PIVOT AND PILLAGE: LATERAL MOVEMENT WITHIN A VICTIM NETWORK

Steve Anson

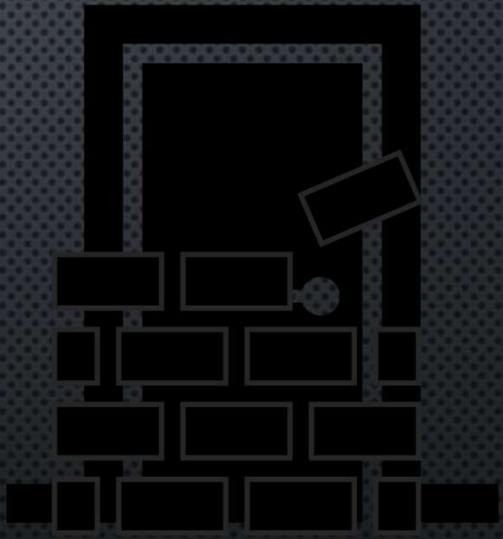
@ForwardDefense

HACKER PROCESS

- Reconnaissance/Scanning
- Exploitation/Initial Foothold
- Expand/Entrench
- Exfiltrate/Damage
- Cover Tracks

INITIAL FOOTHOLD - EXPLOIT

- Direct network attack
  - Right through the front door
  - Past all your DMZ, IPS, Anti-APT, AV, etc.
  - Tougher to accomplish these days…



INITIAL FOOTHOLD - CLIENT

- Wandering client attack
  - Hit you when you leave the castle walls
  - DarkHotel campaign, for example
  - BYOD

INITIAL FOOTHOLD - USERS

- Social Engineering
  - Phishing
  - USB drop
  - Help Desk Scams

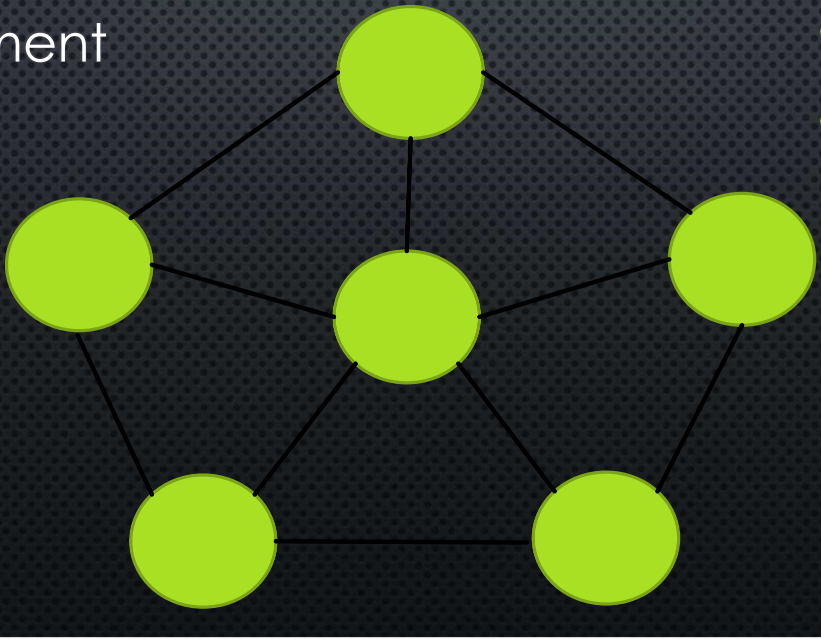
INITIAL FOOTHOLD - INSIDER

- The evil insider already has access

So I have a foothold…What now?

THE PIVOT

- Terms for pivoting
  - Lateral movement
  - Expansion



- Goals
  - Expand control
  - Find booty

PIVOT STYLES

- Are you a pirate or a ninja?
- Old school was more pirate
  - Noisy, but effective
  - Worms
  - Trojans
  - Viruses

PIVOT STYLES

- New school is more ninja
  - Stealthy to avoid detection and response
  - Live off the land
  - Use existing OS tools
  - Steal valid credentials/sessions

Credentials

PREPPING FOR THE PIVOT

- Get full credentials
  - Username and password
  - Mimikatz
  - Mimikittens
  - Key loggers
  - Sniff and crack
  - Find them laying around

PREPPING FOR THE PIVOT

- Get password hashes
  - Meterpreter hashdump
  - Mimikatz
  - SAM or /etc/shadow
  - Insecure database

```
8e7c0772c5ed7921
fd8d3c7984d3b9d3
```

PREPPING FOR THE PIVOT

- Steal a session
  - Kerberos Tickets conveniently sitting in RAM
  - Already authenticated, bypassing MFA
  - Uses existing user context
  - Pass-the-Ticket attacks

PREPPING FOR THE PIVOT

- Steal a session
  - Grab a session cookie
  - Impersonate the user
  - XSS, XSRF, etc.

