Vulnerability Assessment and Mitigating Attacks

Learning Objective

After studying this chapter, you should be able to:

- Understand the meaning and the importance of vulnerability assessment and penetration testing.
- Understand the vulnerability assessment methods.
- Understanding the security testing methodology and be aware of some tools that are used in testing.
- Recognize some security technologies that help in vulnerability assessment and mitigating attacks.

1.Introduction

Let us imagine you set up a network infrastructure with all its software and hardware resources configured. You are fully aware that it is not a good strategy to wait until the weaknesses of your network are exploited, the intruders get inside, steal the sensitive information stored on your servers, encrypt your databases, and only then to turn to cyber security services, saying "We have a problem". In this respect, vulnerability assessment becomes a must-do for your network.

Vulnerability assessment is responsible for highlighting security weaknesses in computer systems, applications (web, mobile, etc.), and network infrastructures. It offers an organization a clearer understanding of their network environment and provides the information on the security flaws in it. The primary goal of network vulnerability assessment is to reduce the probability that cybercriminals will find the weaknesses in your network and exploit them. One of the most common uses for vulnerability assessments is their capability to validate security measures. We will show that it is easier to prevent the problem from occurring than cope with its consequences later.

The tasks of vulnerability assessment are the following:

- Identification, quantification and ranking of vulnerabilities found in network infrastructure, software and hardware systems, and applications.
- Explaining the consequences of a hypothetical scenario of the discovered security ‘holes’.
- Developing a strategy to tackle the discovered threats.
- Providing recommendations to improve a company’s security posture and help eliminate security risks.

2.Vulnerability Assessments and Penetration Testing

Vulnerability assessment and penetration testing (or pen test) are complementary techniques. A vulnerability assessment only identifies the potential vulnerabilities whereas a pen test tries to gain access to the network. Vulnerability assessment and pen testing are not the equivalents to each other. Although both of them can be black box, white box or grey box (as we will see in next section), there are significant differences between these two processes. For example, while vulnerability assessment focuses on uncovering as many security weaknesses as possible, pen test means trying to get inside the network as deep as possible ("the depth over breadth approach"). An example of a vulnerability assessment is looking at a door and thinking if that door is unlocked it could allow someone to gain unauthorized access, whereas a pen test tries to open the door to see where it leads.

A pen test is usually a better indication of the weaknesses of the network or systems but is more invasive and therefore has more potential to cause disruption to network service. Network vulnerability assessment is usually followed by pen testing. There's no use in conducting pen testing before the discovered vulnerabilities are patched, as the goal of pen testing is not just trying to get into the network but also examining the network environment 'with a new set of eyes' after the improvements are made.

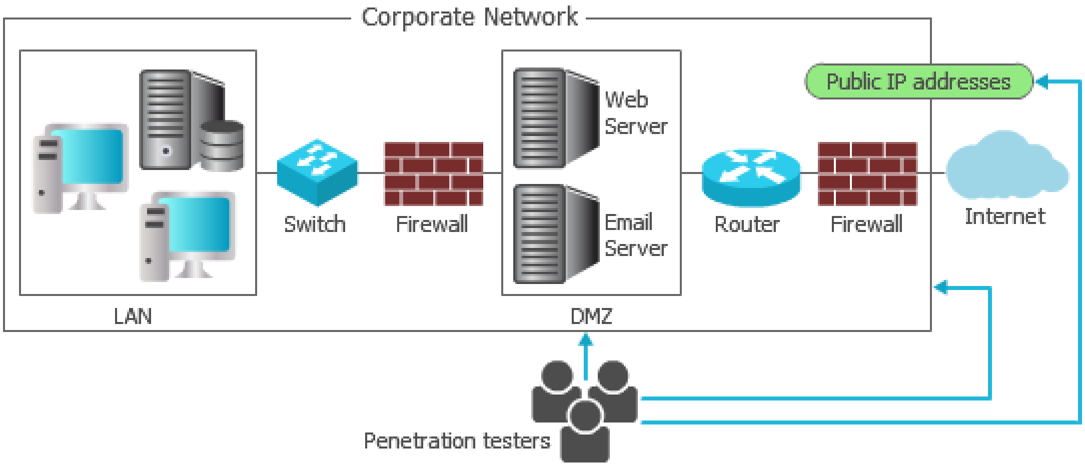
Keep in mind that the only difference between true "hacking" and pen testing is permission. For this reason pen testing is called ethical hacking. It is critical that a person performing a pen test get written consent to perform the testing.

