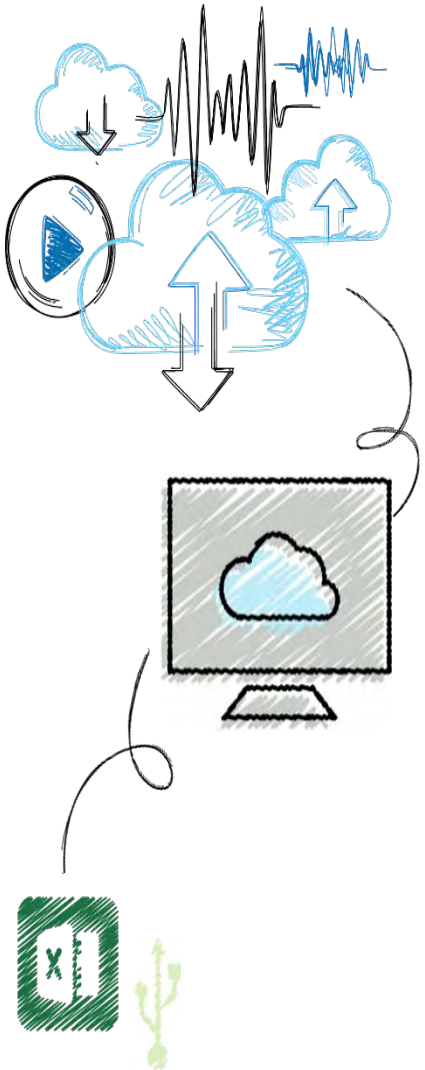
CompTIA Security+

Chapter 13

Vulnerability Assessment and Data Security



Objectives

13.1 Explain how to assess the security posture of an enterprise

13.2 Define vulnerability assessment and explain why it is important

13.3 Explain the differences between vulnerability scanning and penetration testing

13.4 Describe the techniques for practicing data privacy and security

Assessing the Security Posture

- The first step in any security protection plan
  - Vulnerability Assessment of the Enterprise Security Posture
    - How are things being done currently?
    - What is working vs. What is not working?
    - What are the existing vulnerabilities that must be addressed?
- A variety of techniques and tools can be used

What is Vulnerability Assessment?

- A systematic and methodical evaluation of the current security posture
  - It examines the exposure to:
    - Attackers
    - Forces of nature
    - Any potentially harmful entity
- Aspects of vulnerability assessment
  - Asset identification
  - Threat evaluation
  - Vulnerability appraisal
  - Risk assessment
  - Risk mitigation

Asset Identification (1 of 2)

- Asset identification
  - Process of inventorying items with economic value
- Common assets
  - People
  - Physical assets
  - Data
  - Hardware
  - Software

Asset Identification (2 of 2)

- After inventory has been taken, it is important to determine each item's relative value
- Factors to consider in determining value
  - How critical the asset is to the goals of organization
  - How much revenue asset generates
  - How difficult to replace asset
  - Impact of asset unavailability to the organization
- Some organizations assign a numeric value
  - Example: 5 being extremely valuable and 1 being the least valuable

Threat Evaluation (1 of 4)

- Threat evaluation
  - List potential threats that come from threat agents
  - A threat agent is any person or thing with the power to carry out a threat against an asset
- Threat modeling
  - Goal: understand attackers and their methods
  - Often done by constructing threat scenarios
- Attack tree
  - Provides visual representation of potential attacks
  - Drawn as an inverted tree structure

Threat Evaluation (2 of 4)

Category of threat	Example
Natural disasters	Fire, flood, or earthquake destroys data
Compromise of intellectual property	Software is pirated or copyright infringed
Espionage	Spy steals production schedule
Extortion	Mail clerk is blackmailed into intercepting letters
Hardware failure or error	Firewall blocks all network traffic
Human error	Employee drops laptop computer in parking lot
Sabotage or vandalism	Attacker implants worm that erases files
Software attacks	Virus, worm, or denial of service compromises hardware or software
Software failure or errors	Bug prevents program from properly loading
Technical obsolescence	Program does not function under new version of operating system
Theft	Desktop system is stolen from unlocked room
Utility interruption	Electrical power is cut off

Threat Evaluation (3 of 4)

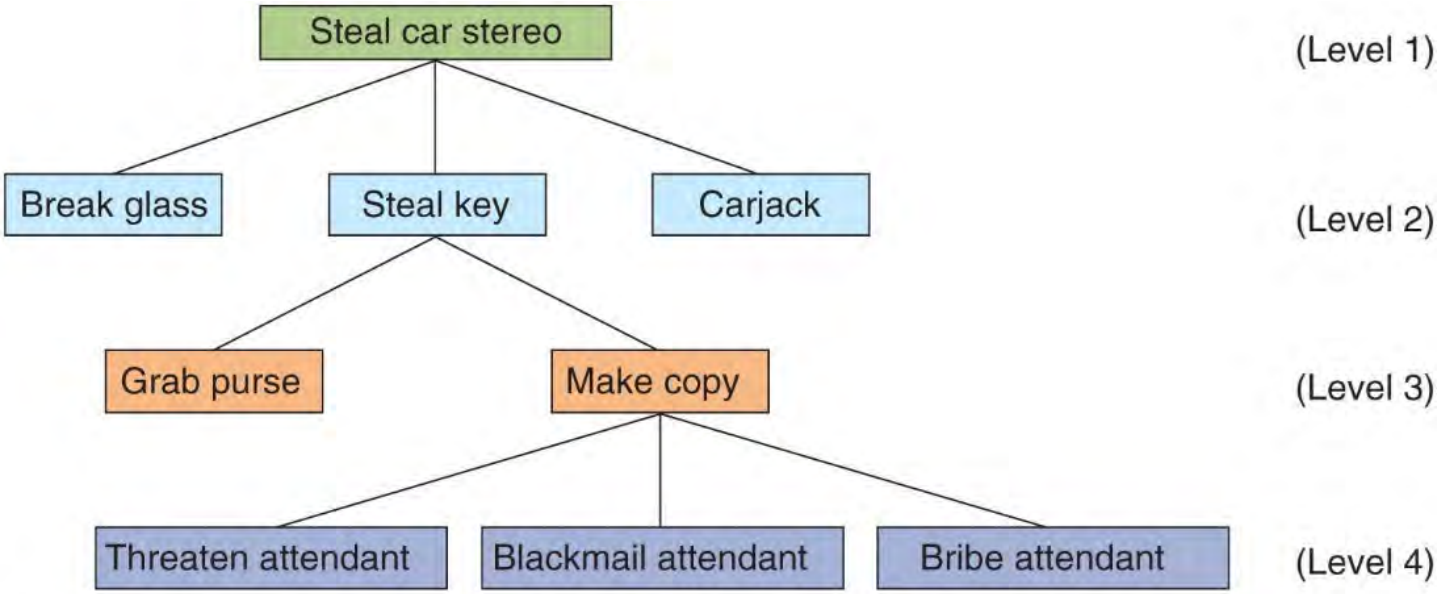


Figure 13-1 Attack tree for stealing a car stereo

Threat Evaluation (4 of 4)

