3W's of Penetration Testing

Presented by:
Joel Prentice, Security Engineer
Appalachia Technologies

2022 Information Technology Security Conference

1

Joel Prentice

- Security Engineer, Appalachia Technologies
- BS – Cybersecurity Operations from Utica University
- MS – Cloud Computing Architecture from University of Maryland
- EC-Council Certified Ethical Hacker (CEH)
- eLearn Security Penetration Testing Professional (eCPPT)

2

About Appalachia:

- HQ in Mechanicsburg, PA - Local Presence, National Reach
- 17 Years of Service Excellence
- 48 Employees, 40 Certified Consulting Engineers
- SOC 2 Type II Audited
- CMMC Registered Provider Organization

BEST PLACES to work in PA

MSSP Alert TOP 250 MSSPs™ 2021 EDITION

THE CHANNEL CO. CRN MSP 500 2022

3

Agenda

- **Why** Do a Pen Test
  - How to get started
- **What** to Expect from a Pen Test
  - A walk through the process
  - And **How** to use the results to begin fixing any vulnerabilities
- **When** is the Right Time for Pen Test

4

Why do a Pen Test?

(And how to get started)

APPALACHIA TECHNOLOGIES, LLC

5

Threat Landscape

- Every 39 seconds there is a cyber attack!
- 43% of all cyber attacks target small business!
- The average cost of a data breach in 2020 will exceed $150 million dollars!
- 3,809,448 records are stolen from data breaches everyday!

WHY Do a Pen Test | WHAT | HOW | WHEN

APPALACHIA TECHNOLOGIES, LLC

6

MITRE ATT&CK Framework

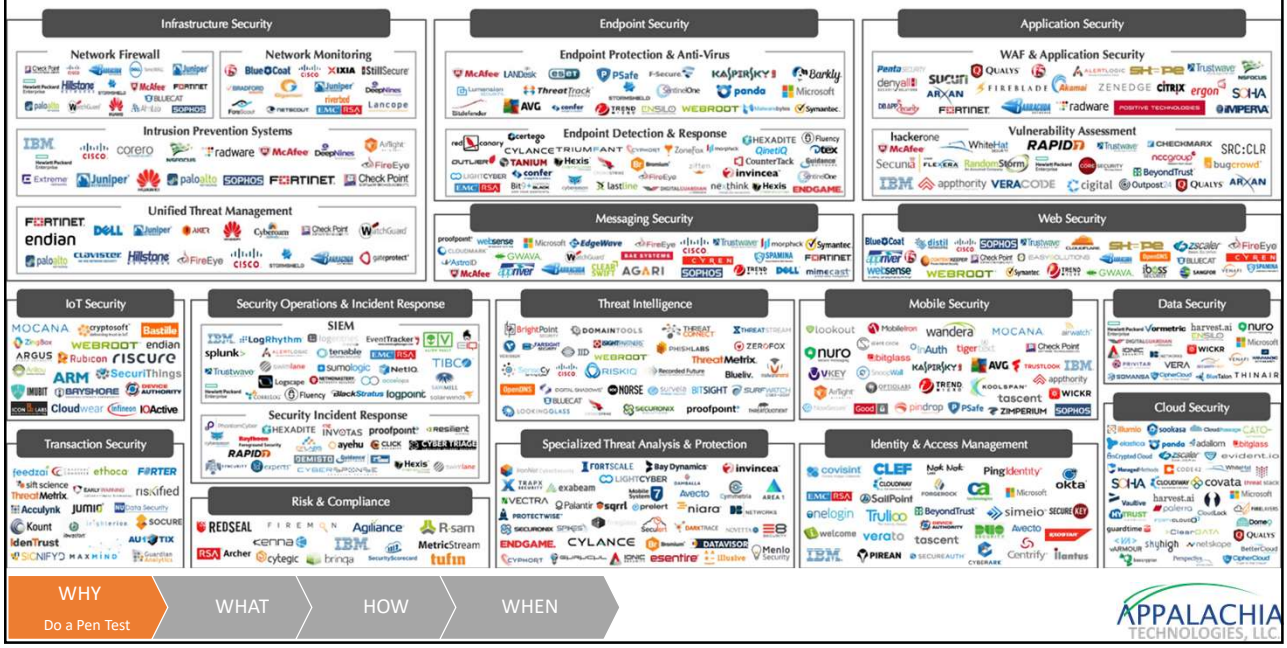
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing		Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL		Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness		Extra Window Memory Injection	Private Keys		Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and		File Deletion	Replication Through Removable Media					Standard Cryptographic
	Scheduled Task			File System Logical Offsets						

WHY
Do a Pen Test
WHAT
HOW
WHEN

APPALACHIA TECHNOLOGIES, LLC

7

The Cybersecurity Vendor Landscape



WHY
Do a Pen Test
WHAT
HOW
WHEN

APPALACHIA TECHNOLOGIES, LLC

8

Massive Skills Shortage

National level

TOTAL CYBERSECURITY JOB OPENINGS

597,767

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

1,053,468

SUPPLY/DEMAND RATIO

GEOGRAPHIC CONCENTRATION

Average

LOCATION QUOTIENT

WHY Do a Pen Test | WHAT | HOW | WHEN

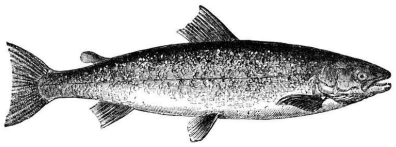
APPALACHIA TECHNOLOGIES, LLC

9

A Bad Cybersecurity Strategy

WHY Do a Pen Test | WHAT | HOW | WHEN

Security by optimism and prayer



Expert

Hoping Nobody Hacks You

O RLY?

@ThePracticalDev

APPALACHIA TECHNOLOGIES, LLC

10

What does a Penetration Test Do?