3.Ways to Reveal Network Vulnerabilities

Vulnerability assessment can be conducted according to the white box, black box and gray box methodologies.

Black Box Method

The main task a cyber-security team needs to do when performing black box network vulnerability assessment is to act like real hackers. According to this method, the security team tries to find ways to get into the company's network 'from the outside. What can they see in this case? Public IP addresses, the external interface of a firewall, systems located in the demilitarized zone (DMZ), etc. No administrator privileges, no access to databases are provided to the ethical hackers.



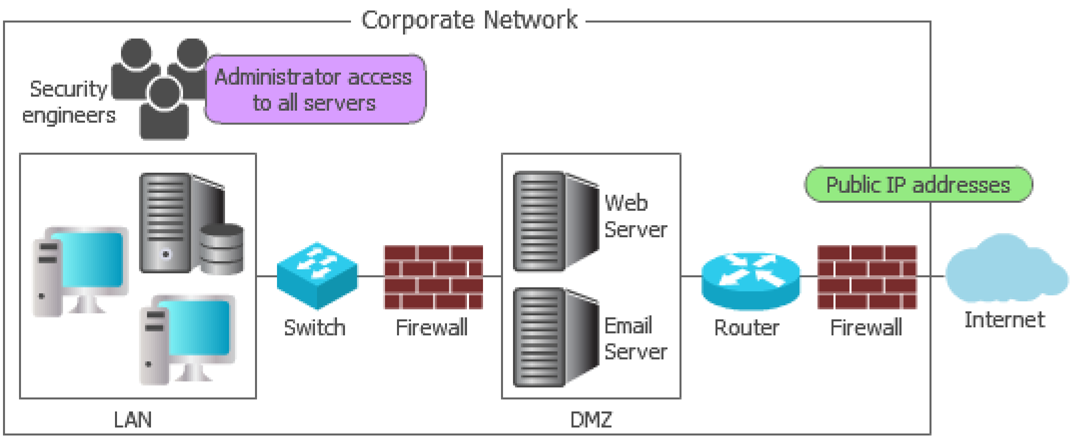
Figure(9.1): Black Box Method

White Box Method

If the cyber security team is to perform white box network vulnerability assessment, they look at the network 'from the inside', having all the privileges of the network authorized users. They can see the entire network with its file servers, databases. The security engineers have administrator access to all the servers inside the network. Their aim is not just to scan the network for vulnerabilities, but also check the security of the configuration of the machines inside the network.

Gray Box Method

In gray box network vulnerability assessment that encompasses both approaches but is closer to black box vulnerability assessment. Security engineers conduct gray box vulnerability assessment if they get some information on the organization's network, such as user login details, but they do not get access to the entire network.



Figure(9.2): White Box Method

There are pros and cons in each approach. In most organizations, there are more internal resources than those seen ‘from the outside’. When performing network vulnerability assessment by ‘looking around from the inside’, ethical hackers have a wider scope for action. However, opting for this approach only, without combining it with black box vulnerability assessment, there will be no possibility to find out which network weaknesses intruders may exploit to get into it.

4.A Scenario of Network Vulnerability Assessment

To get a clearer understanding of the vulnerability assessment process, let us consider its stages performed by a cyber-security team on the basis of the existing case of conducting network vulnerability assessment for a company.

Step 1. Planning and Defining the Scope

The cyber security team identifies the way business processes is carried out in the organization and agree with the customer on the assessment objectives, the scope of work. The organization needs to detect security issues and execute remedial actions. So, the security engineers are tasked with performing vulnerability assessment for the organization’s internal sub networks.

Step 2. Gathering Information on the Network Infrastructure

The security team gathers information about hardware and software present in the network environment. More specifically, the team defines whether the network has open ports or services that should not be opened, gets the understanding of the software and drivers configurations, and learns whether the logs from the network services are sent to a security information and event management solution. They also identify virtual and physical servers, as well as the security measures that are already in place, such as firewalls and intrusion detection and prevention systems (IPS/IDS).

Such "footprinting" of the network is carried out with the use of automated tools, such as Nmap, a network analysis tool. It allows to discover the web server version, check the servers to make sure that their ports are operating properly, ping network segments. Thus, the security team scans target sub networks to fingerprint running services and operating systems. For that, they send requests to the hosts (computers or virtual machines) being scanned and analyze their responses.