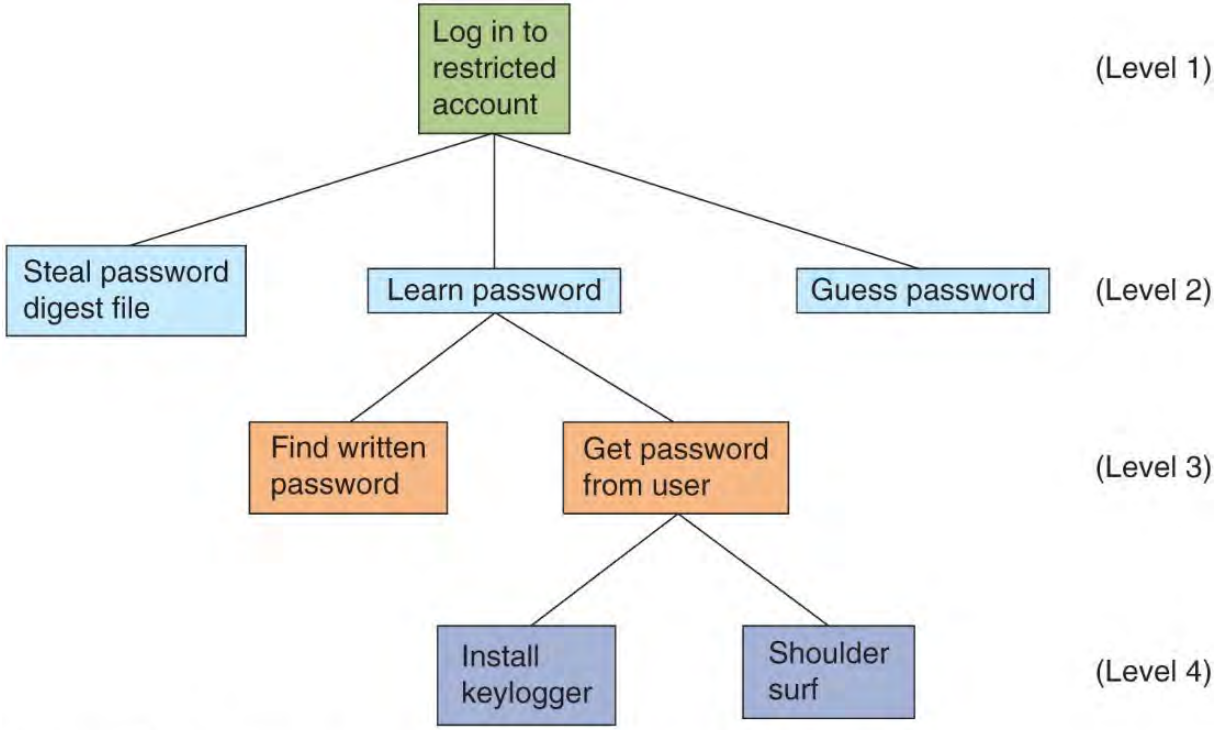


Figure 13-2 Attack tree for logging into restricted account

Vulnerability Appraisal

- Vulnerability appraisal
  - Determine current weaknesses
  - Takes a snapshot of current organization security
  - Every asset should be viewed in light of each threat
  - Catalog each vulnerability

Risk Assessment (1 of 2)

- Risk assessment
  - Determine damage that would result from an attack
  - Assess the likelihood that the vulnerability is a risk to organization

Risk Assessment (2 of 2)

Impact	Description	Example
No impact	This vulnerability would not affect the organization	The theft of a mouse attached to a desktop computer would not affect the operations of the organization
Small impact	Would produce limited periods of inconvenience and possibly result in changes to a procedure	A specific brand and type of hard disk drive that fails might require spare drives be made available and devices with those drive be periodically tested
Significant	A vulnerability that results in a loss of employee productivity due to downtime or causes a capital outlay to alleviate it could be considered significant	Malware that is injected into the network could be classified as a significant vulnerability
Major	Major vulnerabilities are those that have a considerable negative impact on revenue	The theft of the latest product research and development data through a backdoor could be considered a major vulnerability
Catastrophic	Vulnerabilities that are ranked as catastrophic are events that would cause the organization to cease functioning or be seriously crippled in its capacity to perform	A tornado that destroys an office building and all the company's data could be a catastrophic vulnerability

Risk Mitigation

- Risk mitigation
  - Determine what to do about risks
  - Determine how much risk can be tolerated

Vulnerability assessment action	**Steps**
1. Asset identification	a. Inventory the assets b. Determine the assets' relative value
2. Threat identification	a. Classify the threats by category b. Design attack tree
3. Vulnerability appraisal	a. Determine current weaknesses in protecting assets b. Use vulnerability assessment tools
4. Risk assessment	a. Estimate impact of vulnerability on organization b. Calculate risk likelihood and impact of the risk
5. Risk mitigation	a. Decide what to do with the risk

Vulnerability Assessment Tools

- Tool available to perform vulnerability assessments:
  - Port scanners
  - Protocol analyzers
  - Vulnerability scanners
  - Honeypots and honeynets
  - Banner grabbing tools
  - Crackers
  - Command line tools
  - Other tools

Port Scanners (1 of 3)

- TCP/IP communication
  - Involves information exchange between one system's program and another system's corresponding program
  - Uses a numeric value as an identifier to the applications and services on these systems (port number)
- Port number
  - A unique identifier for applications and services
  - 16 bits in length

Port Scanners (2 of 3)

- TCP/IP divides port numbers into three categories:
  - Well-known port numbers (0-1023)
    - Reserved for most universal applications
  - Registered port numbers (1024-49151)
    - Other applications not as widely used
  - Dynamic and private port numbers (49152-65535)
    - Available for any application to use
- Knowledge of what port is being used
  - Can be used by attacker to target a specific service
- Port scanner software
  - Searches system for port vulnerabilities
  - Used to determine port state
    - Open, closed, or blocked

Port Scanners (3 of 3)

