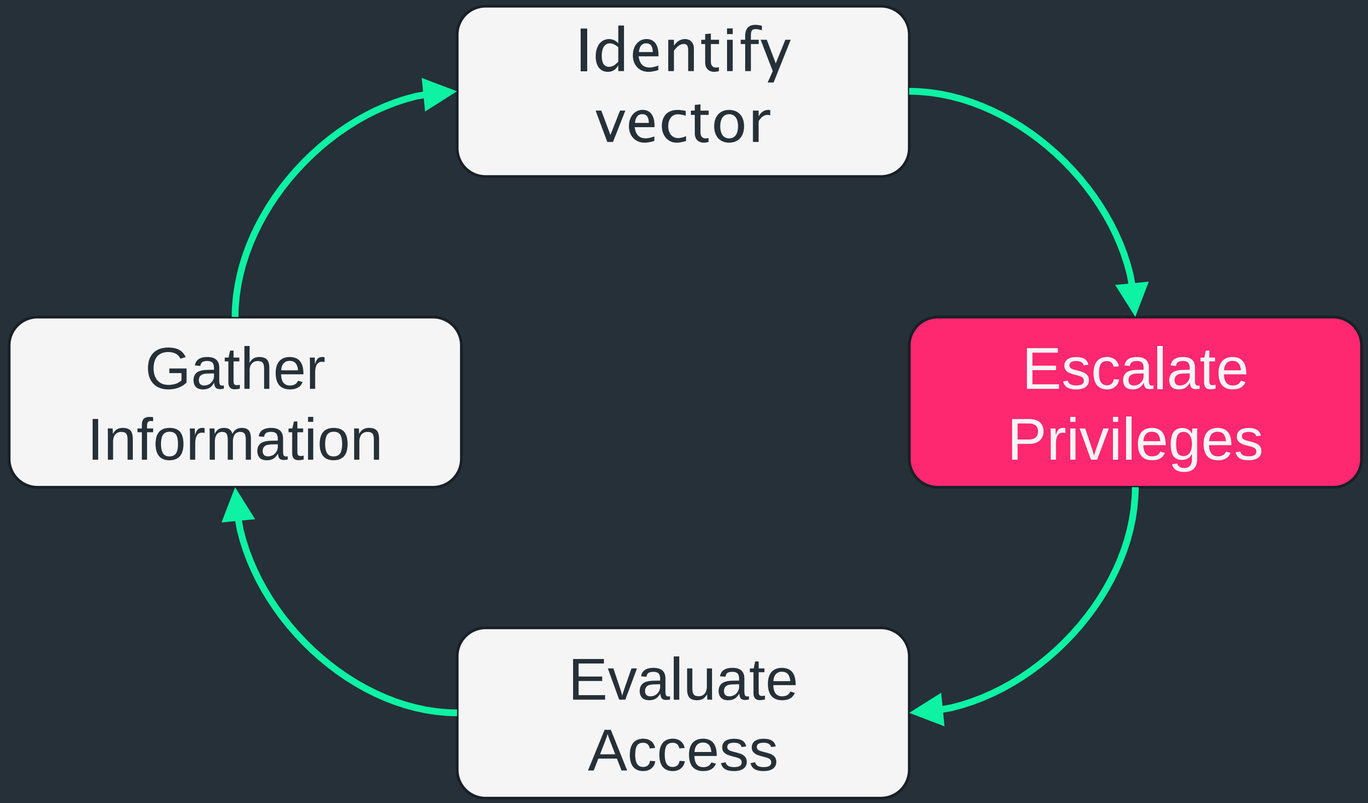
Great example from one of our interns

+ Unintended feature in Microsoft Exchange ActiveSync
+ Valid email account -> read from any file share on an internal network

MWR LABS

++

What is the Process?



MWR LABS

++

Escalate

Exploit the identified vectors

Important to consider potential side effects

+ If exploiting a code bug, will this crash the app?
+ If trying to be stealthy, will this be spotted by EDR, threat hunters or incident responders?