Step 3. Scanning, Detection and Assessment of Network Vulnerabilities

Vulnerability scanning is an automated process of proactively identifying network, application, and security vulnerabilities. Vulnerability scanning is typically performed by the IT department of an organization or a third-party security service provider. This scan is also performed by attackers who try to find points of entry into your network.

The scanning process includes detecting and classifying system weaknesses in networks, communications equipment, and computers. In addition to identifying security holes, the vulnerability scans also predict how effective countermeasures are in case of a threat or attack.

A vulnerability scanning service uses piece of software running from the standpoint of the person or organization inspecting the attack surface in question. The vulnerability scanner uses a database to compare details about the target attack surface. The database references known flaws, coding bugs, packet construction anomalies, default configurations, and potential paths to sensitive data that can be exploited by attackers.

Step 4. Reporting the Final Results and Identifying Countermeasures

The security engineers discover a number of vulnerabilities in the organization's sub networks that could potentially lead to the disclosure of sensitive information and financial losses and affect the organization's business reputation. The security team provides the organization with a report containing the list of vulnerabilities, mentioning their severity level (low, medium or high) and defining corrective measures to reduce risks. The security engineers pay the customer's attention to the critical ones that need to be fixed on a first-priority basis.

5.Understanding the Security Testing Methodology

We can use any of the following techniques to conduct ethical hacking. These ethical hacking steps are not always followed in the same order and might involve some iteration as well. Each step generates useful information about the target systems that support the successful execution of subsequent steps.

1. Reconnaissance: Testers perform general research, such as Internet searches, to reveal information useful to attackers, such as equipment types, uniform resource locators (URLs), usernames, domain names, IP addresses, e-mail addresses, and vulnerable servers (for example, from Google). Social engineering is a powerful reconnaissance technique, but it is rarely authorized for use by security testers in practice.
2. Network and Port Scanning: Testers use network scanning tools (primarily "nmap") to discover active hosts, their open ports, and likely network services.
3. Policy Scanning: Testers conduct policy scans, comparing system and application configurations with best practice benchmarks for security hardening.
4. Vulnerability Probes and Fingerprinting: Testers use vulnerability scanners to perform local and network probes, such as Nessus, nmap, and OpenVas, to discover potential vulnerabilities.
5. Penetration: Testers gain access to systems, networks, websites, databases, and wireless systems to be able to execute commands and attack code inside the systems. Some key tools for penetration include Metasploit, CORE Impact, and Canvas.
6. Enumeration and Cracking: This steps involves harvesting user lists and using sniffing, brute-force, and decryption techniques to gain access credentials.
7. Escalation: The tester obtains administrative privileges on systems.
8. Backdoors and Rootkits: This process involves establishing permanent access and control of a system while staying hidden from the system's owners.

9. Exfiltration and Abuse: The ultimate goal of the process when performed by hackers is to transmit information and damage systems for a variety of malicious motivations.

The preceding ethnical hacking steps are a general approach to penetration testing that is widely applied in practice. Many testing organizations stop at step 4 (vulnerability assessment) for various reasons, such as the subsequent steps have serious potential to damage systems, and the subsequent steps are not comprehensive tests, but rather more demonstrative of potential harm from latent vulnerabilities. Penetration testers generally stop at step 7, escalation.

In addition to this ethical hacking process, there are many alternatives available for security testers, for example, The Open Web Application Security Project method, the Open Source Security Testing Methodology Manual, and the Penetration Testing Framework.

The Open Web Application Security Project (OWASP) created a free, well-crafted method for web vulnerability assessment, which can be found at https://www.owasp.org. The OWASP Test Guide provides specific instructions on how to perform each test, and various OWASP tools are available to support the method.

The Open Source Security Testing Methodology Manual, which is available at www.osstmm.org, is a subscription-based method that attempts to cover all aspects of security, including physical, human, wireless, telecommunications, and networks. This is a relatively short manual for the breadth of material.

The Penetration Testing Framework (PTF) is a web-based resource that is essentially an extensive outline of testing techniques and links to download sites. You can find it at http://vulnerabilityassessment.co.uk. PTF contains seemingly exhaustive lists of thousands of free tools, commands, and Internet resources in fine-grain categories spanning IT security. For example, PTF has a lengthy list of user enumeration tools with sample command lines, lists of default passwords for numerous products, and port-by-port lists of services with tools and command lines for probes and exploits.