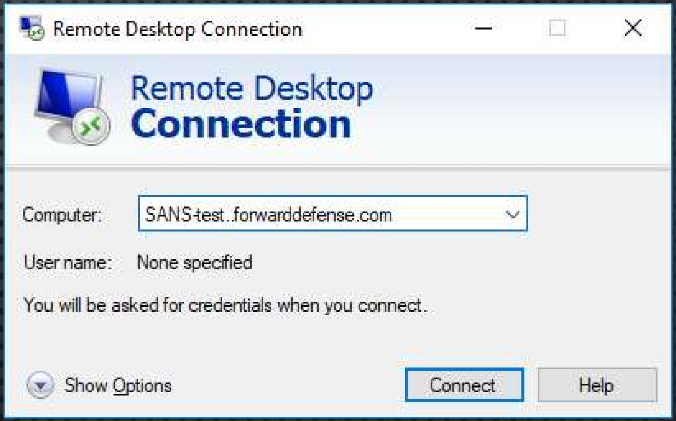
PREPPING FOR THE PIVOT

- Scan for a known vulnerability to exploit

We’re all armed up. Let’s move out…

PIVOT METHODS

- RDP (Remote Desktop Protocol)
  - Built in administration tool
  - Remote GUI control
  - Commonly used by users and admins



Remote Desktop Connection

Remote Desktop **Connection**

Computer: SANS-test.forwarddefense.com

User name: None specified

You will be asked for credentials when you connect.

PIVOT METHODS

- Server Message Block (SMB)
  - Remote file access
  - Administrative Share
    - net use * \\[targetIP]\[share] [password] /u:[domain\user]
    - Passes current user if not specified
  - Upload, download, modify remote data

PIVOT METHODS

- at
  - at [\\targetIP] [HH:MM][A|P] [command]
- schtasks
  - schtasks /create /tn [taskname] /s [targetIP] /u [user] /p [password] /sc [frequency] /st [starttime] /sd [startdate] /tr [command]
  - Can even run as System with /ru SYSTEM

PIVOT METHODS

- SC
  - Dig in really deep, start a malicious service
  - Persists reboots, restarts itself, always on
  - sc \\[targetIP] create [svcname] binpath= [command]
  - sc \\[targetIP] start [svcname]

PIVOT METHODS

- Windows Management Instrumentation Commandline
  - wmic /node:[targetIP] /user:[admin_user] /password:[password] process call create [command]
  - wmic /node:[targetIP] /user:[admin_user] /password:[password] datafile where “path=’\\’” get Name, FileSize
  - Passes current user creds if not specified
  - /node takes a text file
  - Uses RPC/DCOM to connect

PIVOT METHODS

- WinRM
  - Windows Remote Management
  - Based on Web Services for Management
  - winrs -r:http://remote_host “cmd”

PIVOT METHODS

- PowerShell Remoting
  - Object oriented shell
  - PowerShell remoting leverages WS-Management through WinRM
  - Enter-PSSession -ComputerName <Victim> -Credential <user>
  - Invoke-Command -ComputerName <Victim> -Credential <domain>\<user> -ScriptBlock {Get-Process}
  - Many attack kits already built

PIVOT METHODS

- PsExec
  - From Sysinternals
  - Not a native tool, but commonly found
  - psexec \\[Victim] [-d] [-u user] [–p password] [command]
  - Can push the executable with –c
  - Limited to domain accounts with local admin permissions and RID 500 local admin

PIVOT METHODS

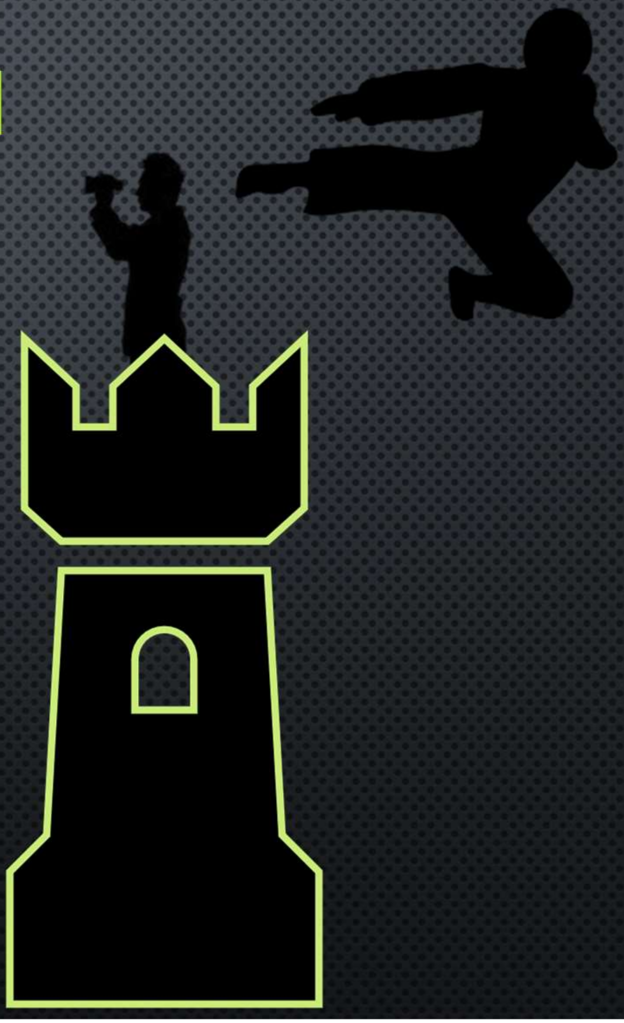
- Meterpreter
  - Schtasksabuse script
  - Route to pivot to other systems
  - Key logging
  - Hash dumping
  - Scanning