MWR LABS

++

Escalate - Examples

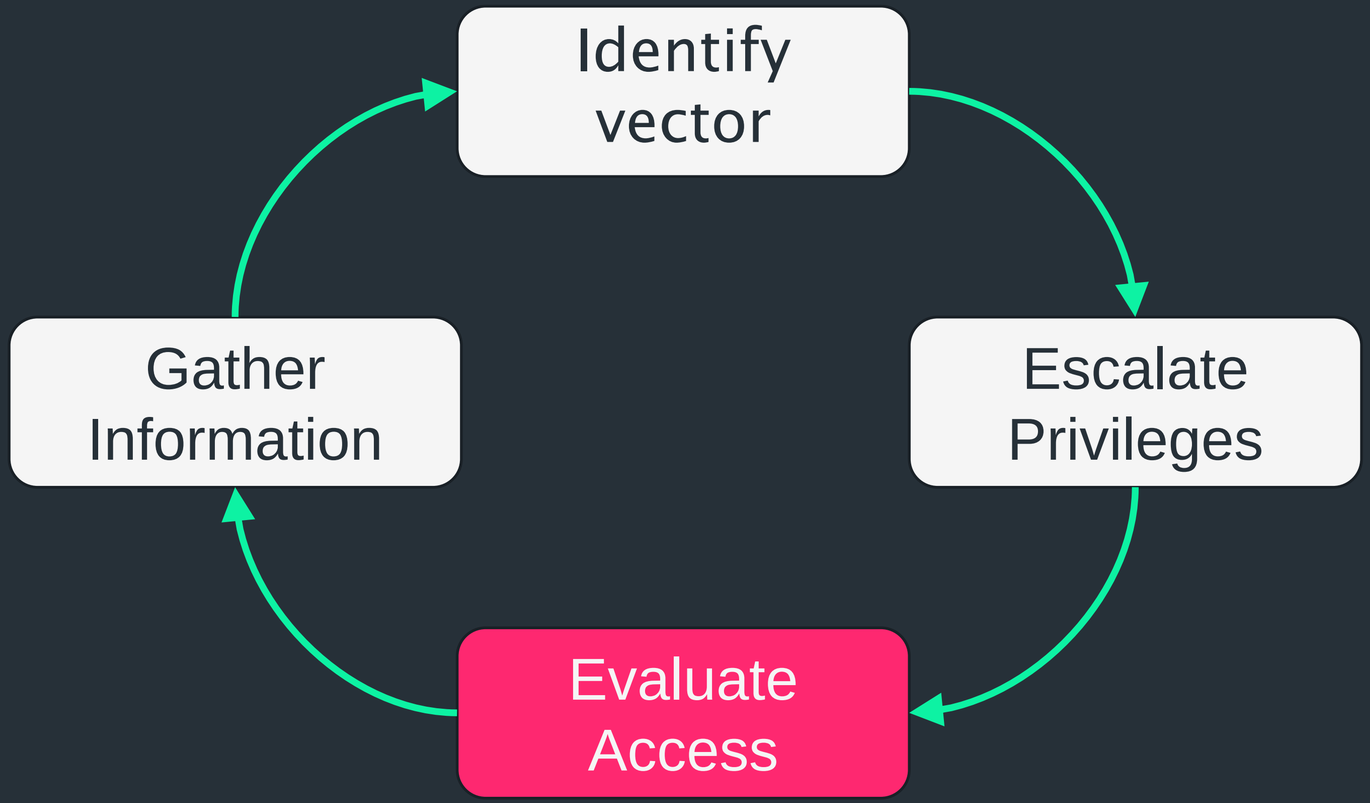
Launch the privilege escalation attack

+ Use an authorisation bypass
+ Log in with a cracked password
+ Run an exploit
+ Alter a windows service to run a malicious binary

MWR LABS

++

What is the Process?



MWR LABS

++

Evaluate Access

Do you have the access you wanted?