6.Intrusion Prevention Systems (IPS)

The intrusion prevention system (IPS), also known as intrusion detection and prevention system (IDPS), is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity. Like an IDS, an IPS can be host-based, network-based, as we discussed in Chapter 3. Similarly, it can use anomaly detection to identify behavior that is not that of legitimate users, or signature detection to identify known malicious behavior.

Once an IDS has detected malicious activity, it can respond by modifying or blocking network packets across a perimeter or into a host, or by modifying or blocking system calls by programs running on a host. Thus, a network IPS can block traffic, as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so.

Host-based IPS

A host-based IPS (HIPS) can make use of either signature or anomaly detection techniques to identify attacks. In the former case, the focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious. In the case of anomaly detection, the IPS is looking for behavior patterns that indicate malware. Examples of the types of malicious behavior addressed by a HIPS include the following:

- Modification of system resources: Rootkits, Trojan horses, and backdoors operate by changing system resources, such as libraries, directories, registry settings, and user accounts.
- Privilege-escalation exploits: These attacks attempt to give ordinary users root access.
- Buffer-overflow exploits.
- Access to e-mail contact list: Many worms spread by mailing a copy of themselves to addresses in the local system's e-mail address book.
- Directory traversal: A directory traversal vulnerability in a Web server allows the hacker to access files outside the range of what a server application user would normally need to access.

The HIPS capability can be tailored to the specific platform. A set of general-purpose tools may be used for a desktop or server system. Some HIPS packages are designed to protect specific types of servers, such as Web servers and database servers. In this case, the HIPS looks for particular application attacks.

In addition to signature and anomaly-detection techniques, a HIPS can use a sandbox approach. Sandboxes are especially suited to mobile code, such as Java applets and scripting languages. The HIPS quarantines such code in an isolated system area, then runs the code and monitors its behavior. If the code violates predefined policies or matches predefined behavior signatures, it is halted and prevented from executing in the normal system environment.

HIPS typically offers the following desktop protection:

- System calls: The kernel controls access to system resources such as memory.
- I/O devices, and processor. To use these resources, user applications invoke system calls to the kernel. Any exploit code will execute at least one system call. The HIPS can be configured to examine each system call for malicious characteristics.
- File system access: The HIPS can ensure that file access system calls are not malicious and meet established policy.
- System registry settings: The registry maintains persistent configuration information about programs and is often maliciously modified to extend the life of an exploit. The HIPS can ensure that the system registry maintains its integrity.
- Host input/output: I/O communications, whether local or network-based, can propagate exploit code and malware. The HIPS can examine and enforce proper client interaction with the network and its interaction with other devices.

Network–based IPS

A network–based IPS (NIPS) is in essence an inline NIDS with the authority to modify or discard packets and tear down TCP connections. As with a NIDS, a NIPS makes use of techniques such as signature detection and anomaly detection. Among the techniques used in a NIPS but not commonly found in a firewall is flow data protection. This requires that the application payload in a sequence of packets be reassembled. The IPS device applies filters to the full content of the flow every time a new packet for the flow arrives. When a flow is determined to be malicious, the latest and all subsequent packets belonging to the suspect flow are dropped.

In terms of the general methods used by a NIPS device to identify malicious packets, the following are typical:

- Pattern matching: Scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks.
- Stateful matching: Scans for attack signatures in the context of a traffic stream rather than individual packets.
- Protocol anomaly: Looks for deviation from standards set forth in RFCs.
- Traffic anomaly: Watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network.
- Statistical anomaly: Develops baselines of normal traffic activity and throughput, and alerts on deviations from those baselines.

Distributed or Hybrid IPS

The final category of IPS is in a distributed or hybrid approach. This gathers data from a large number of host and network–based sensors, relays this intelligence to a central analysis system able to correlate, and analyze the data, which can then return updated signatures and behavior patterns to enable all of the coordinated systems to respond and defend against malicious behavior. A number of such systems have been proposed. One of the best known is the digital immune system that was proposed by IBM and Symantec.

7.Honeypots

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems. Honeypots are designed to:

- Divert an attacker from accessing critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect. The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities. Because any attack against the honeypot is made to seem successful, administrators have time to mobilize and log and track the attacker without ever exposing productive systems.

