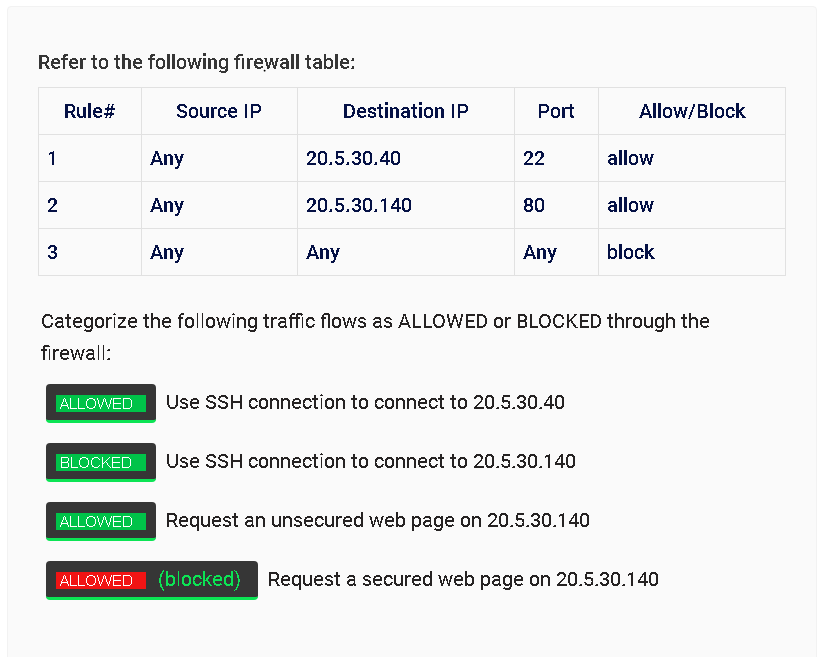
Study Guide:

**PART ONE:**

1. You are troubleshooting a faulty network. You need to illustrate the route packets take through the inter-network in order to identify the weak spot. Assuming you are working on a Windows environment, type the command to find where the packets are dropped.

Answer : c:\> tracert

1. There are no open ports to 443, so fourth question should’ve been blocked.



1. You are working at a Linux command prompt. Set the permissions of “file.txt” to ‘owner can read and write, group can only read, others can only read’ using permissions notation.

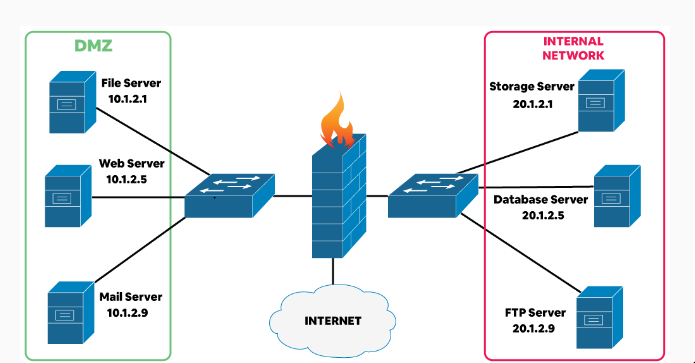
Answer: student@root:~$ chmod 644 file.txt

Another command to achieve the same outcome is ‘chmod u=rwx, g=rx, o=r file.txt’

1. You are at a windows 10 workstation and have a command prompt open. Type the command to view resource record information on a particular DNS server.

Answer: c:\> nslookup

Nslookup displays information that you can use to diagnose DNS infrastructure – it has two modes, interactive and noninteractive.

1. Configure the following stateful firewall rules:
   1. Allow the File Server to access the Database Server using LDAP
   2. Block the Storage Server to transfer files to the Web Server using FTP
   3. Allow the FTP Server to transfer files to the Mail Server over HTTPS



In the above scenario, I assumed that I would have to block the connection from the Storage Server to the FTP server, however blocking the connection from the Storage Server directly to the Webserver on the FTP port ( 21 ) was the correct methodology.