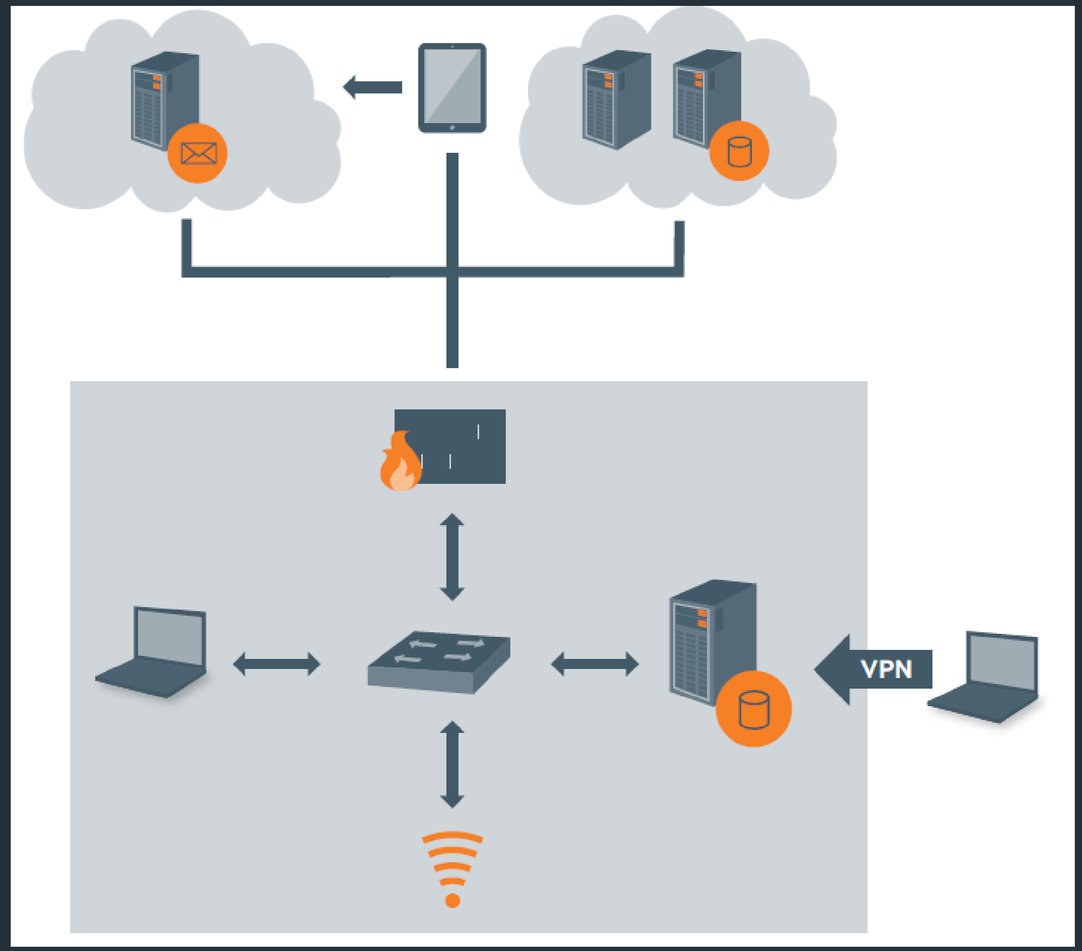
+ If yes, game over
+ If not, repeat the process

MWR LABS

++

Modern Enterprise Networks

+ Thousands of endpoints
+ Hundreds of servers
+ Mobile Devices
+ VPNs
+ Custom Apps