The honeypot is a resource that has no production value. There is no legitimate reason for anyone outside the network to interact with a honeypot. Thus, any attempt to communicate with the system is most likely a probe, scan, or attack.

Conversely, if a honeypot initiates outbound communication, the system has probably been compromised.

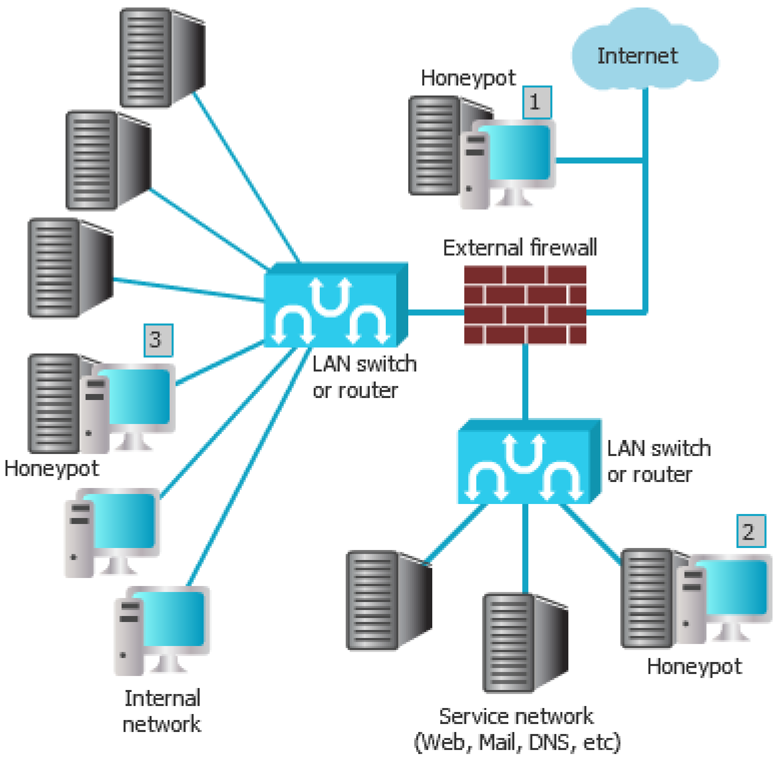
Initial efforts involved a single honeypot computer with IP addresses designed to attract hackers. More recent research has focused on building entire honeypot networks (i.e. honeynet) that emulate an enterprise, possibly with actual or simulated traffic and data. Once hackers are within the network, administrators can observe their behavior in detail and figure out defenses.

Honeypots can be deployed in a variety of locations. Figure(9.3) illustrates some possibilities. The location depends on a number of factors, such as the type of information the organization is interested in gathering and the level of risk that organizations can tolerate to obtain the maximum amount of data.

Location 1: A honeypot outside the external firewall is useful for tracking attempts to connect to unused IP addresses within the scope of the network. A honeypot at this location does not increase the risk for the internal network. The danger of having a compromised system behind the firewall is avoided. Further, because the honeypot attracts many potential attacks, it reduces the alerts issued by the firewall and by internal IDS sensors, easing the management burden. The disadvantage of an external honeypot is that it has little or no ability to trap internal attackers, especially if the external firewall filters traffic in both directions.

Location 2: The DMZ (demilitarized zone), is another candidate for locating a honeypot. The security administrator must assure that the other systems in the DMZ are secure against any activity generated by the honeypot. A disadvantage of this location is that a typical DMZ is not fully accessible, and the firewall typically blocks traffic to the DMZ that attempts to access unneeded services. Thus, the firewall either has to open up the traffic beyond what is permissible, which is risky, or limit the effectiveness of the honeypot.

Location 3: A fully internal honeypot has several advantages. Its most important advantage is that it can catch internal attacks. A honeypot at this location can also detect a misconfigured firewall that forwards impermissible traffic from the Internet to the internal network. There are several disadvantages. The most serious of these is if the honeypot is compromised so that it can attack other internal systems. Any further traffic from the Internet to the attacker is not blocked by the firewall because it is regarded as traffic to the honeypot only. Another difficulty for this honeypot location is that, as with location 2, the firewall must adjust its filtering to allow traffic to the honeypot, thus complicating firewall configuration and potentially compromising the internal network.