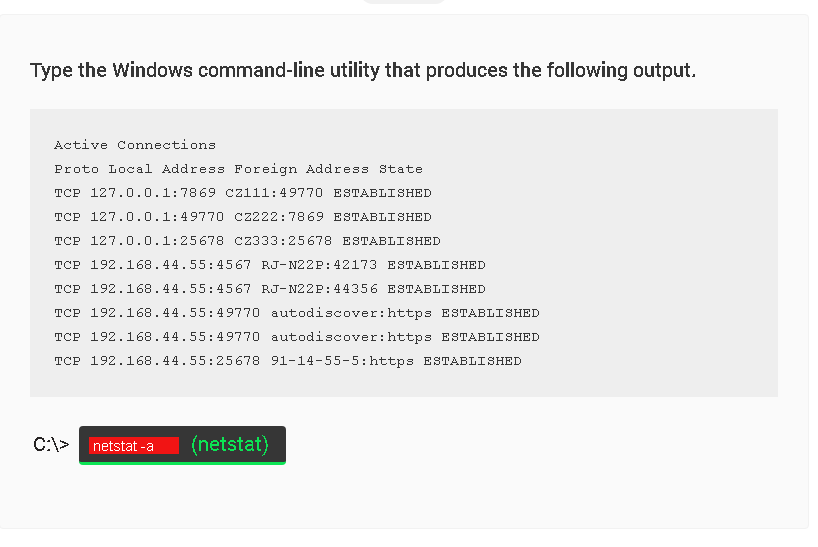
1. You want to capture HTTP packets using tcpdump. The HTTP service is running on its default port and your Ethernet adapter is eth1. Type the command to capture the packets.

Answer: student@root:~$ tcpdump –I eth1 tcp port80

1. Match the characteristics to type:
   1. An attack that shuts down a machine or network, making it inaccessible to its intended users
      1. DoS ( Denial of Service )
   2. A type of social engineering attack where an attacker sends a fraudulent (“spoofed”) message designed to trick a human victim into revealing sensitive information to the attacker.
      1. Phishing
   3. An attacker impersonates an authorized device or user to steal data, spread malware, or bypass access control systems
      1. Spoofing
   4. The act of changing the registration of a domain name without the permission of the original owner
      1. Domain hijacking
2. You need to search and display the total number of times that the tag “h1” appears in a file named main.html using grep. Type in the linux command for it.

Answer = student@root:~$ grep –c “h1” main.html

1. Type in the Windows command-line utility that produces the following output



1. Identify the type of attack
   1. An attack that is implemented through text messages or SMS. The criminal executes the attack with the intent to gather personal information, including social insurance and/or credit card numbers
      1. Smishing (SMS phishing)
   2. A phone attack designed to get you to share personal information. The attacker uses social engineering to get you to share personal information and financial details, such as account numbers and passwords
      1. Vishing (Voice Phishing)
   3. A type of social engineering attack which is used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerades as a trusted entity.
      1. Phishing
   4. An email or electronic communications scam targeted towards a specific individual, organization or business
      1. Spear phishing