Simulates a real cyber attack

Baseline your defenses

Train your team on how to defend

Test incident response processes

Meet compliance requirements

Learn your organizational weaknesses

WHY Do a Pen Test | WHAT | HOW | WHEN

APPALACHIA TECHNOLOGIES, LLC

11

How to Get Started

- **What** *type* of pen test
  - Internal or External Network Pen Test
  - Web Application Pen Test
- **What** is the *scope* of what is to be tested
  - Compliance requirements?
  - Excluded devices/segments
- **Who** is the *vendor*
  - Experience, industry recognized credentials/certifications, follows industry-standard framework
  - Shared goal of improvement and a more secure organization

WHY Do a Pen Test | WHAT | HOW | WHEN

APPALACHIA TECHNOLOGIES, LLC

12

What to Expect from a Pen Test

(And how to use the results to begin fixing any vulnerabilities)

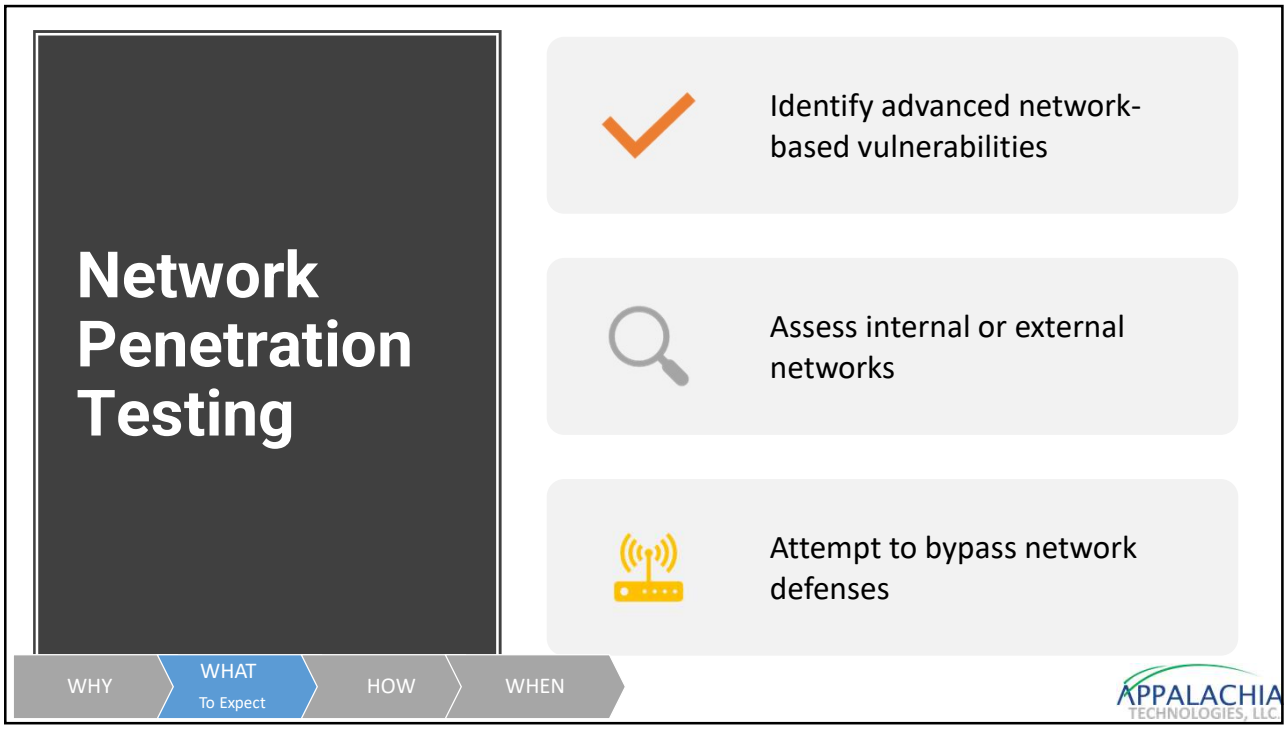
13

What You Should Know

- How long will it take?
- What is the difference between a Pen Test and a Vulnerability Scan?
- Will my users/network be affected?

Phases of a Pen Test:

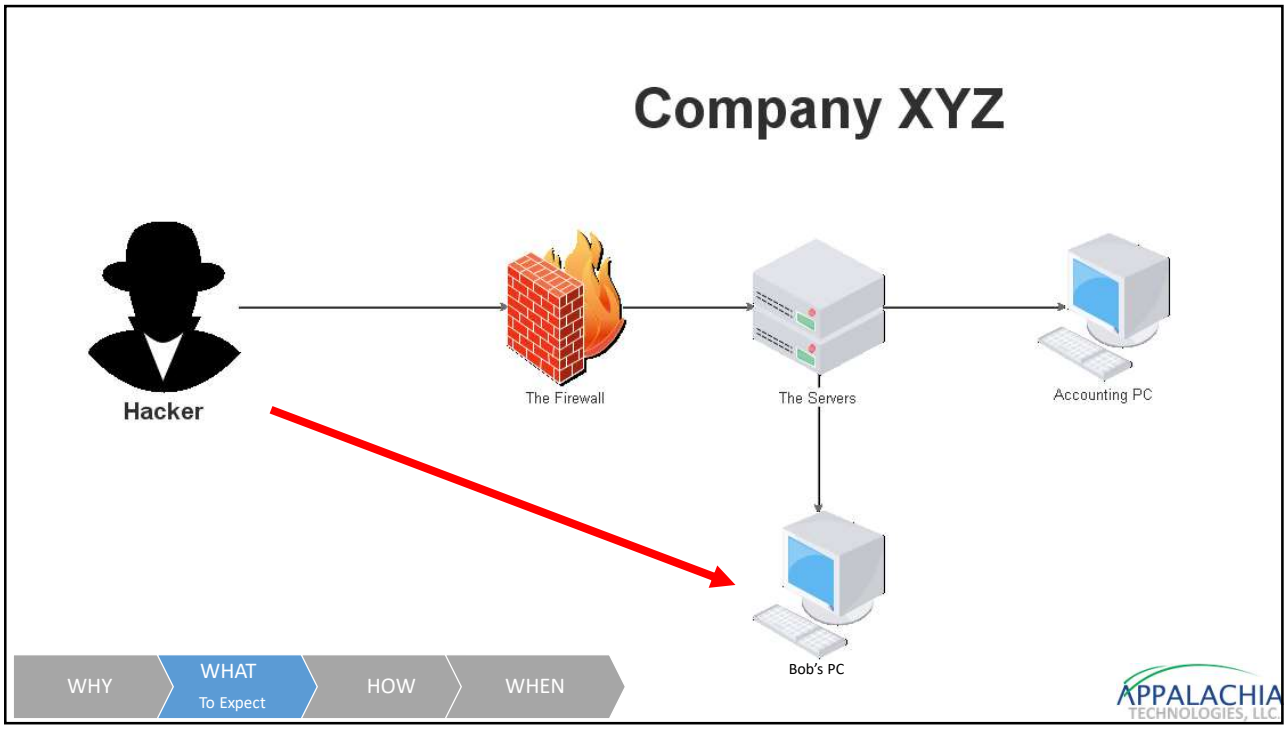
14


Network Penetration Testing
Identify advanced network-based vulnerabilities
Assess internal or external networks
Attempt to bypass network defenses
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

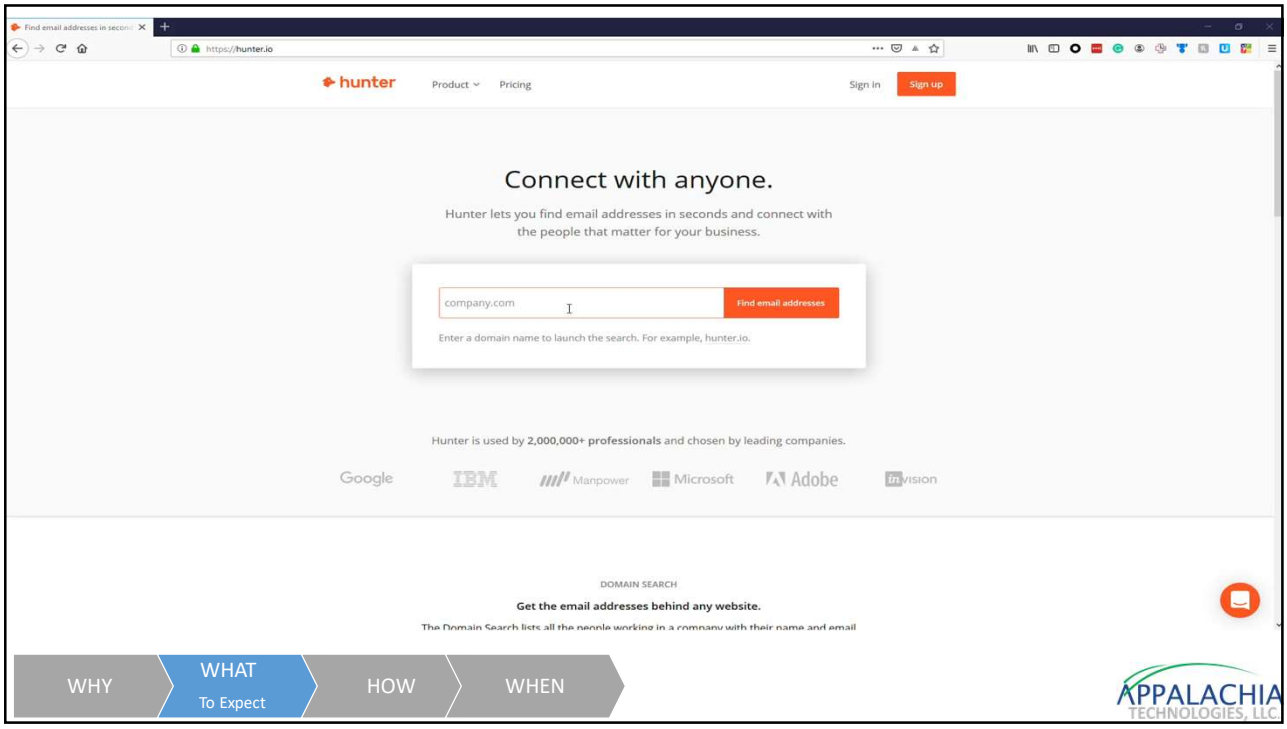
15


Intelligence Gathering & Recon
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

16


Company XYZ
Hacker
The Firewall
The Servers
Accounting PC
Bob's PC
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