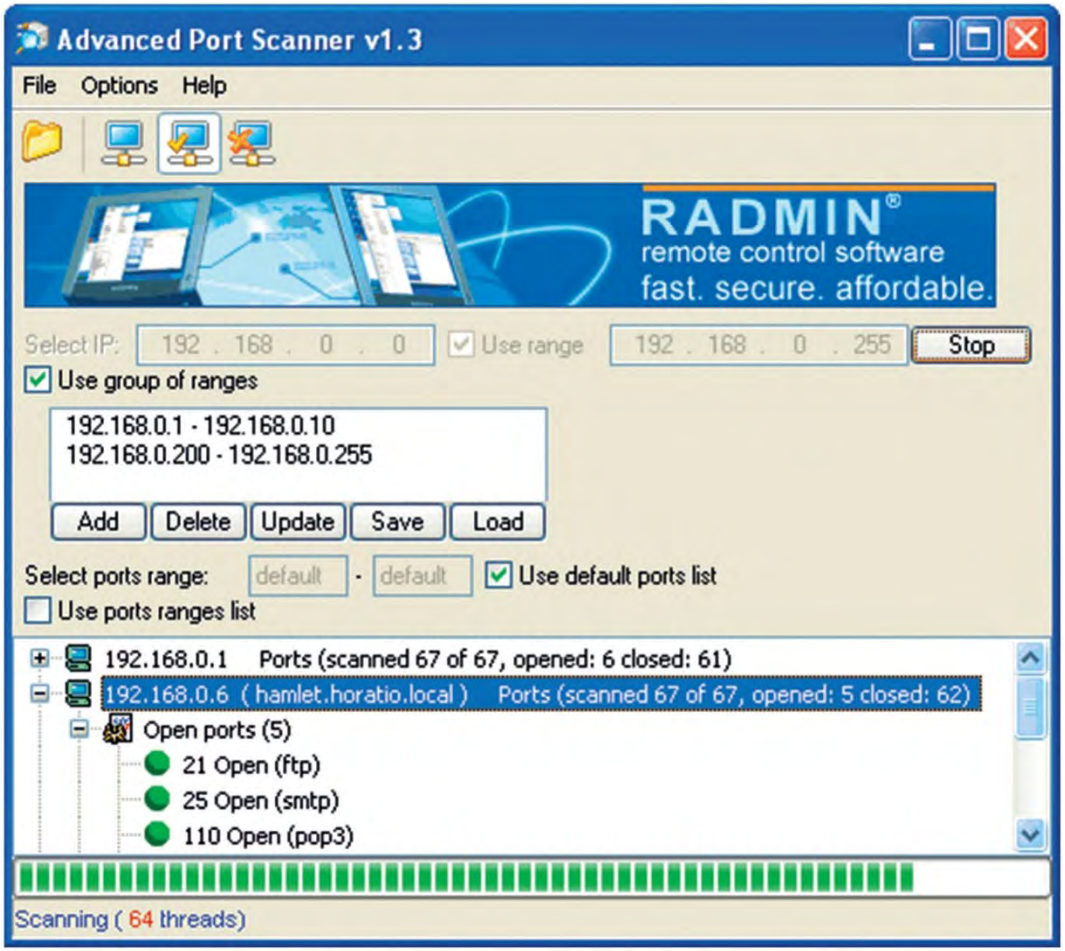


Figure 13-3 Port scanner

Source: RADMIN Advanced Port Scanner. Copyright © 1999-2014 Famatech. All rights reserved

Protocol Analyzers (1 of 2)

- Protocol analyzers
  - Hardware or software that captures packets t decode and analyze contents
  - Also known as sniffers
- Common uses for protocol analyzers
  - Used by network administrators for troubleshooting
  - Characterizing network traffic
  - Security analysis
- Can be used to fine-tune the network and manage bandwidth

Protocol Analyzers (2 of 2)

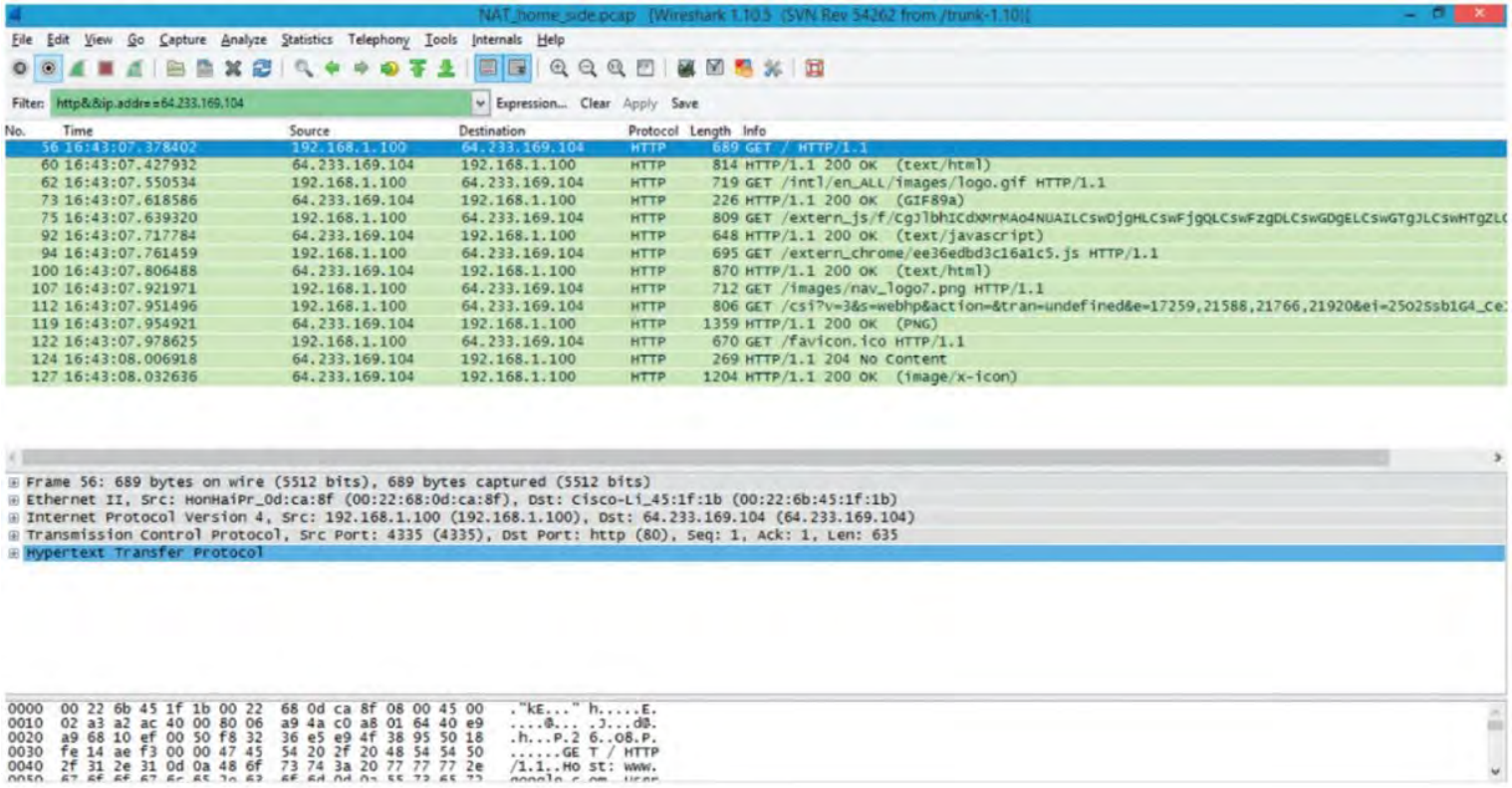


Figure 13-4 Protocol analyzer

Source: Wireshark Software

Vulnerability Scanners (1 of 4)

- Vulnerability scanners
  - A generic term for a range of products that look for vulnerabilities in networks or systems
- Vulnerability scanners for enterprises are intended to
  - Identify several vulnerabilities and alert network administrators
- Two types of vulnerability scanners:
  - Active scanner – sends “probes” to network devices and examine the responses received back to evaluate whether a specific device needs remediation
  - Passive scanner – can identify the current software OS and applications being used on the network and indicate which devices might have a vulnerability
    - Cannot take action to resolve security problems

Vulnerability Scanners (2 of 4)

- A vulnerability scanner can:
  - Alert when new systems are added to network
  - Detect when an application is compromised
  - Detect when an internal system begins to port scan other systems
  - Detect which ports are served and which ports are browsed for each individual system
  - Identify which applications and servers host or transmit sensitive data
  - Maintain a log of all interactive network sessions
  - Track all client and server application vulnerabilities
  - Track which systems communicate with other internal systems

Vulnerability Scanners (3 of 4)

Type	Description	Uses
Network mapping scanner	Combines network device discovery tools and network scanners to find open ports or discover shared folders	Can be used to create visual maps of the network that also identify vulnerabilities that need correction
Wireless scanner	Can discover malicious wireless network activity such as failed login attempts, record these to an event log, and alert an administrator	Detects security weaknesses inside the local wireless network with internal vulnerability scanning
Configuration compliance scanner	Used to evaluate and report any compliance issues related to specific industry guidelines	A compliance audit is a comprehensive review of how an enterprise follows regulatory guidelines