**PART TWO:**

1. **OTP vs HOTP vs TOTP**
   1. OTP ( One-time password)
   2. HOTP (HMAC-based One-time Password)
      1. HMAC stands for Hash-based Message Authentication Code
      2. Event-based OTP where the moving factor in each code is based on a counter
      3. Each time the HOTP is request and validated, the moving factor is incremented based on a counter
      4. The generated code is valid until you request for another code and that code is validated
      5. No Expiration (only expires when new code is requested)
   3. TOTP ( Time-based One-time Password)
      1. Moving factor is time-based rather than counter-based
      2. Amount of time each password is valid is called a ‘timestep’
      3. Timesteps are usually set to 30seconds or 60 seconds – and if you haven’t used the password in that time-frame, it will no longer be valid and a new one must be requested.
      4. Expiration ( Expires when duration of Timestep has been reached)
2. **Asymmetric Encryption and Symmetric Encryption**
   1. Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message
      1. Older technique
      2. Takes less time to deliver message
   2. Asymmetric encryption uses a pair of public keys and a private key to encrypt and decrypt messages when communicating.
      1. Newer Technique
      2. Introduced to solve the need to share the key in the symmetric encryption model, eliminating the need to share the key by using a pair of public-private keys.
      3. Takes more time to deliver message
      4. Examples of Asymmetric Algorithms
         1. RSA (Rivest, Shamir, Aldeman)
         2. ECC(elliptic curve cryptography)
         3. Diffie-Hellman,
         4. EIGamal,
         5. McElience,
         6. NTRU(N-th degree Truncated polynomial Ring Units),
         7. PGP (Pretty Good Privacy),
         8. DSA (Digital Signature Algorithm)
3. **Incident Response, Recovery and Repair**
   1. Terminology
      1. MTTR = Mean time to recovery or Mean time to restore
      2. MTBF = Mean time between failures
      3. RTO = Recovery Time Objective
         1. How long it will take to recover and get back to business
      4. RPO = Recovery Point Objective
         1. The maximum allowed time that a business can go without data loss.
         2. The maximum time a service can be down before serious damage is incurred
4. **AI vs ML**
   1. AI does not need datasets to learn what traffic is malicious
   2. MI needs datasets to learn what traffic is malicious\
5. **PPTP(Point-to-Point Tunnelling Protocol) & SSL(Secure Sockets Layer)**
   1. SSL
      1. Protocol for establishing secure, encrypted links between networked computers
      2. SSL certificates initiate secure sessions with the users browser via the SSL protocol
      3. This secure connection cannot be established without the SSL certificate
      4. Digitally connects information to a cryptographic key
      5. Successor to SSL is TLS(Transport Layer Security)
   2. PPTP
      1. Protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network across TCP/IP-based networks.
      2. Uses TCP control channel and Generic Routing Encapsulation tunnel to encapsulate PPP packets.
      3. Operates on port 1723
      4. Most common, easiest to setup and computationally the fastest
      5. Useful for applications in which speed is paramount, like audio or video streaming.
      6. There are many known security issues.
   3. Insecure for VPN, use IPSec instead
      1. IPSec is a group or framework of protocols that are used together to setup encrypted connections between devices
         1. Often used by VPNS
         2. Works by encryption IP packets
         3. authenticates source of packets
         4. Enables data confidentiality, integrity, origin authentications and anti-replay
         5. Used to protect one or more data flows between peers
         6. Works at the network or packet processing layer.
6. **Types of Data Deletion**
   1. Shredding
      1. Process of irreversible file destruction, so that its contents cannot be recovered
      2. sometimes called erasing or wiping
   2. Purging
      1. Removing sensitive data from drive using its internal electronics OR outside sources, such as degausser (device that interferes or demagnetizes the magnetic strips inside hard drive)
   3. Wiping
      1. Wiping allows for data to be overwritten so it cannot be recovered
      2. Can be done 1x, 7x, 35x and drive is still usable afterwards
   4. Deleting
      1. Removal of files the hard drive however there is still possibility of them being recovered using recovery techniques/software.
7. **Data Employment Positions**
   1. Data Protection Officer (DPO)
      1. Responsible for organization data privacy, sets policies, implements processes and procedures
   2. Data Owner
      1. Responsible for CIA (Confidentially, Integrity, Availability) and privacy of informational assets.
      2. Usually senior executives
      3. Typically selects Data Steward and Data Custodian and has the authority to direct their actions and budget
   3. Data Steward & Custodians
      1. Responsible for data quality
      2. Ensure compliance with the law and standards
      3. Manages access rights to the data
      4. Implements Security Controls
   4. Data Controller
      1. Manages the purpose and means by which the data is processed
8. **Access Control Models**
   1. Role Based Access Control (RBAC)
      1. Your role in your company will determine what you will have access to.
   2. Attribute Based Access Control (ABAC)
      1. Access is based on many criteria and “attributes” that an employee possesses.
      2. Next generation access control
   3. Discretionary Access Control (DAC)
      1. Owner of the object decides what level of access will be provided
      2. Most common and least secure due to the creator being able to decide solely without systematic security measures.
   4. Mandatory Access Control (MAC)
      1. Restricting access to resources based on the sensitivity of the information.
      2. Requires formal authorization of users to access sensitive information
      3. Difference Clearance levels for different levels of sensitive information
9. **Single Sign-on Details**
   1. Identity Provider (iDP): Third party tool that manages user identity data. Stores and manages user’s digital identities, guest lists. Used to support SSO.
      1. Authentication Methods
         1. SAML (Security Assertion Mark-up Language)
            1. XML-based authentication industry standard
            2. Eliminates the need for application-specific password
            3. Single-use expiring, digital tokens to exchange authentication and authorization data between an identity provider and a service provider that have an established trust relationship
            4. Works by exchanging user information, such as logins, authentication state, identifiers and other relevant attributes between the identity and service provider.
            5. Open Standard / Umbrella standard that covers federation, identity management and SSO
            6. Can authenticate through third parties
            7. Activates SSO for browser based applications
            8. Not Designed for mobile apps
            9. Allows for federated identities
            10. Simplifies and secures the authentication process as the user only needs to login once ( Single Sign On)
      2. OAuth
         1. Provides authorization on various third-parties applications or servers.
         2. Uses access tokens to allow an application to authenticate on behalf of a user to another application AND to retrieve data owned by the user.
         3. Created by Google and Twitter
         4. OAuth is used for authorization while OpenID is used for authentication
         5. NOT AUTHETICATION SERVICE, it is an AUTHORIZATION SERVICE
      3. RP (Resource Provider)
         1. Application within the SSO federation that contains protected data
      4. SP (Service Provider)
         1. A web server from where the user accesses information
         2. Uses SAML protocol to authenticate user logins within an SSO federation
         3. Also requests access to protected data from an RP (resource provider) on behalf of an authenticated user
      5. SSO (Single Sign On)
         1. Authentication scheme that allows a user to login with a single ID & password on independent systems across a federation.
10. **Hash Algorithms**