17

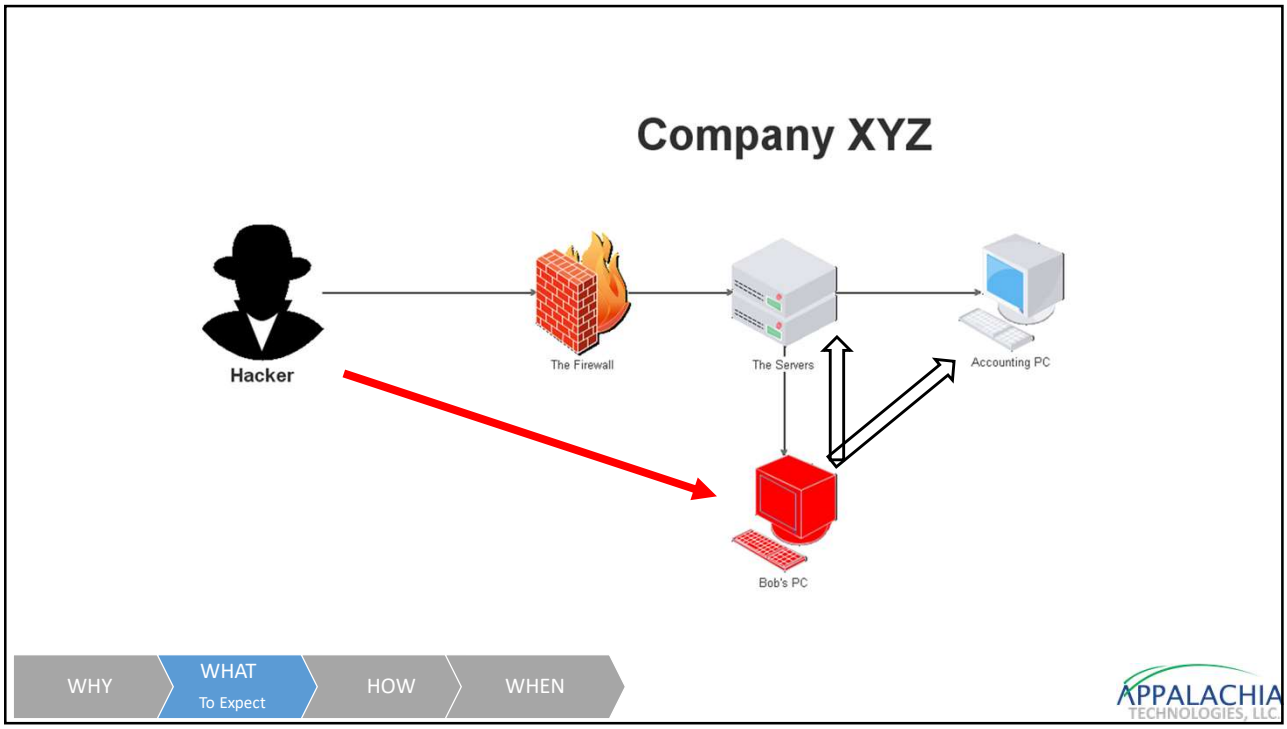

hunter
Product
Pricing
Sign in
Sign up
Connect with anyone.
Hunter lets you find email addresses in seconds and connect with the people that matter for your business.
company.com
Find email addresses
Enter a domain name to launch the search. For example, hunter.io.
Hunter is used by 2,000,000+ professionals and chosen by leading companies.
Google
IBM
Manpower
Microsoft
Adobe
Vision
DOMAIN SEARCH
Get the email addresses behind any website.
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

18

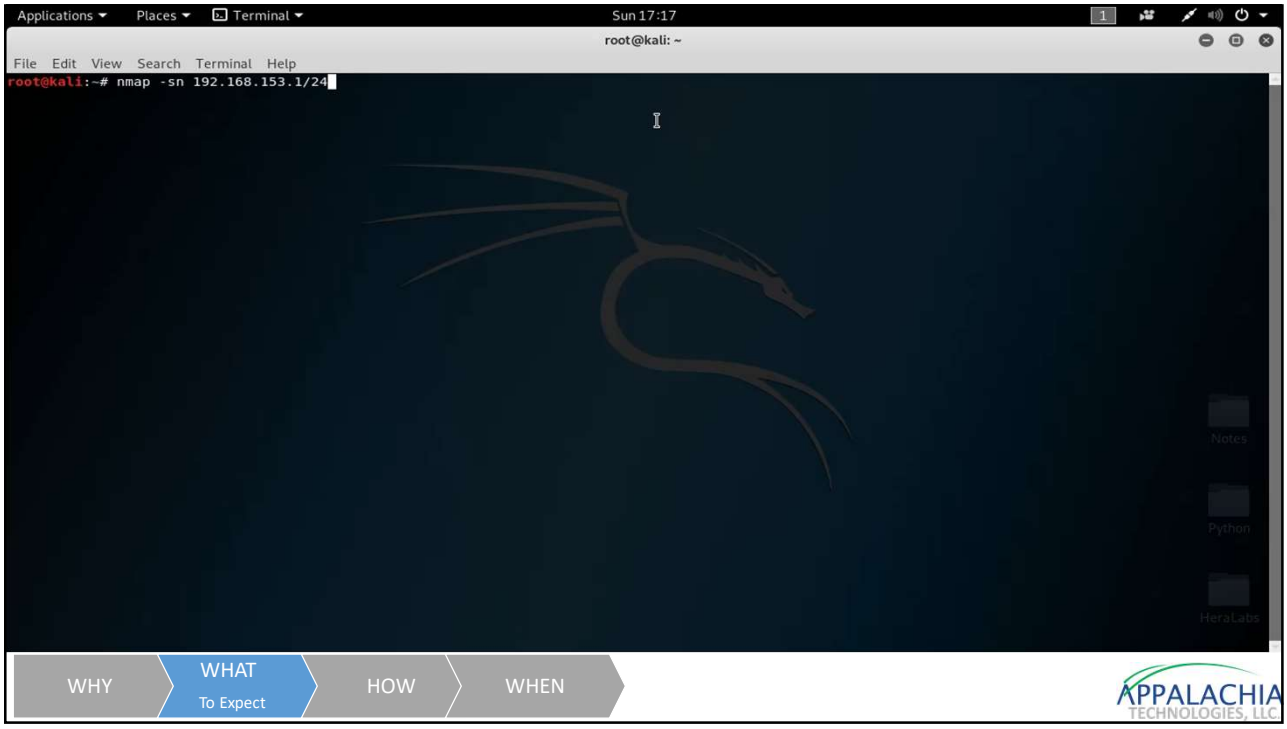
19

Threat Modeling and Vulnerability Analysis

20


Company XYZ
Hacker
The Firewall
The Servers
Accounting PC
Bob's PC
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

21


Applications
Places
Terminal
Sun 17:17
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -sn 192.168.153.1/24
Notes
Python
HeraLabs
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

