CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel Due: 1/24/21

Lab Homework 1: Configuring Windows Firewall

1 Chapter 1 Questions

1.1 Short Answer

1. If you have been contracted to perform an attack against a target system, you are what type of hacker?
   White hat.

2. Which of the following describes an attacker who goes after a target to draw attention to a cause?
   Hactivist.

3. What level of knowledge about hacking does a script kiddie have?
   Low.

4. Which of the following does an ethical hacker require to start evaluating a system?
   Permission.

5. A white-box test method means the tester has which of the following?
   Complete information of system / network.

6. Which of the following describes a hacker who attacks without regard for being caught or punished?
   Suicide Hacker.

7. What is a code of ethics?
   A description of expected behavior.

8. The group anonymous is an example of what?
   Hacktivists.

9. Companies may require a penetration test for which of the following reasons?
   Regulatory reasons, IT audit, Network performance.

10. What should a pen-tester do prior to initiating a new penetration test?
    Get permission.

11. Which of the following best describes what a hacktivist does?
    Hacks for political / ideological reasons.

12. Which of the following best describes what a suicide hacker does?
    Hacks without stealth.

13. Which type of hacker may use their skills for both benign and malicious goals at different times?
    Gray Hat.

14. What separates a suicide hacker from other attackers?
    Lack of fear of being caught.

15. Which of the following would most likely engage in the pursuit of vulnerability research?
    White Hat.

16. Vulnerability research deals with which of the following?
    Passively uncovering vulnerabilities / weaknesses.

17. How is black-box testing performed?
    With no knowledge.

18. A contract is important because it does what?
    Gives proof of permission.

19. What does TOE stand for?
    Target of evaluation.

20. Which of the following best describes a vulnerability?
    Weakness (in a system).

21. What is the most important aspect when conducting a penetration test?
    Recieving formal written agreement, Documenting all actions and activities and maintaining proper handoff with the information assurance team, remediating serious threats immediately

22. Some detail of target system is what kind of assessment?
    Gray box testing.

23. A team that conducts penetration testing can be refereed to as what?
    Red team.

24. Which of the following organizations provides government-backed standards?
    NIST (National Institute of Standards and Technology).

25. Which term best describes the several hacking attacks in sequence?
    Daisy Chaining.

26. A penetration tester is which of the following?
    A security professional who's hired to break into a network to discover vulnerabilities.

27. How can you find out which computer crim law are applicable in your state?
    contact you local law enforcement agencies.

28. What organization offers the CEH certification exam?
    EC-Council

29. A written contract isn't necessary when a friend recommends a client?
    False

1.2 Long Answer

1. What is Ethical hacking? Who are Hackers? Describe types of Hackers.
   Ethical hacking is breaking into a system with the owners permission to report on the weaknesses of the system to correct unsecured applications as well as analyze a companies security policy and procedures for industry regulations. Hackers are categorized by their skill and intent. Black hat hackers are criminals that illegally break into systems, White hat hackers follow a code of ethics to separate themselves from black hat hackers. Gray hat hackers could be good or bad and should not be fully trusted. Suicide hackers are not worried about stealth because they do not fear prison time. Script kiddies require the lowest skill and do not understand most of what they do.

2. Describe tasks of the penetration tester.
   Once receiving a contract, the penetration tester will follow 7 phases, footprinting, scanning, enumeration, system hacking, privilege escalation, planting backdoors, and covering tracks, where the last 4 could be lumped into one 'hacking' task. After assessing the security of the system, the tester will prepare a report of everything they found to be presented to the client. Depending on the contract the tester could have to also give remedial recommendations or perform the remediation themselves.

3. Why Companies / organizations need penetration testers?
   Security is becoming more important with the increased access to personal data. Penetration testers ensure compliance with industry laws such as HIPPA and to keep the IT staff from becoming to complacent. Hackers are finding new vulnerabilities and the IT team needs to be assured that their data is secure. Monitor networks.

4. Describe Pen-testing methodologies.
   Using a black box methodology, the penetration tester is not given any information about the network topology or devices / services in use. The tester will have to find out as much as they can from outside the network before attempting to break into it. With a white box model, the pen tester is given all crucial information about the system such as network topology, devices, operating systems and staff.