|  |  |  |
| --- | --- | --- |
| ***Algorithm*** | ***Bits*** | ***Block Size*** |
| MD5 | 128 | 512 |
| SHA/SHA-1 | 160 | 512 |
| SHA2 | 224/256/384/512 | 512/1024 |
| SHA3 | 224/256/384/512 | 1152/1088/832/576 |
| RIPEMD | 128 | 512 |
| NTLM | 128 |  |

1. **Books**
   1. Playbook
      1. Check list of actions to perform to detect and respond to an incident
   2. Runbook
      1. Automated version of a playbook
2. **Bluetooth Attacks**
   1. Bluejacking
      1. sends unsolicited messages over Bluetooth to a mobile device
   2. Bluesnarfing
      1. Takes data from the mobile device
3. **Reconnaissance Tools**
   1. Traceroute / Tracert
      1. determines the route packets take, and maps it
      2. Uses ICMP time-to-live(TTL) exceeded error messages to determine number of hops
      3. TTL is hops and not time (TTL1 = 1st router, TTL2 = 2nd router etc...)
   2. Nslookup / dig
      1. Looks up DNS servers, IP addresses, Cache Timers and Names
      2. Nslookup is simple but deprecated
      3. Dig is more advanced, should be used as a first choice
   3. Ipconfig / Ifconfig
      1. Determines TCP/IP and network adapter info
      2. Most troubleshooting starts with this command
      3. ipconfig /all
         1. Shows more in-depth information such as MAC addresses DNS servers etc...
   4. Nmap
      1. Used for port scanning, mapping, operating system scans, service scans
   5. Pathping
      1. Combines ping and traceroute
      2. first phase runs traceroute
      3. second phase finds round trip time and packet loss
   6. Hping
      1. TCP/IP packet assembler and/or analyser.
      2. Allows the sending of crafted frames
      3. Very powerful, can accidently DoS
   7. Netstat
      1. Provides Network Statistics
   8. Netcat
      1. Reads or writes to network
      2. Many functionalities
         1. Listens on ports
         2. Transfers data
         3. Scans ports
         4. Sends data to port
   9. Arp
      1. View local Address Resolution Protocol Table
   10. theHarvester
       1. Open-source Intel Gathering Tool
       2. Scrapes info from websites
       3. Can find PGP(Pretty Good Privacy) keys by email domain
   11. sn1per
       1. Combines many tools into one
          1. These include:
             1. dnsenum, metasplot, nmap, theharvester
             2. both intrusive and non-instrusive scanning options
             3. bruteforce, server scanning
   12. Nessus
       1. General Vulnerability Scanner (Web apps etc.)
   13. Cuckoo
       1. Sandbox software for malware analysis
   14. Cat
       1. View contents of a file, create a new file, combine two files into one etc.
       2. can also be used to view contents of file in reverse by using:
   15. Grep
       1. Searches for a string in groups of files
   16. **Shell and Scripts**
       1. .ps1 ext is a windows powershell file
       2. OpenSSL is a toolkit and library for SSL/TLS
          1. Can create x509 certs
             1. standard format for public key certificates
             2. shell scripts can retrieve x509 certificates associated with TLS wrapped TCP port and uses openssl to create similar certificates
             3. x509 command can be used to display certificate information, convert certificates to various forms etc.
   17. **File Manipulation Tools**
       1. Head
          1. view part of the file from the start
       2. Tail
          1. view last part of a file
   18. **Forensic Tools**
       1. Dd (linux)
          1. command to create disk image
       2. FTK Imager
          1. include file tools, and read only image mounting
          2. Widely Supported
          3. Can support dd (raw format), ghost images, expert witness disk image format
       3. Autopsy
          1. Allows for forensics of storage, smartphones etc..
          2. Allows to extract many types of files
   19. **Incident Response Life Cycle**
       1. Preparation
          1. Phase of preparation for an incident before they occur
       2. Detection & Analysis
          1. Incidents occur all the time
          2. Requires constant monitoring of organizations activities
          3. Difficult due to mass of data
       3. Containment, Eradication & Recovery
          1. Containment or Preventing more damage can include:
             1. Sandboxing

Isolated OS designed to run and analyse the results

* + - * 1. Isolation

Can create problems because the system won’t be accessible to the production environment.