Sounds like a good time to be a hacker…

But I play for the Blue Team…

DETECTION

- Change your mindset
  - Need to look for pirates and ninjas



DETECTION

- Network Indicators
  - Odd activity on 5895/5896 (TCP)
  - Odd activity on 445 (TCP)
  - Odd RPC activity 135 (TCP) plus high ports
  - Connections between workstations
  - First connection to new systems

DETECTION

- Authentication and Logon Auditing
  - Local
    - 4624 – Type 3 Network Logon
    - 4672 – Special (Admin) Logon
    - 4776 – NTLM-based Authentication

DETECTION

- Authentication and Logon Auditing
  - DC
    - 4768 – TGT Issued
    - 4769 – Service ticket issued
    - 4776 – NTLM-based Authentication

DETECTION

- RDP Sessions
  - Security Log Events
    - 4624 - Logon Type 10
    - 4778 – Session reconnected
    - 4779 – Session disconnected

  - Additional detail in winevt/Logs/Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational

DETECTION

- WinRM Auditing
- winevt/Logs/Microsoft-Windows-WinRM%4Operational
  - 6 – shows initiation of an outbound connection
    - Appears on the local computer
    - Includes remote destination
  - 91 – Creating WSMan shell
    - Appears on remote computer
    - User field shows the user context

DETECTION

- PowerShell Auditing
  - Module Logging
    - Logs pipeline execution events
  - Script Block Logging
    - Captures de-obfuscated code sent to PowerShell
    - Commands only, no output

DETECTION

- PowerShell Auditing
  - Transcription
    - Logs terminal input/output to text files

DETECTION

- PowerShell Auditing
  - winevt/Logs/Windows PowerShell
    - Event 400, 800
  - winevt/Logs/Microsoft-Windows-PowerShell%4Operational
    - Event ID 4103, 4104

So I detected evil…How do I stop it?

ACTIVE DEFENSE

- Prevent – Detect - Respond
- Threat Hunt

ACTIVE DEFENSE

- Get your house in order
- Good IT security hygiene
- Center for Internet Security Basic Controls

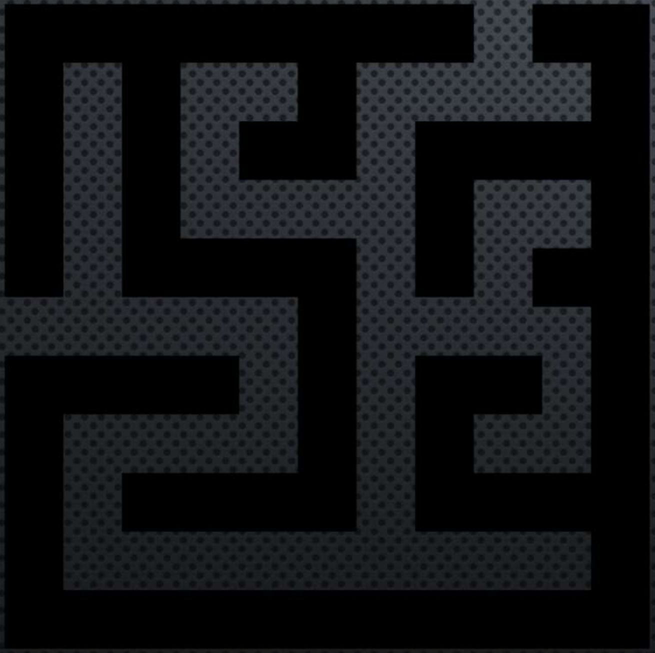
ACTIVE DEFENSE

- Restrict admin accounts
  - Least privilege
  - Tiered Administrative Accounts
  - Secure Admin Workstation (SAW)

ACTIVE DEFENSE

- Honey things
  - Honey pots
  - Honey tokens
  - Honey files
  - Honey creds

DEFENSE



- Network segmentation
  - Important OUs
  - BYOD
  - Private VLANs

CONCLUSIONS

- Client-side attacks and pivots are the new normal
- Bad guys continue to adapt, we need to as well
- The bad guys will get in
- Detection in depth, look for ninjas as well as pirates

CONTACT

@forwarddefense

www.forwarddefense.com

info@forwarddefense.com

Find PDFs of this presentation and more here:

www.AppliedIncidentResponse.com