MWR LABS

++

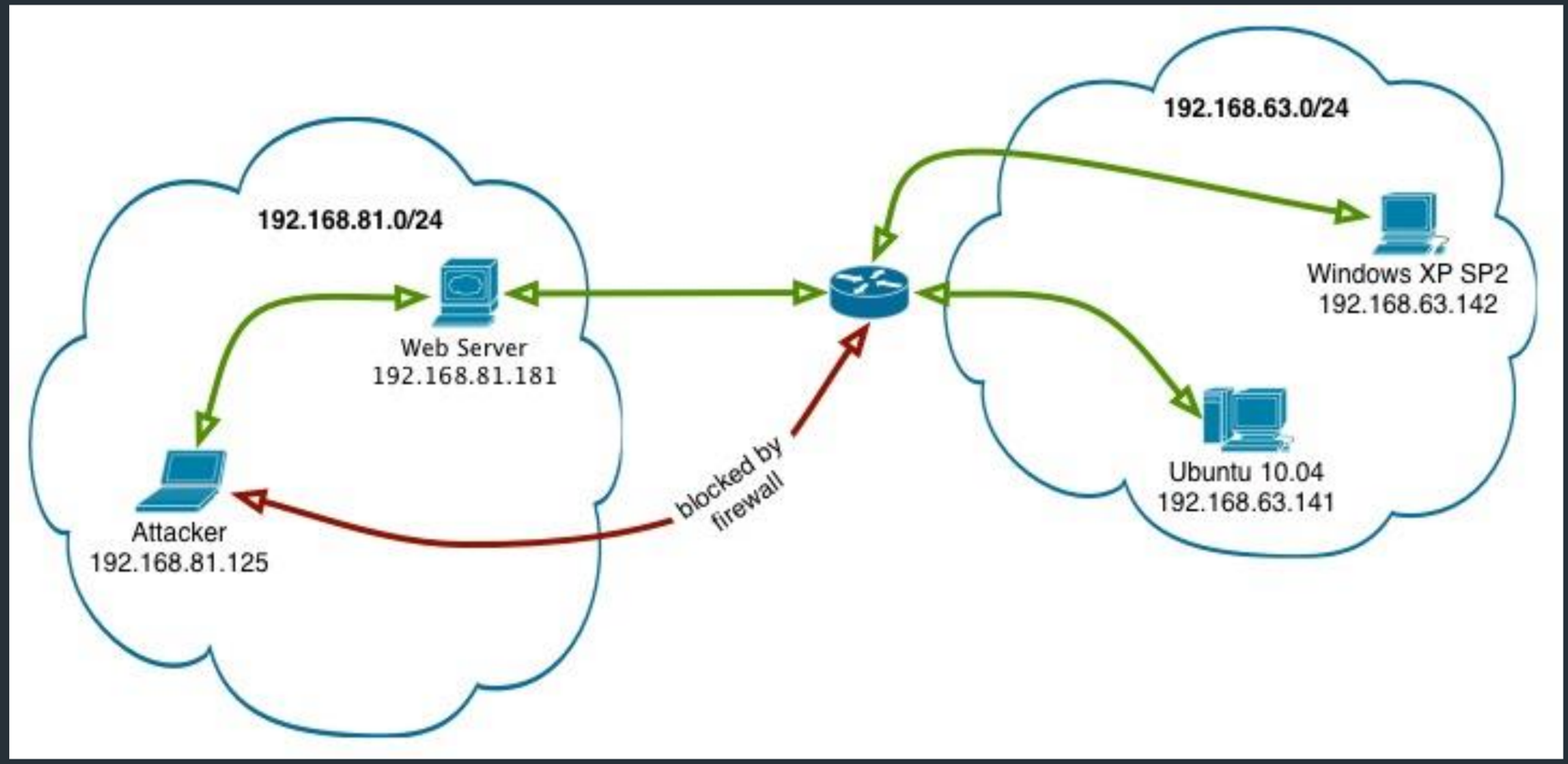
Modern Attacks

+ Sophisticated attacks are usually objective-based
+ Compromising one system is rarely enough
+ Escalate across multiple systems or applications
+ Pivot between systems to gain greater access

MWR LABS

++

Pivoting



https://blog.techorganic.com/2012/10/06/introduction-to-pivoting-part-1-ssh/

MWR LABS

++

Pivoting Techniques

Tunnel over:

+ VPN
+ SSH – port forwarding or SOCKS proxy
+ HTTP CONNECT proxy
+ …

MWR LABS

++

Escalation in Windows Domains

Active Directory

+ Centralised management for windows networks
+ Domain controller – server controlling authentication/authorisation
+ Domain admin – Admin on all systems within the domain

MWR LABS

++

Get Domain Admin, ???, Profit!

+ Identify domain admin accounts
+ Find active domain admin sessions
+ Gain administrative access on those systems
+ Steal their credentials or tokens

MWR LABS

++

Identifying Target Users and Systems

Can be done manually

+ Net user – find domain admins
  `net user “domain admins” /domain`

+ Net view – find all machines in the domain
  `net view /domain`

+ netsess.exe – who’s logged in on a machine?
  `netsess.exe \\<host>`

MWR LABS

++

PowerView

Automates most of this

+ Invoke-CheckLocalAdminAccess - Check if user is local admin on specified machine

```
Invoke-CheckLocalAdminAccess -ComputerName sqlserver
```

+ Invoke-UserHunter - Find where a user's logged in

```
Invoke-UserHunter -UserName "John Smith"
```

+ Invoke-UserHunter - Find all domain admin sessions where current user has admin access

```
Invoke-UserHunter -CheckAccess
```