5. Describe phases of Pen testing process.
   Footprinting is the initial phase of the penetration test where the tester gathers as much information about the system from the outside, ip addresses of servers and users, what operating systems are on which machines, domain information from websites. The scanning phase is a deeper look into the data gathered from footprinting, which ports are open on what machines. Enumeration establishes an active connection to the target hosts to discover potential attack vectors in the system, gathering usernames, group names, hostnames, network shares and services. Next the pen tester can start hacking using the data that has been gathered.

6. Describe detail on any two certification exams available in industry, that prepare you for jobs in domain of 'ethical hacking'.
   The OSCP is the offensive security certified professional, which teaches network and application exploits, buffer overflows, data manipulation scripts and hands on system exploits.
   The Certified Ethical Hacker course developed by the International Council of Electronic Commerce Consultants (EC-Council) covers 22 subject areas

2 Chapter 2 Questions

2.1 Short Answer

1. At which layer of the OSI model does a proxy exist?
   Layer 7, application.

2. If a device is using node MAC (media access control) address to funnel traffic, what layer of OSI model is this device working on?
   Layer 2 (data link layer).

3. Which port uses SSL to secure web traffic?
   443.

4. What kind of domain resides on a single switch-port?
   Collision domain.

5. Which network topology uses a token-based access methodology?
   Ring

6. Hubs operate at what layer of the OSI model?
   Layer 1

7. What is the proper sequence of the TCP three-way-handshake?
   SYN, SYN-ACK, ACK

8. Which of these protocols is a connection-oriented protocol?
   TCP

9. A scan of a network client show that port 23 is open; What protocol is this aligned with?
   Telnet

10. What port range is an obscure third-party application most likely to use?
    49152 to 65535

11. Which category of 'firewall filters' is based on packet header data only?
    Packet filter

12. An administrator has just been notified of irregular network activity; what appliance functions in this manner?
    IDS (Intrusion detection system)

13. Which topology has built-in redundancy because of its many client connections?
    Mesh

14. When scanning a network via a hardline connection to a wired-switch NIC, in promiscuous mode, what would be the extent of network traffic you would expect to see?
    All nodes attached to same port.

15. What device acts as an intermediary between an internal client and a web resource?
    Proxy

16. Which technology allows the use of a single public address to support many internal clients while also preventing exposure of internal IP addresses to the outside world?
    NAT (Network Address Translation)

17. What network appliance senses irregularities and plays an active role in stopping that irregular activity from continuing?
    IPS (Intrusion prevention system)

18. Matthew has selected the option in IDS to notify via email if it senses any network irregularities. Checking the logs, there are incidences but he did not receive any emails. What protocol needs to be enabled on the IDS?
    SMTP.

19. Choosing a protective network appliance, you want a device that will inspect packets at the most granular level possible, while providing improved traffic efficiency. What appliance would satisfy these requirements?
    Proxy firewall

20. What is the difference between a traditional firewall and an IPS?
    IPS can dissect packet.

21. Which of the following options shows the well-known ports?

22. Of the following methods, which one acts as a middleman between an external network and the private network by initiating and establishing the connection?