Malware monitors for this type of containment

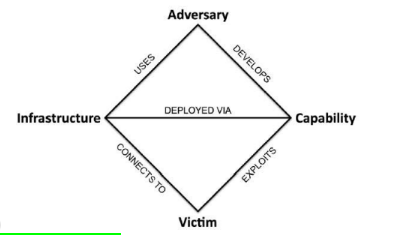
* + - * 1. Eradicating

Can involve completely deleting or recovering the system

* + - * 1. Recovery

Process of rebuilding after a incident or damage has occurred

* + 1. Post-Incident Activity
       1. Stage where you analyse what went wrong, how you could have done better and what you should do to improve
       2. Generate a Lessons Learned Report
  1. **Attack Frameworks**
     1. MITRE ATT&CK Frameworks: Supports U.S Gov’t Agencies
        1. Determine actions of the attacker
        2. Identify point of intrusion
        3. Understand the methods of the attack
        4. Identify potential security measures to block future attacks
     2. Diamond Model of Intrusion
        1. Designed by the intelligence community
        2. Integrates well with other frameworks
        3. Applies scientific principles
        4. Very complex despite simple appearance



* + 1. Cyber Kill chain
       1. Seven phase attack
          1. Reconnaissance

Research, Identification and selection of targets

* + - * 1. Weaponization

Pairing remote access malware with exploit into a deliverable payload

Such as via Adobe PDF, Office Files, Malicious Links

* + - * 1. Delivery

Transmission of the weapon to the target

Ex. Via email attachments, websites or USB devices, exploiting hardware of software flaws

The key of successful delivery is to deliver the payload undetected

* + - * 1. Exploitation

Once weapon has been delivered to the target, the weapons code is triggered, exploiting vulnerable applications or systems

Ex. Exploiting password vulnerabilities, credential extraction, brute force attacks and targeting other system vulnerabilities.

* + - * 1. Installation

Actions taken by a threat actor to establish a backdoor into the targets system all while keeping their presence a secret

The weapon installs a backdoor on a targets system allowing persistent access

ex. Installation of tools, creation of script files, modify security certificates, and search for additional vulnerabilities

* + - * 1. Command and Control (C2)

Outside servers communicates with the weapons providing “hands-on keyboard access” inside the targets network

Once C2 is established within a target, threat actors will have access to the target system and possibly the entire network.

C2 allows threat actors to issue commands to the malicious software that has been installed on the target/s

* + - * 1. Actions on Objectives

The attacker works to achieve their objective

Ex. Exfiltration or Destruction of data or traversal/intrusion of another target, encryption for ransom etc.

They also may attempt to cause confusion, such as masking the activity, in order to meet their objectives.

* + - 1. A military concept developed by Lockheed-Martin
    1. HITRUST CSF
       1. Certifiable framework that provides organizations with comprehensive, flexible and efficient approach to regulatory compliance and risk management.
       2. Control Categories
          1. Information Security Management Control Program
          2. Access Control
          3. Human Resources Security
          4. Risk Management
          5. Security Policy
          6. Organization of Information Security
          7. Compliance
          8. Asset Management
          9. Physical and Environmental Security
          10. communications and Operations Management
          11. Information Systems Acquisition, Development and Maintenance
          12. Information Security Incident Management
          13. Business Continuity Management
          14. Privacy Practices
       3. Held to the standards of HIPAA, NIST 800-53, PCI-DSS, ISO 27001/2, COBIT, and GDPR among others.
    2. NIST Framework
       1. Core elements comprise of:
          1. Functions, Categories, Subcategories and Informative References
       2. Core functions
          1. Identify

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management Strategy

Supply Chain Risk Management

* + - * 1. Protect

Identity Management and Access Control

Awareness and Training

Data Security

Information Protection Processes and Procedures

Maintenance

Protective Technology

* + - * 1. Detect

Anomalies and Events

Security Continuous Monitoring

Detection Processes

* + - * 1. Respond

Response Planning

Communications

Analysis

Mitigation

Improvements

* + - * 1. Recover

Recovery Planning

Improvements

Communications

* 1. **Vulnerability Scans**
     1. Credentialed Scans
        1. Scan that uses login credentials on an asset it scans to get deeper access to the assets data.
           1. Windows, this means a login ID and password
           2. Linux, can be in the form of a SSH key.
     2. Non-Credentialed Scans
        1. Provide a quick view of vulnerabilities by only looking at network services exposed by the host