Figure(9.3): Honeypot Deployment Options

Exercises:

Multiple Choice Questions

1. What is the purpose of a pen test?

   A. To simulate methods that intruders take to gain escalated privileges

   B. To see if you can get confidential network data

   C. To test the security posture and policies and procedures of an organization

   D. To get passwords

2. Security assessment categories include which of the following? (Choose all that apply).

   A. White-hat assessments

   B. Vulnerability assessments

   C. Penetration testing

   D. Security audits

   E. Black-hat assessments

3. What type of testing is the best option for an organization that can benefit from the experience of a security professional?

   A. Automated testing tools

   B. White-hat and black-hat testing

   C. Manual testing

   D. Automated testing

4. What is the objective of ethical hacking from the hacker's prospective?

   A. Determine the security posture of the organization

   B. Find and penetrate invalid parameters

   C. Find and steal available system resources

   D. Leave marks on the network to prove they gained access

5. What is the first step of a pen test?

   A. Create a map of the network by scanning

   B. Locate the remote access connections to the network

   C. Sign a scope of work, and liability release document with the client

   D. Perform a physical security audit to ensure the physical site is secure

6. Which tools are not essential in a pen tester's toolbox?

   A. Password crackers

   B. Port scanning tools

   C. Vulnerability scanning tools

   D. Web testing tools

   E. Database assessment tools

   F. None of the above

7. An assessment report for management may include which of the following? (Choose all that apply).

   A. Suggested fixes or corrective measures

   B. Names of persons responsible for security

   C. Extensive step by step countermeasures

   D. Findings of the penetration test

8. What makes penetration testing different from hacking?

   A. The tools in use

   B. The location of the attack

   C. Permission from the owner

   D. Malicious intent

9. ___________ are attacks that attempt to give ordinary users root access.

   A. Privilege-escalation exploits

   B. Directory transversals

   C. File system access

   D. Modification of system resources

10. __________ scans for attack signatures in the context of a traffic stream rather than individual packets.

A. Pattern matching

B. Protocol anomaly

C. Traffic anomaly

D. Stateful matching

11. __________ looks for deviation from standards set forth in RFCs.

A. Statistical anomaly

B. Protocol anomaly

C. Pattern matching

D. Traffic anomaly

12. _________ matching scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks.

A. Pattern matching

B. Protocol anomaly

C. Traffic anomaly

D. Stateful matching

13. __________ anomaly watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network.

A. Pattern matching

B. Protocol anomaly

C. Traffic anomaly

D. Stateful matching

14. How does an IPS differ from an IDS?

A. An IPS detects network attacks, but doesn't issue alerts

B. An IPS detects network attacks and issues alerts

C. An IPS responds to network attacks by blocking traffic and resetting connections

D. An IPS sits inline and monitors traffic

15. What primary advantage does an IPS offer over IDS that makes it a crucial component of a security strategy?

A. The amount of logs generated

B. The speed at which attacks can be mitigated

C. The lower price tag

D. A reduced quantity of false positives

16. Something set up on a separate network (or in DMZ) to attract hackers and lure them away from the real network, it logs keystrokes, provides other information about an attacker.

A. Proxy Server

B. State Table

C. Evasion

D. Honeypot

17. In order to help prevent spam, a honeypot performs which of the following functions?

A. Acts as a desirable mail server in order to lure spammers

B. Delivers suspected spam messages more slowly

C. Traps suspected spam messages

D. Routes suspected spam to special enclaves in the system

18. Which of the following is a system designed to attract and identify hackers?

A. Honeypot

B. Firewall

C. Honeytrap

D. IDS

19. A form of software virtualization that lets programs and processes run in their own isolated virtual environment:

A. Rim lock

B. Mortise lock

C. Cipher lock

D. Sandboxing

References

1. Graves, K.: CEH: Certified Ethical Hacker Study Guide, Wiley Publishing Inc. 2006.
2. Stallings, W.: Network Security essentials: application and standards, 6th edn. Pearson India Education Services Pvt. LTD (2017).
3. https://www.scnsoft.com/blog/network-vulnerability-assessment-guide.

Number of the Question	Answer
1	C
2	B,C,D
3	C
4	A
5	C
6	F
7	A,D
8	C
9	A
10	D
11	B
12	A
13	C
14	C
15	B
16	D
17	A
18	A
19	C
20	D