Vulnerability Scanners (4 of 4)

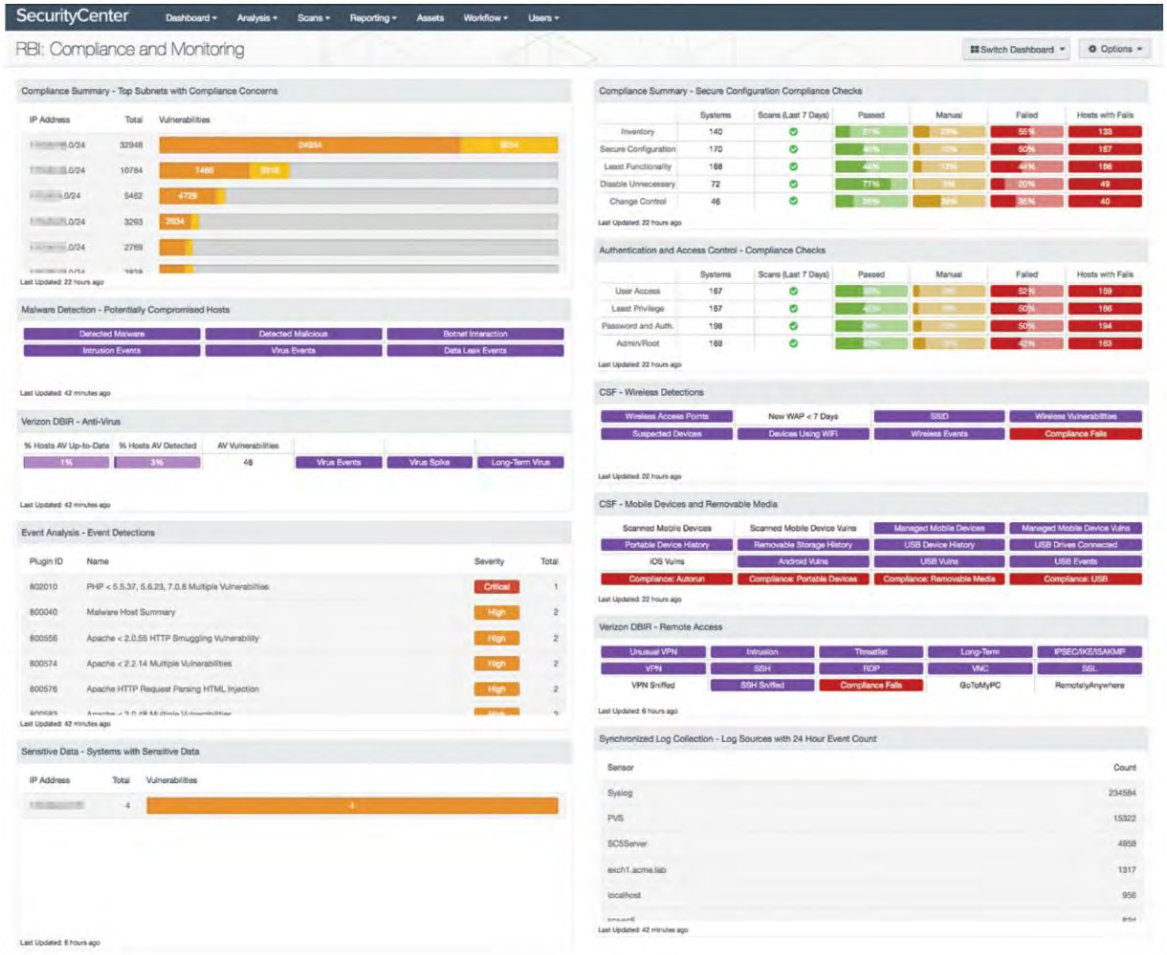


Figure 13-5 Configuration compliance scanner

Source: Tenable

Honeypots and Honeynets (1 of 2)

- Honeypot: a computer protected by minimal security
  - Intentionally configured with vulnerabilities
  - Contains bogus data files
- Goal: to trick attackers into revealing their techniques
  - Can then be determined if actual production systems could thwart such an attack
- Honeynet: a network set up with one or more honeypots
  - Set up with intentional vulnerabilities

Honeypots and Honeynets (2 of 2)

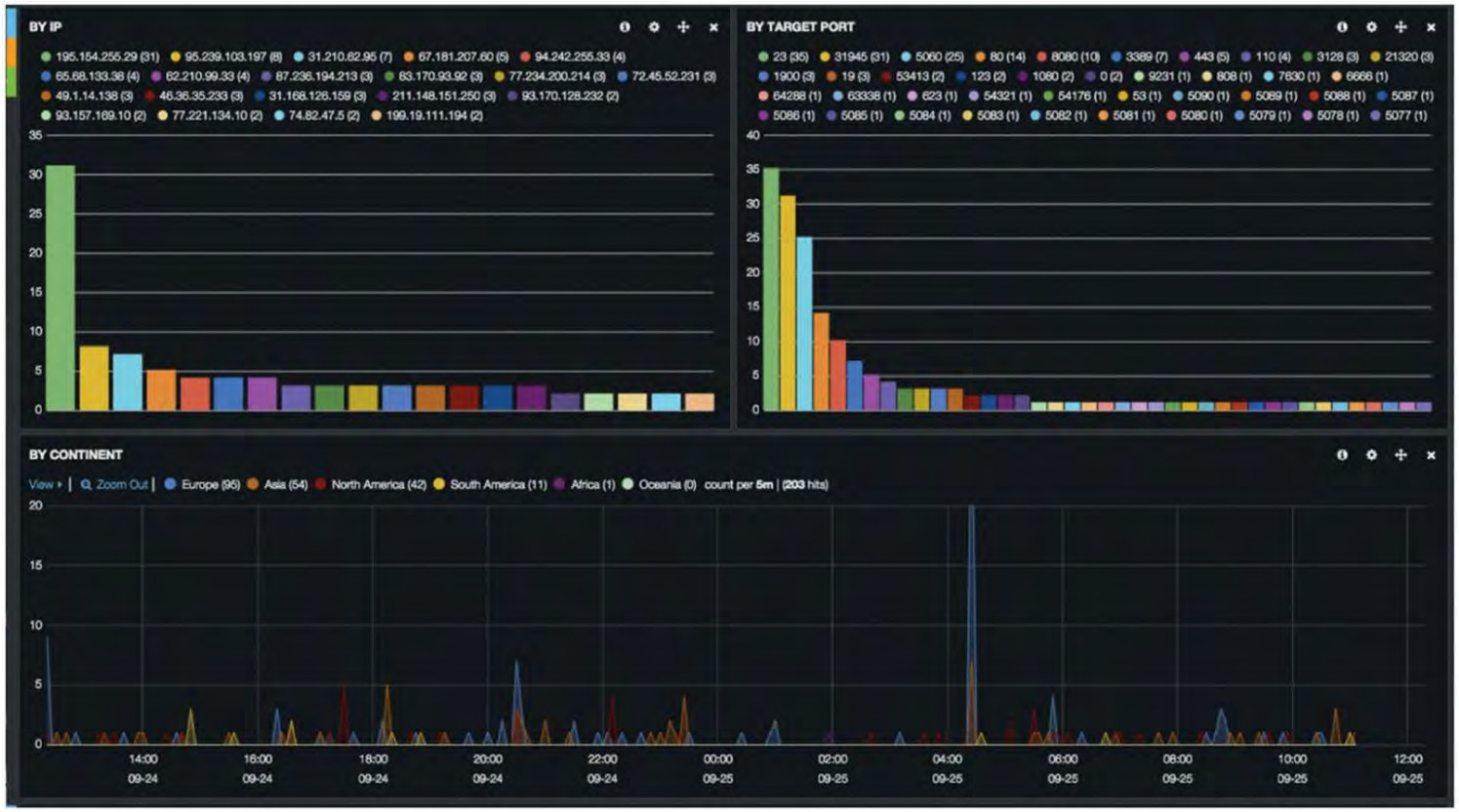


Figure 13-6 Honeypot dashboard

Source: Elasticsearch BV

Banner Grabbing Tools

- Banner: a message that a service transmits when another program connects to it
  - Example: the banner for a HT
  - TP service will typically show the type of server software, version number, when it was last modified, an other similar information
- Banner grabbing: when a program is used to intentionally gather this information
  - Can be used as an assessment tool to perform an inventory on the services and systems operating on a server