23. What are two common ports used to connect to a web server?
    443 and 80

24. Which two protocols are connectionless?
    IP and UDP

25. At which layer of the OSI model does FTP reside?

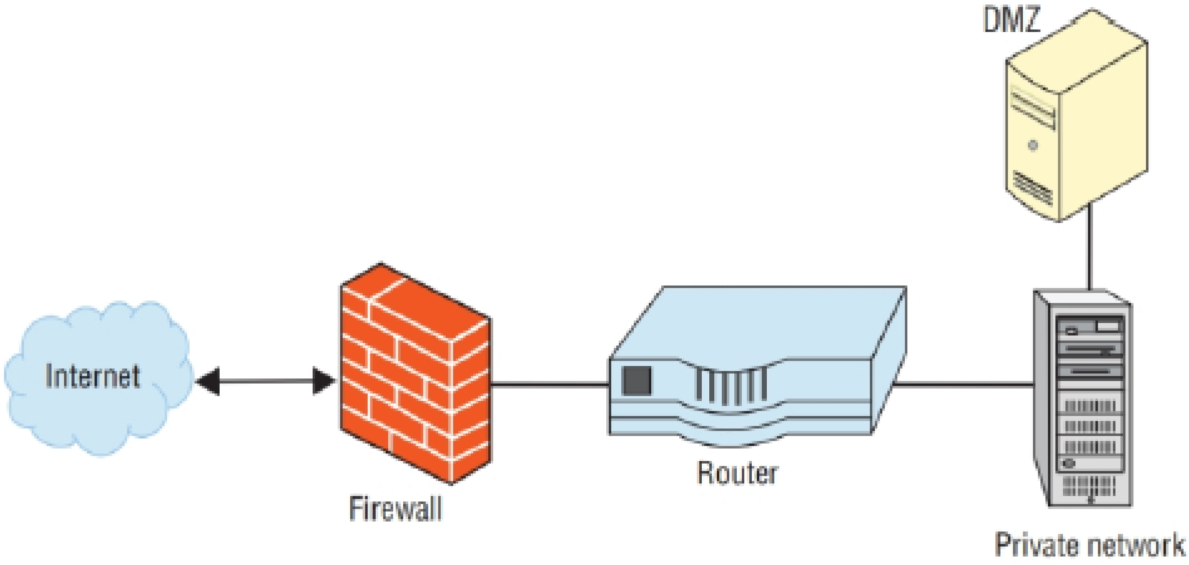
26. What port is used by DNS?
    53

27. What would you call an IP address bonding with a port number?

28. Which of the following allows networks to be sub netted into various sizes in IP4 system as IP6 will take years to be fully implemented?

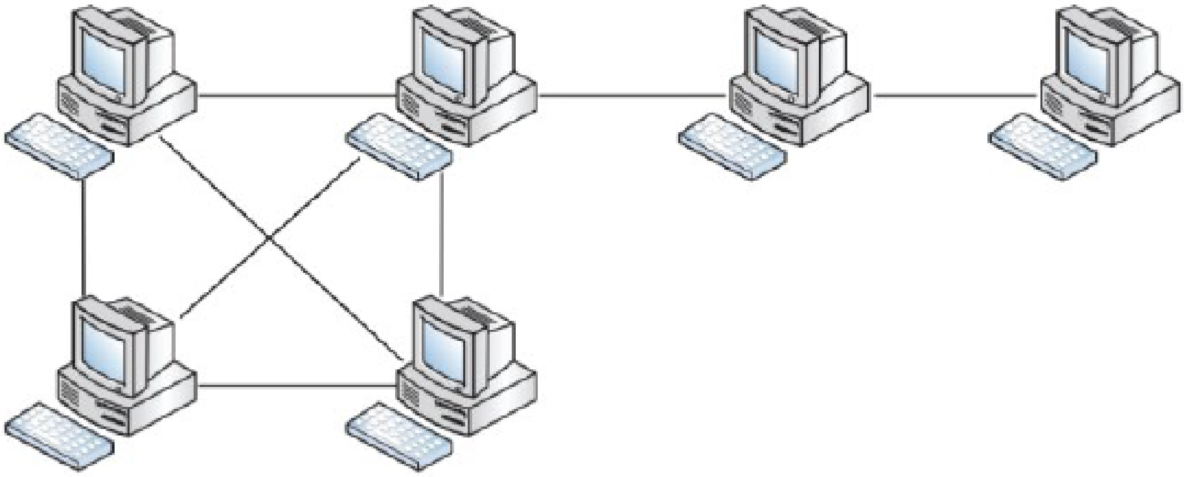
29. At what layer does ICMP (internet control message protocol) operate?

30. What is wrong with the following diagram?



The DMZ should be associated with the Internet. The DMZ should reside off the firewall and not directly off from the private network.

31. What type of network topology is being shown in the following diagram?



32. Which header field is used to reassemble fragmented IP packets?

33. What for a MAC address used?

2.2 Long Answer

- Describe types of network. What is importance of Mesh network / hybrid network. Types of networks vary based on their level of connectivity and redundancy, Bus networks have one connection that every nodes use, the design is simple but hard to troubleshoot if an issue comes up. Ring networks are similar to bus networks but provide more redundancy by layering rings. Star networks are popular for the ease of setup and troubleshooting, by connecting every node to a central device that ties the network together. Mesh and hybrid networks attach groups of nodes to each other, have a high level of redundancy and resistance to outages. These are important because our current networks are built and improved off of past networks, creating more complicated structures as networks are expanded, mesh and hybrid networks better support this.