22

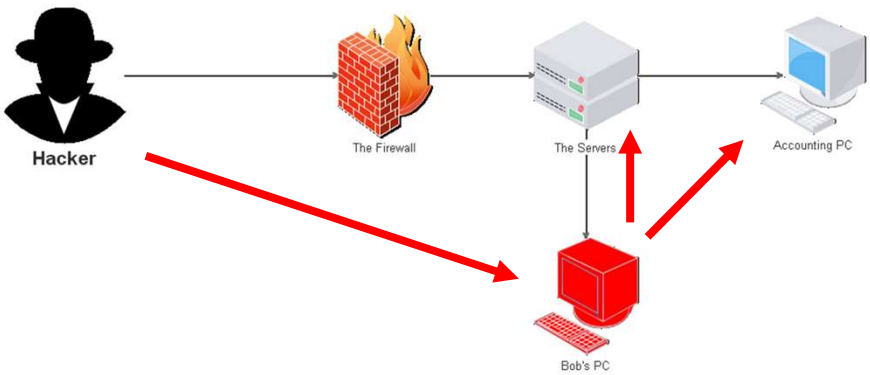
Exploitation

WHY | WHAT To Expect | HOW | WHEN

APPALACHIA TECHNOLOGIES, LLC

23

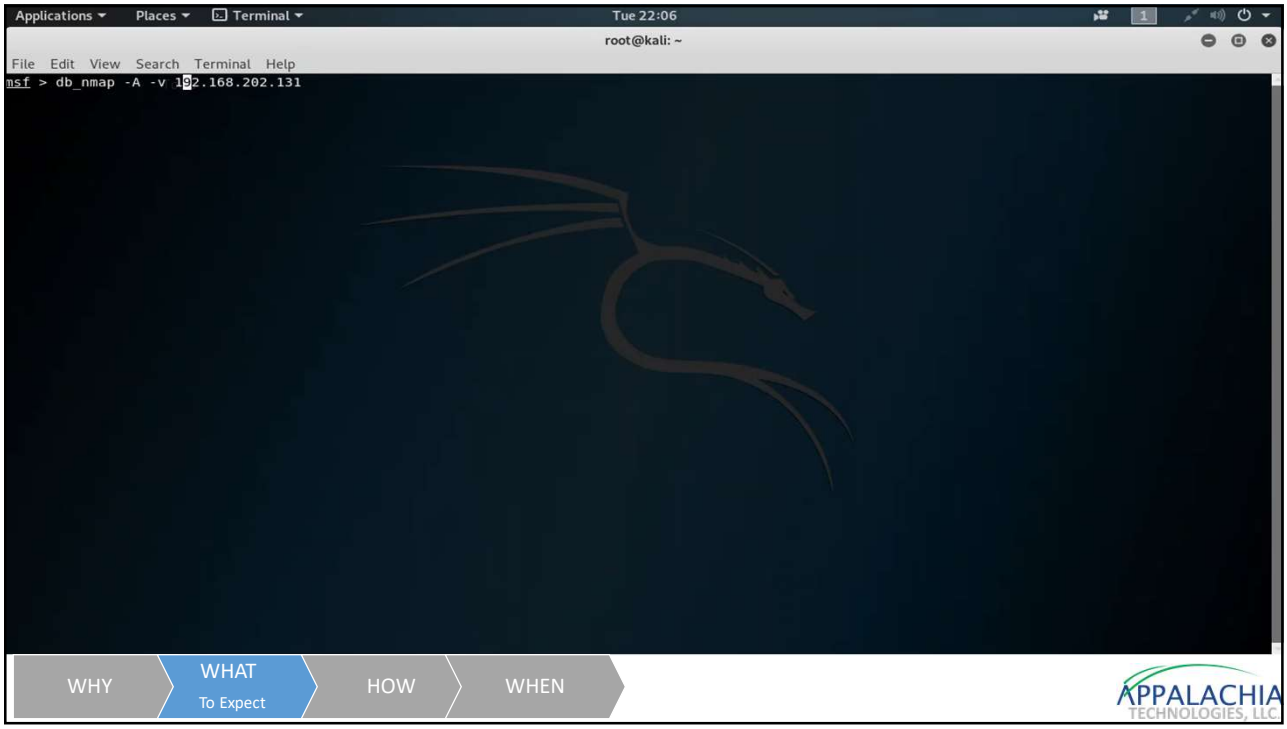
Company XYZ



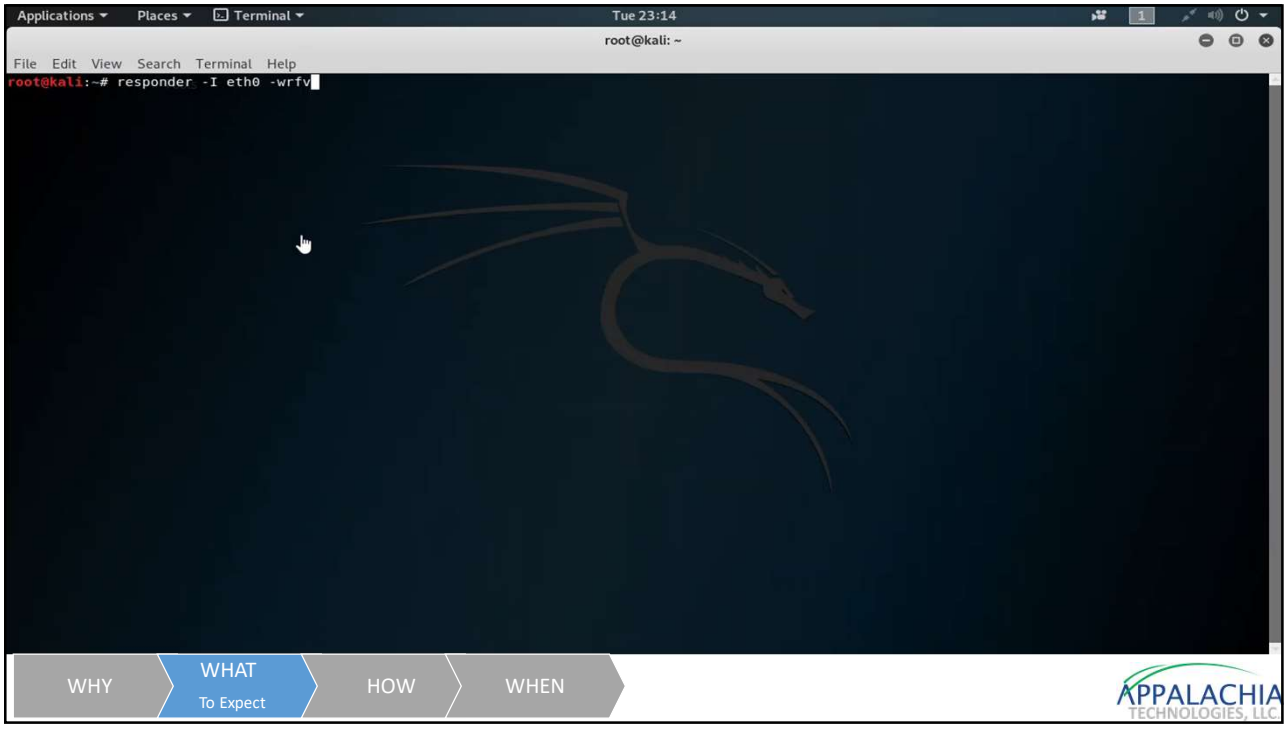
WHY | WHAT To Expect | HOW | WHEN

APPALACHIA TECHNOLOGIES, LLC

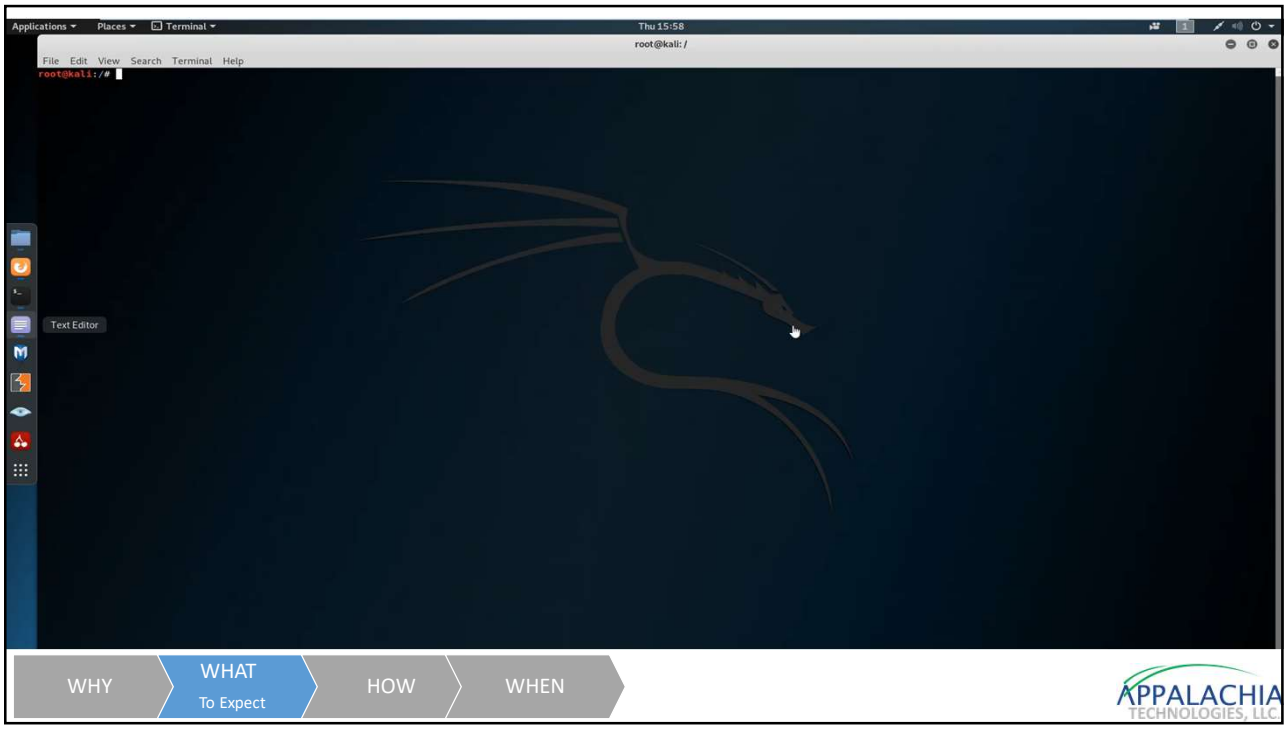
24


Applications
Places
Terminal
Tue 22:06
root@kali: ~
File Edit View Search Terminal Help
msf > db_nmap -A -v 192.168.202.131
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

25


Applications
Places
Terminal
Tue 23:14
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# responder -I eth0 -wrfv
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