MWR LABS

++

Bloodhound

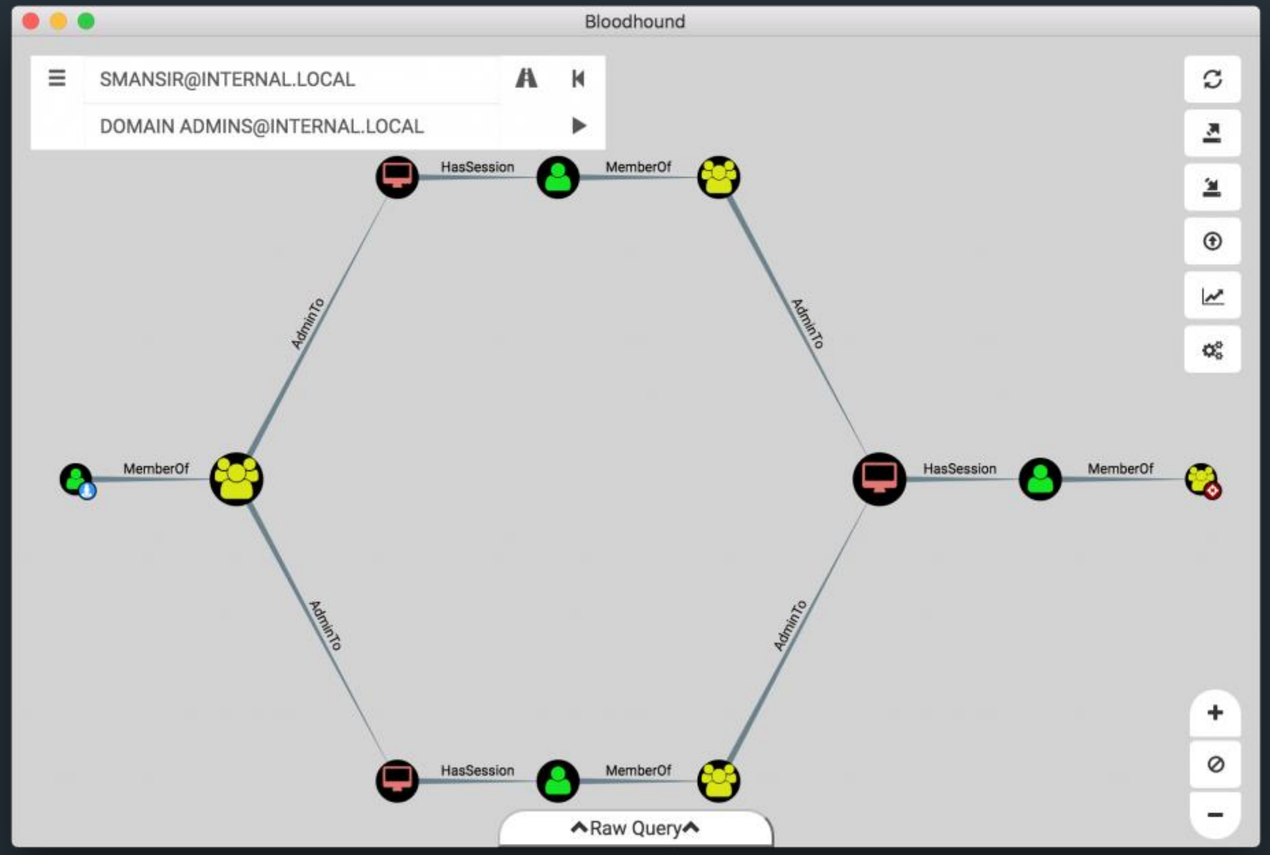
Enumerate windows domains and identify multi-hop paths to domain admin automatically

+ Collect data with the powershell ingestor
+ Load collected data into Bloodhound
+ Review graph for escalation routes