Crackers

- Crackers
  - Intended to break (“crack”) the security of a system
- Using a cracker in a vulnerability assessment can help determine how secure that system is
- Wireless cracker
  - Designed to test the security of a wireless LAN system by attempting to break its protections of Wi-Fi Protected Access (WPA) or WPA2
- Password cracker
  - Intended to break the digest of a password to determine its strength

Command-Line Tools (1 of 3)

Name	Description	How Used
Ping	Tests the connection between two network devices	Can flood the network to determine how it responds to a Denial of Service attack
Netstat	Displays detailed information about how a device is communicating with other network devices	Used to determine the source of malware that is sending out stolen information or communicating with a command and control server
Tracert	Shows the path that a packet takes	Can detect faulty or malicious routing paths
Nslookup	Queries the DNS to obtain a specific domain name or IP address mapping	Used to verify correct DNS configurations
Dig	Linux command-line alternative to Nslookup	More robust tool that can also verify DNS configurations
Arp	View and modify Address Resolution Protocol cache	Can view ARP cache to uncover ARP poisoning attacks
Ipconfig	Displays all current TCP/IP network configuration values and refreshes DHCP and DNS settings	Used to alter current settings such as IP address, subnet mask, and default gateway
IP and Ifconfig	Linux implementations of Ipconfig	Can test to determine if configurations are secure
Tcpdump	Linux command-line protocol analyzer	Can monitor network traffic for unauthorized traffic

Command-Line Tools (2 of 3)

- There are third-party tools that can be used for vulnerability scanning
- Nmap (network mapper)
  - A security vulnerability scanner that can determine which devices are connected to the network
- Netcat
  - A command-line alternative to Nmap
  - Can be used by itself or driven by other programs and scripts

Command-Line Tools (3 of 3)

- CLI Tools exist on Windows and Linux for network testing and scripting
- The best Reference Guide on the market, IMHO.
- “The NooB RaG!” – by Brian O’Hare
  - Available on Amazon
  - Yes, that’s me
- Both Windows and Linux
  - Command Line Tools
  - All Switches and Options Explained
  - Cross-Referenced

Other Tools

- Exploitation framework
  - Used to replicate attacks during a vulnerability assessment
  - Provides a structure of exploits and monitoring tools
- Steganography
  - A technology that hides the existence of data in a seemingly harmless data file, image file, audio file, or video file
- Steganography assessment tools
  - Can be used to determine if data is hidden well enough to thwart unauthorized users from finding the data

Vulnerability Scanning (1 of 2)

- Vulnerability scan
  - An automated software search through a system for known security weaknesses
  - Creates a report of potential exposures
  - Should be compared against baseline scans
    - Any changes can be investigated
- A scan looks to:
  - Identify vulnerabilities or security weaknesses found in the system
  - Identify a lack of security controls that are missing to establish a secure framework
  - Identify common misconfigurations (in hardware and software)

Vulnerability Scanning (2 of 2)

- Two methods for performing a vulnerability scan:
  - Intrusive vulnerability scan - attempts to actually penetrate the system to perform a simulated attack
  - Non-intrusive vulnerability scan - uses only available information to hypothesize the status of the vulnerability
- Credentialed vulnerability scan
  - Provides credentials (username and password) to the scanner so tests for additional internal vulnerabilities can be performed
- Non-credentialed scans do not use credentials

Penetration Testing (1 of 3)

- Designed to exploit system weaknesses
- Relies on tester's skill, knowledge, cunning
- Usually conducted by independent contractor
- Tests are usually conducted outside the security perimeter
  - May even disrupt network operations
- End result: penetration test report

Penetration Testing (2 of 3)

- Three different techniques can be used:
  - Black box test - tester has no prior knowledge of network infrastructure
  - White box test - tester has in-depth knowledge of network and systems being tested
  - Gray box test - some limited information has been provided to the tester
- Two methods by which information is gathered:
  - Active reconnaissance – involves actively probing the system to find information
  - Passive reconnaissance – the tester uses tools that do not raise any alarms

Penetration Testing (3 of 3)

- Once the tester has gathered information
  - The next step is to perform an initial exploitation by using that information to determine if it provides entry to the secure network
- Once in side the network
  - Tester attempts to perform a pivot (moving around inside the network)
- Pentester's goal
  - Privilege escalation or exploiting a vulnerability to access an ever-higher level of resources
  - Testers must rely on persistence to continue to probe for weaknesses and exploit them

Practicing Data Privacy and Security

- Enterprise data theft may involve stealing proprietary business information
  - Such as research for a new product
- Personal data theft involves user personal data
  - Such as credit card numbers
  - Identify theft
- Practicing data privacy and security involves understanding what privacy is and its risks
  - As well as practical steps in keeping data safe

What is Privacy?

- Privacy
  - The state or condition of being free from public attention to the degree that you determine
  - The right to be left alone to the level that you choose
- Data is collected on almost all actions today
  - Through web surfing, purchases, user surveys, and questionnaires
- Data is then aggregated by data brokers
  - Who sell the data to interested third parties

Risks Associated with Private Data

- Risks associated with use of private data fall into three categories:
  - Individual inconveniences and identity theft
  - Associations with groups
  - Statistical inferences
- Risks have led to concern by individuals regarding how their private data is being used

Maintaining Data Privacy and Security

- There is a need to keep data private and secure for legal and compliance issues, which is following the:
  - Requirements of legislation, prescribed rules and regulations, specified standards, and terms of a contract
- Some laws include
  - HIPAA, Sarvox, GLBA, and PCI DSS
- Steps in maintaining data privacy and security:
  - Creating and following a overall security methodology
  - Properly labeling and handling sensitive data
  - Ensuring that data is destroyed when no longer needed

Secure Methodology

- Standard techniques for mitigating and deterring attacks
  - Creating a security posture
  - Selecting and configuring controls
  - Hardening
  - Reporting

Creating a Security Posture

- Security posture describes an approach, philosophy, or strategy regarding security
- Elements that make up a security posture:
  - Initial baseline configuration
    - Standard security checklist
    - Systems evaluated against baseline
  - Continuous security monitoring
    - Regularly observe systems and networks
  - Remediation
    - As vulnerabilities are exposed, put plan in place to address them