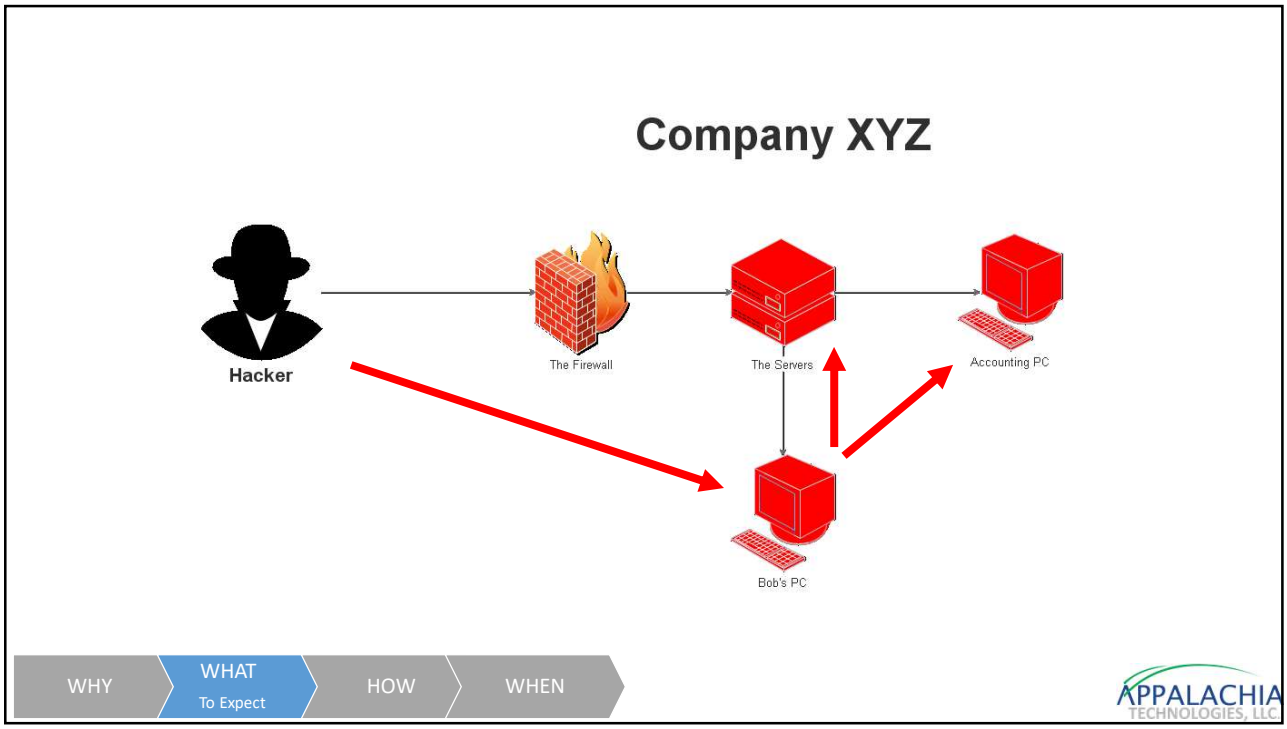
26


Applications
Places
Terminal
Thu 15:58
root@kali: /
File Edit View Search Terminal Help
root@kali:/#
Text Editor
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