MWR LABS

++

Bloodhound



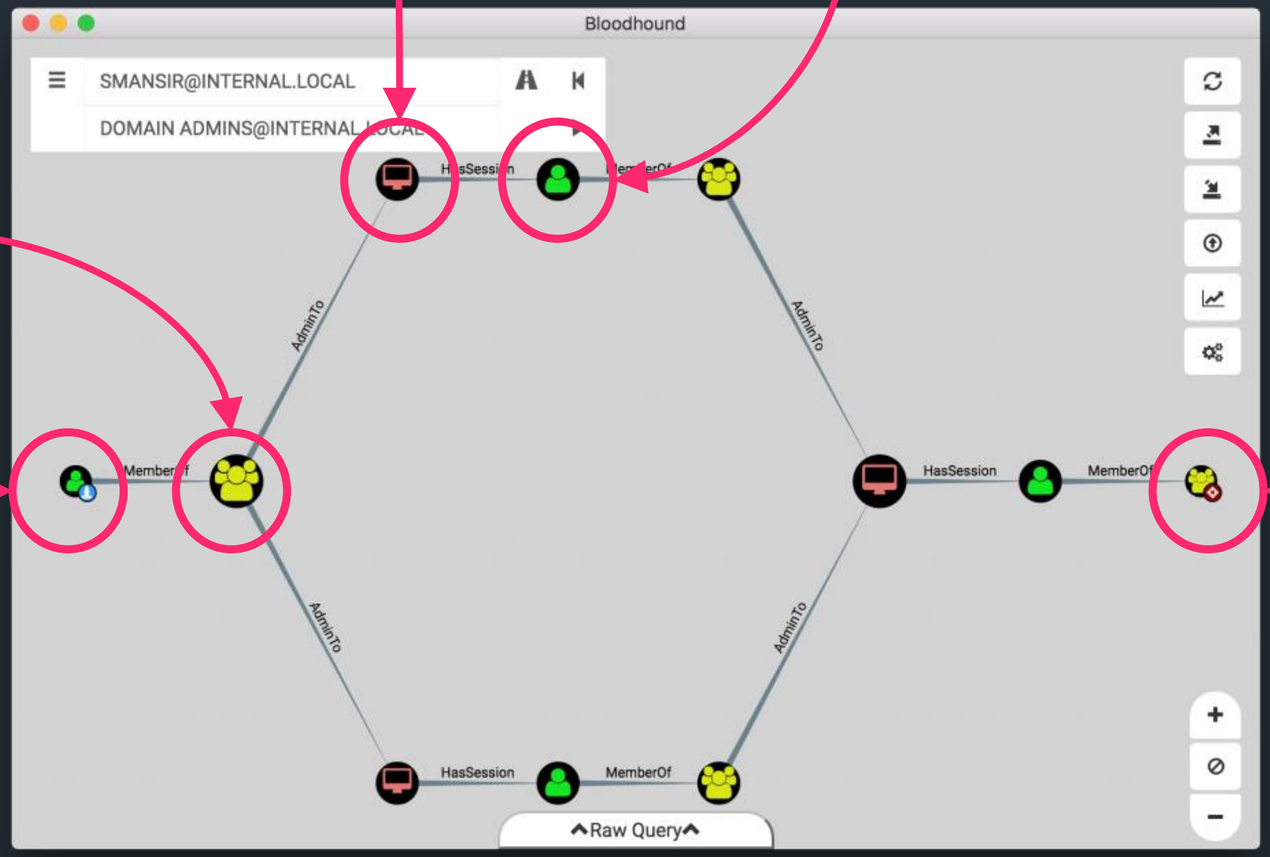
https://wald0.com/?p=68

Privilege Escalation

++

Bloodhound

MWR LABS



https://wald0.com/?p=68

MWR LABS

++

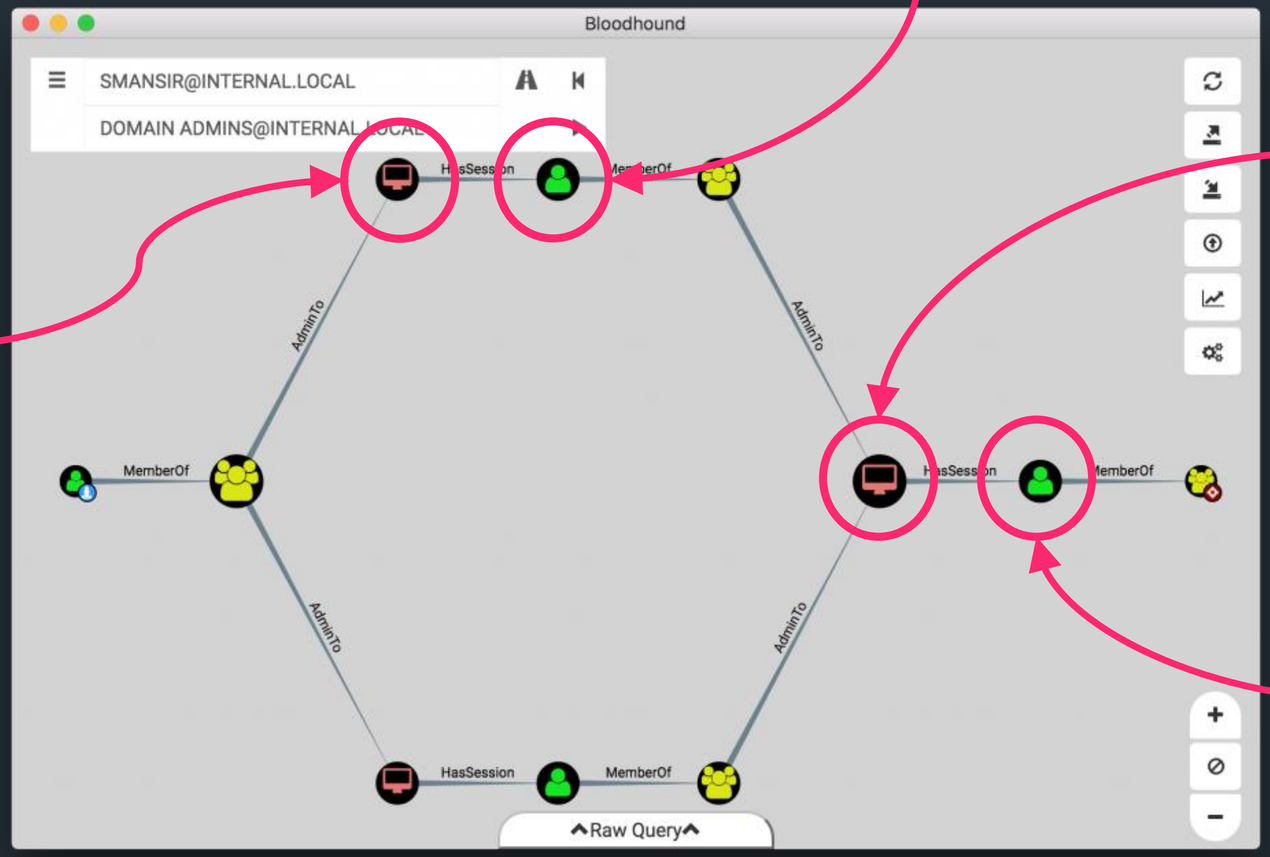
Bloodhound

Steal their credentials