- What is ports in computer networking. Write on different categories of ports and their functionalities.
  Ports identify types of traffic associated with a protocol or application. If you need to connect to the internet, port 80 or 443 will be used depending on if you are connecting via HTTP or HTTPS. In our lab we disabled connections on port 80, meaning the client could not connect to a web server via unsecured HTTP, but could connect to a HTTPS webpage. Well known ports are between 0 and 1023, registered ports are between 1024 and 49151, dynamic ports are from 49152 to 65535.

- Describe on IP address assignment system.
  When connecting to a network for the first time DHCP will assign a ip address that connects the MAC address of the device to a single IP on the network. This allows connections to be made by using the assigned IP address. You can view the IP address via `ipconfig` command in Windows. The commaind `ipconfig /release` will free the IP address from you machine and allow it for use on a different machine. `ipcocfig /renew` will request a new IP address for the host from DHCP.
  `ipconfig, ipconfig \all, ipconfig \release, ipconfig \renew`

- What firewall does. Write on types of firewalls
  Firewalls are used to block unwanted or malicious connections by analyzing the packets header information, state of connections or the packet payload for any abnormalities. Packet filtering firewalls drop packets by filtering the source and destination addresses, ports, and protocols. Stateful firewalls determine if traffic is legitimate based on the state of connection from which the traffic originated. Deep packet inspection firewalls look into the payload of the packet for any malware or attack before the packet reaches its destination.

- Explain what type of information a packet (computer networking technology) contain.
  Packets are small chunks of data passed over networks and have defined sections of information to ensure that the packet will get to its location.

3 Chapter 4

3.1 Short Answer

1. Which of the following best describes footprinting?
   Investigation of a target.

2. Which of the following is not typically used during footprinting?
   Port Scanning.

3. Why use Google Hacking?
   To fine tune search results.

4. Which of the following is natively installed on *nix OS systems to conduct DNS queries?
   Dig.

5. What is EDGAR used to do?
   Chech financial files.

6. Which of the following can be used to tweak or fine-tune search results?
   Operators.

7. Which of the following can an attacker use to determine the technology and structure within an organization?
   Job boards.

8. Which of the following can be used to assess physical security?
   Street views.

9. Which of the following can help you determine business processes of your target through human interaction?
   Social Engineering.

10. The Wayback Machine is used to do which of the following?
    View archived versions of websites

11. Which record will reveal information about a mail server for a domain?
    MX.

12. Which tool can be used to view web server information?
    Netcraft.

13. what can be configured in most search engines to monitor and alert you of changes to content?
    Alerts.

14. What phase comes after footprinting?
    Scanning.

15. If you can't gain enough information directly from a target, what is another option?
    Competitive analysis.

16. Which of the following provides free information about a website that includes phone numbers, administrator's email, and even domain registration authority?
    `lookup.icann.org`

17. Which of the following would be a very effective source of information as it relates to people's personal and contact information?
    Social networking.

18. Footprinting can determine all of the following except `_____`?
    Detail business distribution and number of personnel.

19. Footprinting has mainly two types. What are they?
    Active and passive.

20. Which tool can trace the path of a packet?
    `tracert`.

21. What does the TTL value mean?
    Time to leave : packet remaining live until it times out.

22. What information does the traceroute tool provide?
    Route path information an hop count.

23. Which of the following acronyms represent the institution that governs / tracks North American IP space?
    ICANN.

24. What phase of hacking is: gathering publicly available information, staking out the facility, observing workers as they enter and leave?
    Passive reconnaissance.

25. What program can be used to discover firewalls.
    Traceroute.

26. what DNS record type provides the port and services the server is hosting?
    SRV (service record).

27. You see the following text written down – Port:502. What does that likely reference?
    Shodan search.

28. What would you be looking for with the following Google query? `filetype:txt administrator:5`
    Text files including the text 'administrator:500:'

3.1.1 Long Answer

1. What is footprinting. What information can be gathered using the footpringing process?
2. Describe types of footprinting, with examples.
3. Write on "Offline website downloading and analyzing" - Tools / utilities available and in use.
4. How Google hacking can be useful for footprinting process.
5. Write at lease 3 examples of Operators / Queries within google hacking.
6. Write on Tools / utilities / websites useful for gathering PII of target people, with example.