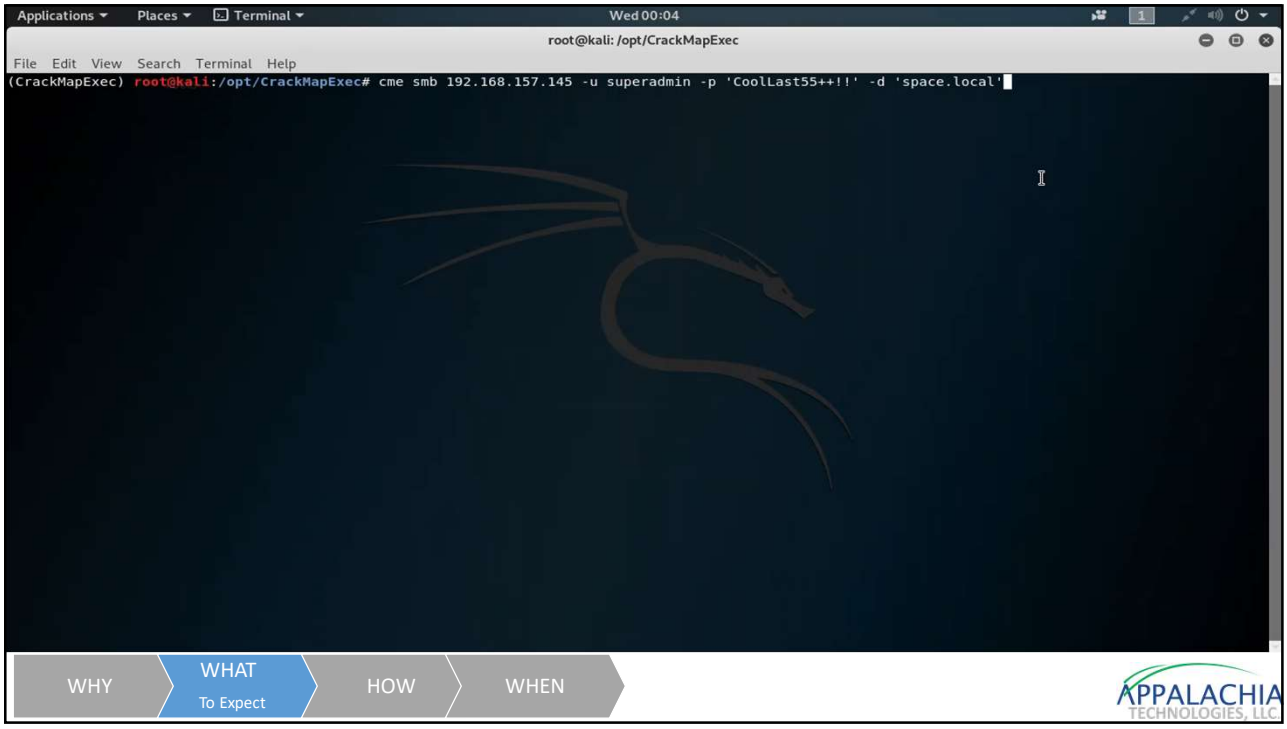
27


Post Exploitation
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

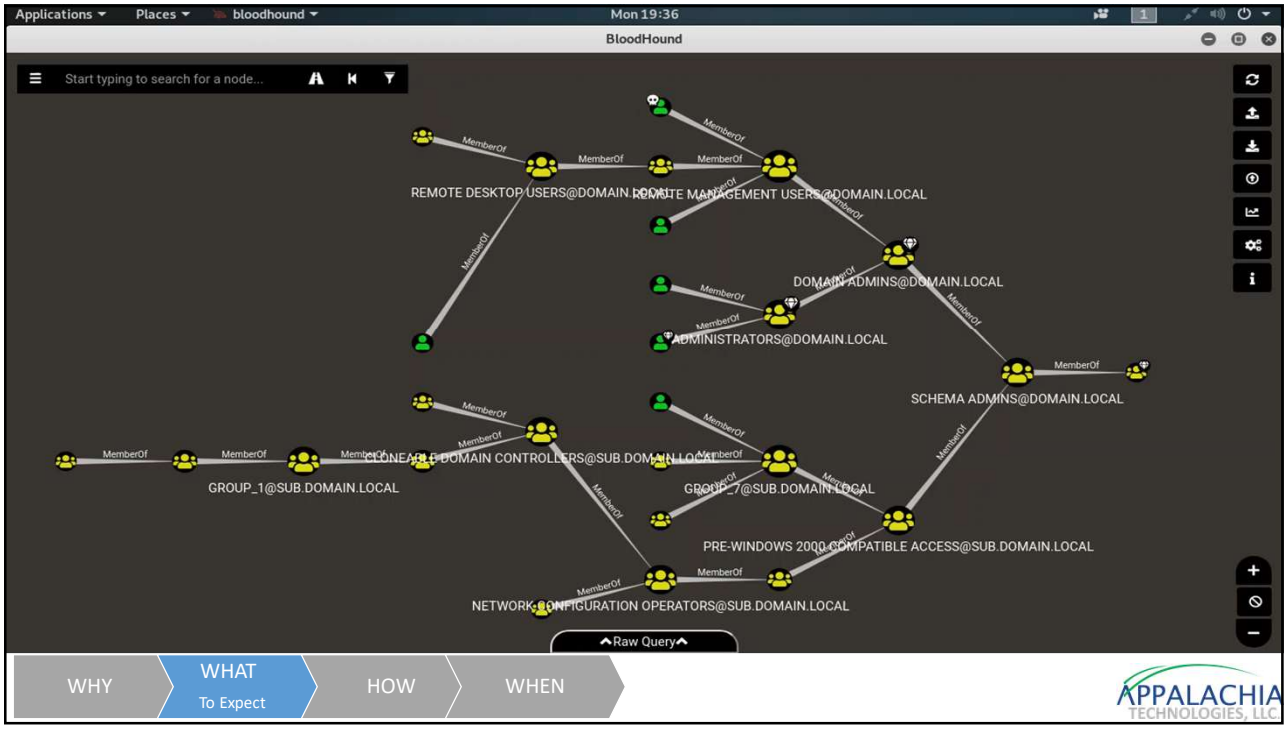
28


Company XYZ
Hacker
The Firewall
The Servers
Accounting PC
Bob's PC
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

29


Applications
Places
Terminal
Wed 00:04
root@kali: /opt/CrackMapExec
File Edit View Search Terminal Help
(CrackMapExec) root@kali:/opt/CrackMapExec# cme smb 192.168.157.145 -u superadmin -p 'CoolLast55++!!' -d 'space.local'
WHY
WHAT
To Expect
HOW
WHEN
APPALACHIA
TECHNOLOGIES, LLC

30



31

How to Use the Results to Begin Fixing Any Vulnerabilities

APPALACHIA TECHNOLOGIES, LLC

32

Final Report

DETAILED REPORT WITH ALL FINDINGS

STEP BY STEP WALKTHROUGH OF EXPLOITATION PATH

FILES AND EVIDENCE FOR REVIEW BY TEAM

PRESENTATION TO EXPLAIN RESULTS AND RECOMMENDATIONS

WHY | WHAT | HOW To Use Results | WHEN

APPALACHIA TECHNOLOGIES, LLC

33

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

WHY | WHAT | HOW To Use Results | WHEN

APPALACHIA TECHNOLOGIES, LLC

34

Remediation Post Exploitation

Pass the hash:

Mitigation	Description
Password Policies	Ensure that built-in and created local administrator accounts have complex, unique passwords.
Privileged Account Management	Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems.
Update Software	Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group.
User Account Control	Enable pass the hash mitigations to apply UAC restrictions to local accounts on network logon. The associated Registry key is located HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy Through GPO: Computer Configuration > [Policies] > Administrative Templates > SCM: Pass the Hash Mitigations: Apply UAC restrictions to local accounts on network logons.
User Account Management	Do not allow a domain user to be in the local administrator group on multiple systems.

WHY | WHAT | HOW (To Use Results) | WHEN

APPALACHIA TECHNOLOGIES, LLC

35

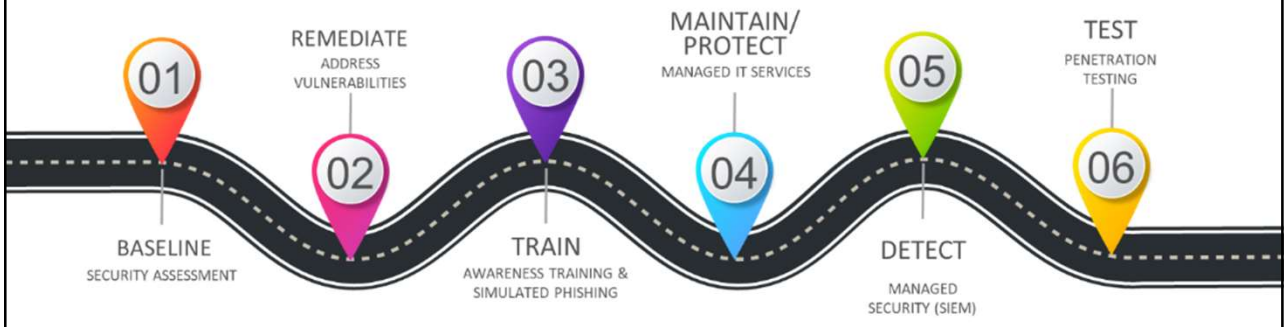
When is the Right Time for a Pen Test?

APPALACHIA TECHNOLOGIES, LLC

36

Make sure you're doing the basics first….

- If you haven't had an assessment, you should start there!
- Make sure you're in a good place first. Not just technically, but with policies and procedures, etc.



WHY | WHAT | HOW | WHEN Is the Right Time

APPALACHIA TECHNOLOGIES, LLC

37

How often should you get a penetration test?

- When you make significant Network or Application changes
- When you have Compliance requirements
- When you're asked by a Client

WHY | WHAT | HOW | WHEN Is the Right Time

APPALACHIA TECHNOLOGIES, LLC

38

THANK YOU

APPALACHIA TECHNOLOGIES, LLC.

CONNECT WITH US

http://www.appalachiatech.com/

39