Login here with initial creds

Login here with stolen creds

Domain Admin



https://wald0.com/?p=68

MWR LABS

++

Pass-The-Hash

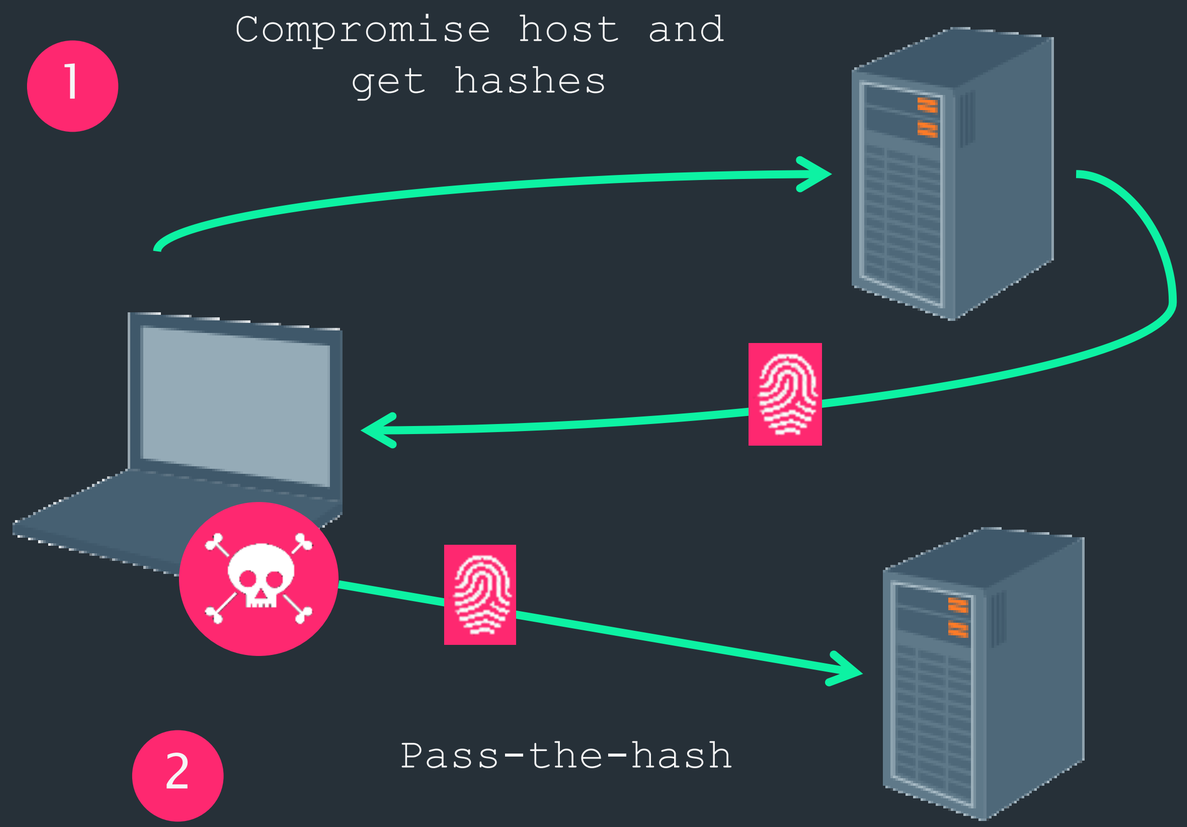
Some Windows Protocols allow authentication via hash rather than passwords