Selecting Appropriate Controls

Security goal	Common controls
Confidentiality	Encryption, steganography, access controls
Integrity	Hashing, digital signatures, certificates, nonrepudiation tools
Availability	Redundancy, fault tolerance, patching
Safety	Fencing and lighting, locks, CCTV, escape plans and routes, safety drills

Configuring Controls (1 of 2)

- Properly configuring controls is key to mitigating and deterring attacks
- Some controls are for detection
  - Security camera
- Some controls are for prevention
  - Properly positioned security guard
- Information security controls
  - Can be configured to detect attacks and sound alarms, or prevent attacks

Configuring Controls (2 of 2)

- Additional consideration
  - When a normal function is interrupted by failure:
    - Which is higher priority, security or safety?
  - Fail-open lock unlocks doors automatically upon failure
  - Fail-safe lock automatically locks
    - Highest security level
  - Firewall can be configured in fail-safe or fail-open state

Hardening

- Purpose of hardening
  - To eliminate as many security risks as possible
- Types of hardening techniques include:
  - Protecting accounts with passwords
  - Disabling unnecessary accounts
  - Disabling unnecessary services
  - Protecting management interfaces and applications

Reporting

- It is important to provide information regarding events that occur
  - So that action can be taken
- Alarms or alerts
  - Sound warning if specific situation is occurring
  - Example: alert if too many failed password attempts
- Reporting can provide information on trends
  - Can indicate a serious impending situation
  - Example: multiple user accounts experiencing multiple password attempts

Data Labeling and Handling (1 of 2)

- Data Sensitive data must be properly labeled
  - If mislabeled, could accidentally be publicly distributed
- Data sensitive labeling
  - Can help ensure proper data handling

Data Labeling and Handling (2 of 2)

Data label	Description	Handling
Confidential	Highest level of security	Should only be made available to users with highest level of preapproved authentication
Private	Restricted data with a medium level of confidentiality	For users who have a need-to-know basis of the contents
Proprietary	Belongs to the enterprise	Can be available to any current employees or contractors
Public	No risk of release	For all public consumption; data is assumed to be public if no other data label is attached
Personally Identifiable Information (PII)	Data that could potentially identify a specific individual	Should be kept secure so that an individual cannot be singled out for identification
Protected Health Information (PHI)	Data about a person's health status, provision of health care, or payment for health care	Must be kept secure as mandated by HIPAA

Data Destruction

- Paper media can be destroyed by burning, shredding, pulping, or pulverizing
- Electronic media
  - Data should never be erased using the OS “delete” command
    - Data could still be retrieved by using third-party tools
  - Wiping – overwriting the disk space with zeros or random data
  - Degaussing – permanently destroys the entire magnetic-based drive
    - By reducing or eliminating the magnetic field

Chapter Summary (1 of 2)

- Vulnerability assessment
  - Methodical evaluation of exposure of assets to risk
  - Three are five steps in a vulnerability assessment
- One tool used to assist in determining potential threats is a process known as threat modeling
- Several techniques can be used in a vulnerability assessment
- Port scanners, protocol analyzers, honeypots, and honeynets are used as assessment tools
- Banner grabbing can be used to perform an inventory on the services and systems operating on a server

Chapter Summary (2 of 2)

- A vulnerability scan searches system for known security weakness and reports findings
- Penetration testing designed to exploit any discovered system weaknesses
  - Tester may have various levels of system knowledge
- Privacy is defined as the state or condition of being free from public attention to the degree that you determine
- Standard techniques used to mitigate and deter attacks
  - Healthy security posture
  - Proper configuration of controls
  - Hardening and reporting

NMAP / ZenMap

- Download and Install NMAP / ZenMAP

  - https://nmap.org/dist/nmap-7.80-setup.exe

NMAP / ZenMap

In order to scan your Router

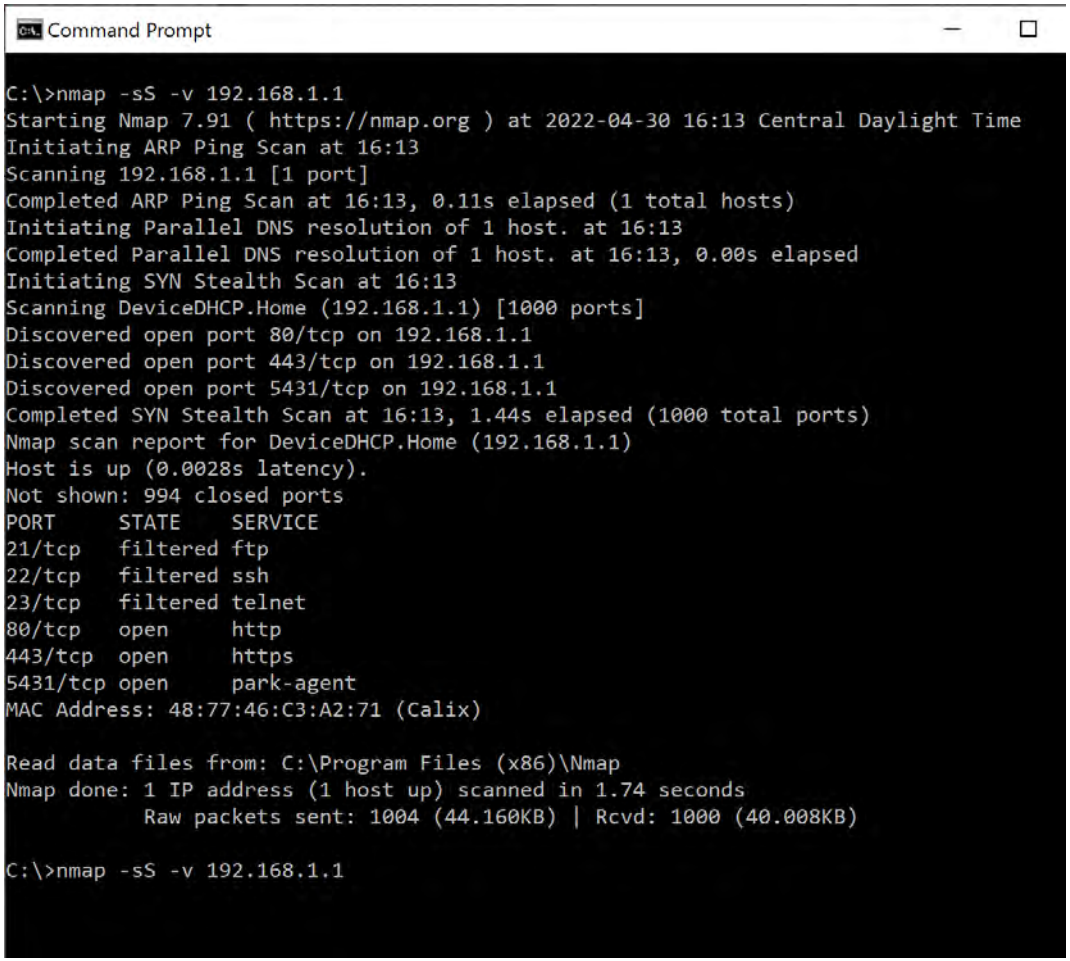
- Open a command prompt
- Type **nmap** with the appropriate switches/options
- **-sS** – SYN Scan