1. Compromise host
2. Acquire hashes
3. Transmit hashes as part of authentication requests to services using NTLM authentication

MWR LABS

++

Pass-The-Hash



MWR LABS

++

Credential Theft – Mimikatz

"A little tool to play with Windows security"

Mimikatz can dump passwords from different sources:

+ Terminal Services
+ Wdigest
+ Kerberos (Domain Authentication)
+ Windows Live

MWR LABS

++

Credential Theft – Mimikatz

"A little tool to play with Windows security"

+ Extract plaintext passwords, hashes and Kerberos tickets from memory.

```
mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 911306 (00000000:000de7ca)
Session           : Interactive from 3
User Name         : lukeskywalker
Domain            : ADSECLAB
SID               : S-1-5-21-1581655573-3923512380-696647894-2629
        msv :
         [00000003] Primary
         * Username : LukeSkywalker
         * Domain   : ADSECLAB
         * LM       : 3c0978ad4d3672cebe5ef0f17c30ad5e
         * NTLM     : 177af8ab46321ceef22b4e8376f2dba7
         * SHA1     : e1e310802741223f486f661032e1472a308dae3b
        tspkg :
         * Username : LukeSkywalker
         * Domain   : ADSECLAB
         * Password : TheForce99!
        wdigest :
         * Username : LukeSkywalker
         * Domain   : ADSECLAB
         * Password : TheForce99!
        kerberos :
         * Username : lukeskywalker
         * Domain   : LAB.ADSECURITY.ORG
         * Password : TheForce99!
        ssp :
        credman :
```

MWR LABS

++

Escalation in Windows Domains

+ In this example, accounts are always admin on target system

+ If not? Escalate your privileges on each system.

MWR LABS

++

Useful Resources

+ Vulnhub – Vulnerable VMs
  https://www.vulnhub.com/

+ All Roads Lead to SYSTEM
  https://labs.mwrinfosecurity.com/publications/windows-services-all-roads-lead-to-system/

+ g0tmi1k's Basic Linux Privilege Escalation
  https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

MWR LABS

Thanks for listening!

Questions?

MWR LABS

++

Tool References – Web Apps

+ Burp Suite – https://portswigger.net/burp/
+ ZAP (Zed Attack Proxy) – https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
+ NMAP – https://nmap.org/
+ Nikto – https://github.com/sullo/nikto
+ Arachni – http://www.arachni-scanner.com/
+ Netsparker – https://www.netsparker.com/web-vulnerability-scanner/

MWR LABS

++

Tool References - Windows

+ Sysinternals - https://technet.microsoft.com/en-gb/sysinternals/bb545021.aspx
+ Sysinternals Suite - https://technet.microsoft.com/en-gb/sysinternals/bb842062
+ Powersploit - https://github.com/PowerShellMafia/PowerSploit
+ Windows Exploit Suggester - https://github.com/GDSSecurity/Windows-Exploit-Suggester
+ Windows-privesc-check - https://github.com/pentestmonkey/windows-privesc-check
+ Netsess.exe - http://www.joeware.net/freetools/tools/netsess/index.htm
+ Bloodhound - https://github.com/BloodHoundAD/BloodHound

MWR LABS

++

Tool References - Linux

+ Metasploit - https://github.com/rapid7/metasploit-framework
+ LinuxPrivChecker - https://www.securitysift.com/download/linuxprivchecker.py
+ Unix-privesc-check - https://github.com/pentestmonkey/unix-privesc-check
+ LinEnum - https://github.com/rebootuser/LinEnum