  OR

- **-sC** – Scripted Scan

  --script also works

- **-v** – Verbose Mode
- IP Address to scan
  - Example: 192.168.1.1



NMAP / ZenMap

In order to scan your Computer

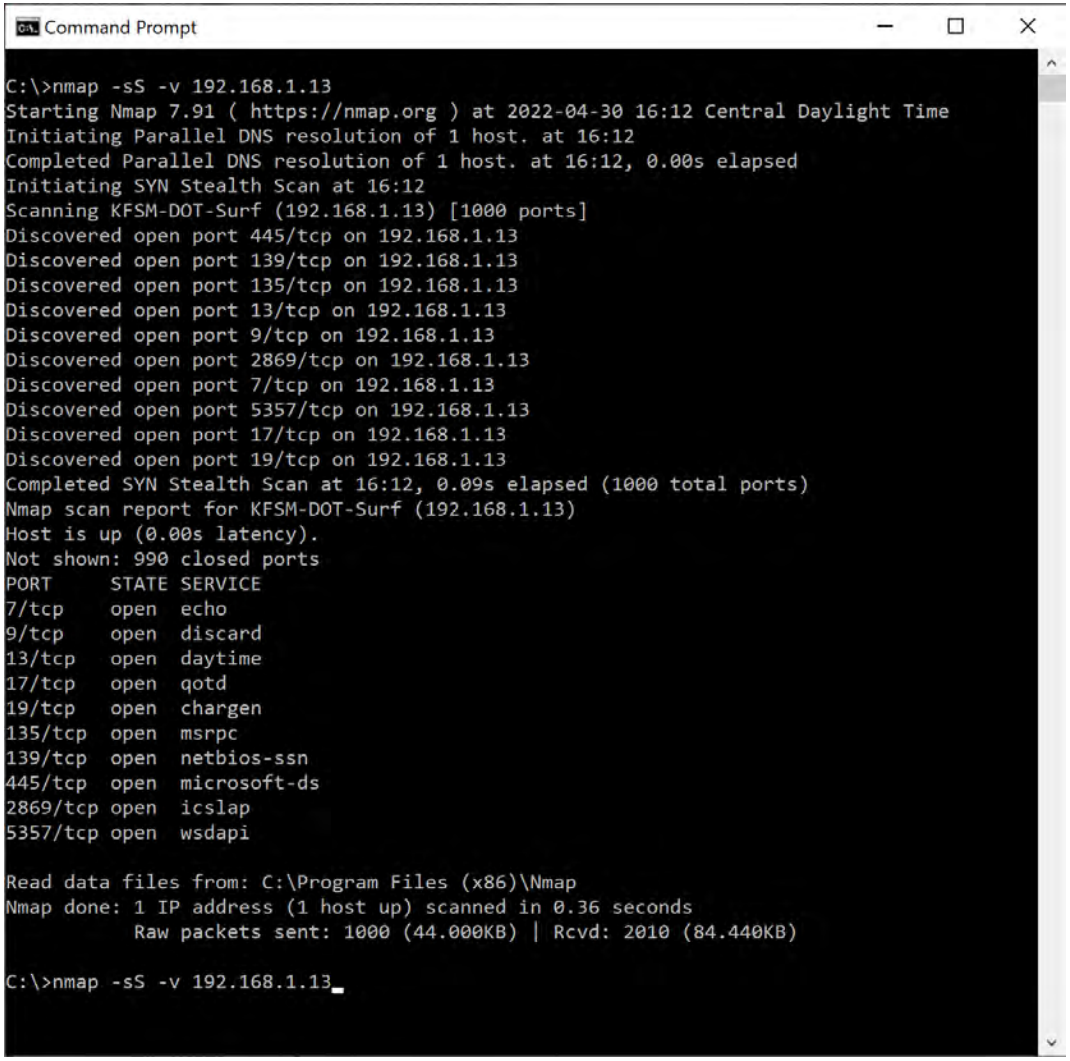
- Open a command prompt
- Type **nmap** with the appropriate switches/options
- **-sS** – SYN Scan

  OR

- **-sC** – Scripted Scan

  --script also works

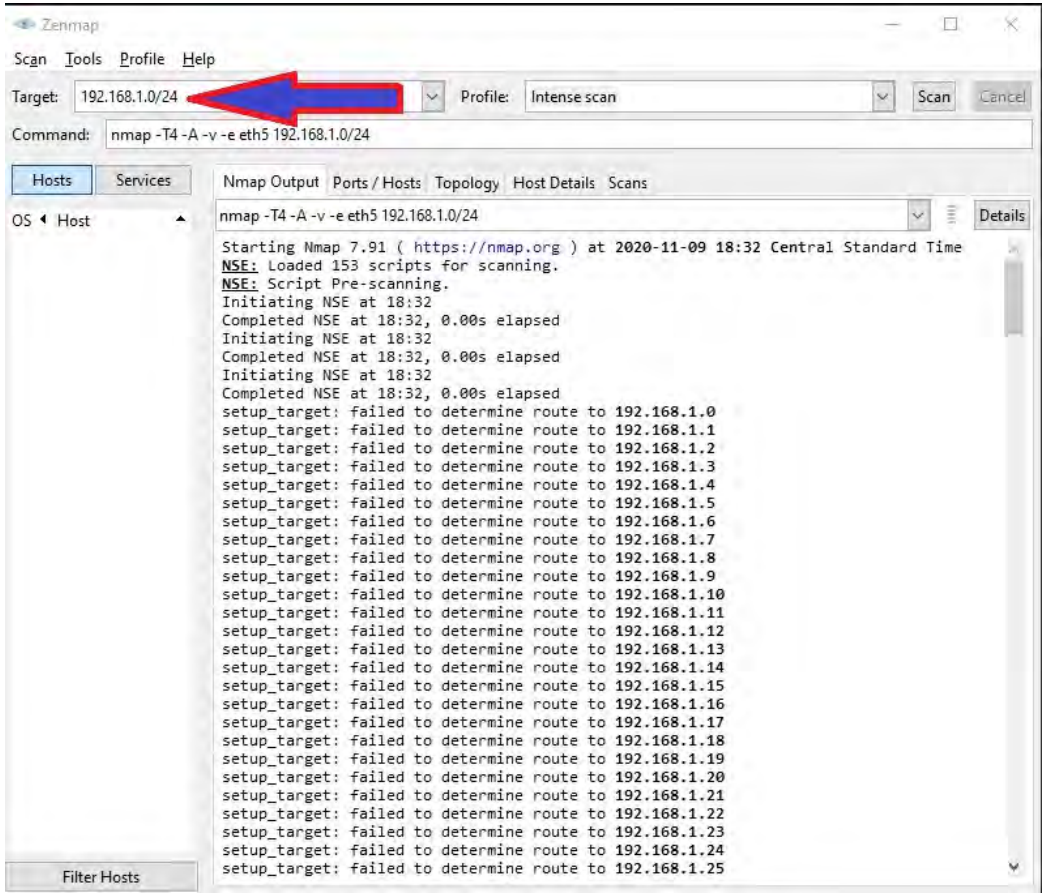
- **-v** – Verbose Mode
- IP Address to scan
  - Example: 192.168.1.13



NMAP / ZenMap

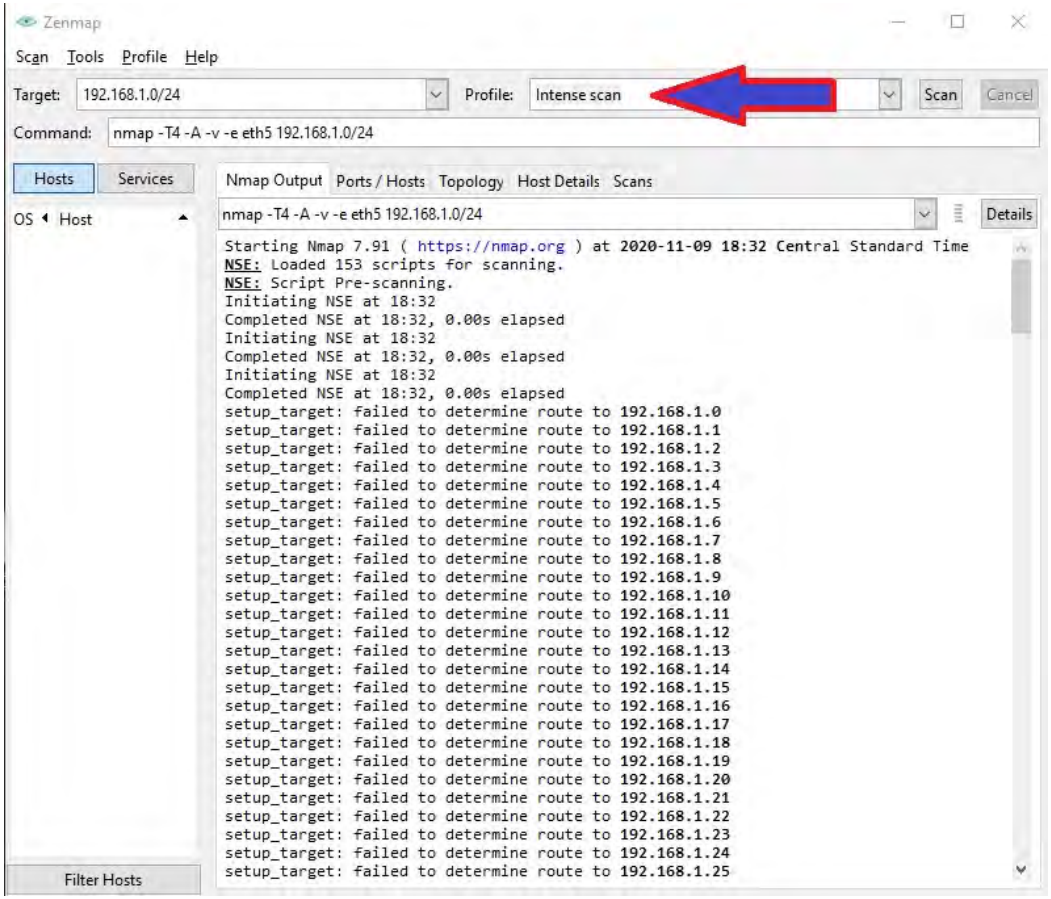
- GUI Version
- ZenMAP
  - In order to scan your network, simply add your network to the “Target” box.
  - A Single IP:
    - **192.168.0.1**

    OR
  - An Entire Network:
    - **192.168.0.1-254**



NMAP / ZenMap

- Select the type of Scan Under "Profile:"
  - "**Intense Scan**" is the default.



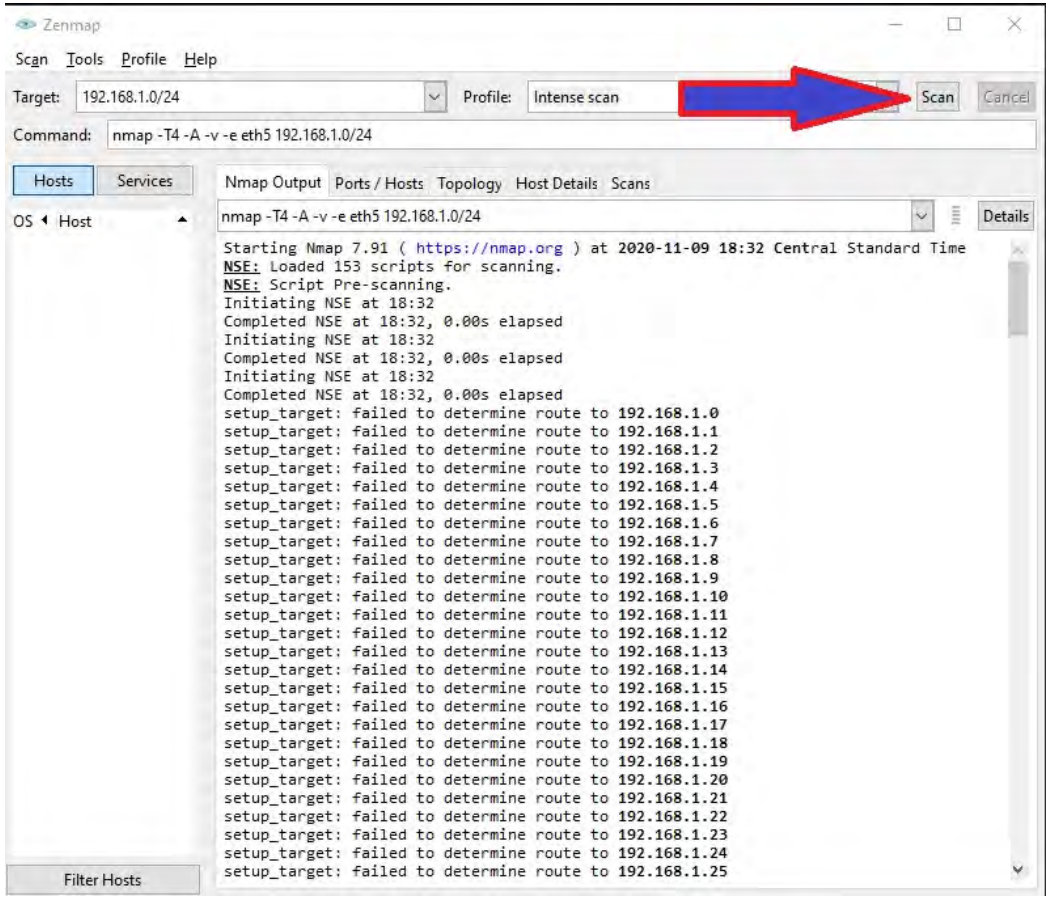
NMAP / ZenMap

- Finally Click:
  - "**Scan**"

    To begin the network scan.

    *Don't be alarmed if you don't see results right away…

    …This can take a while.



Review Questions

Which of the following is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm?

A. Vulnerability assessment

B. Penetration test

C. Vulnerability scan

D. Risk appraisal

Review Questions

Which of the following is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm?

A. **Vulnerability assessment**

B. Penetration test

C. Vulnerability scan

D. Risk appraisal

Review Questions

Which of the following command-line tools tests a connection between two network devices?

A. Netstat

B. Ping

C. Nslookup

D. Ifconfig

Review Questions

Which of the following command-line tools tests a connection between two network devices?

A. Netstat

B. **Ping**

C. Nslookup

D. Ifconfig

Review Questions

Which of the following is a command-line alternative to Nmap?

A. Netcat

B. Statnet

C. Mapper

D. Netstat

Review Questions

Which of the following is a command-line alternative to Nmap?

A. **Netcat**

B. Statnet

C. Mapper

D. Netstat

Review Questions

Which of these is NOT a state of a port that can be returned by a port scanner?

A. Open

B. Busy

C. Blocked

D. Closed

Review Questions

Which of these is NOT a state of a port that can be returned by a port scanner?

A. Open

B. **Busy**

C. Blocked

D. Closed

Coming Up Next…

CompTIA Security+

Chapter 14

Business Continuity