Fundamentals of Security in Ethical Hacking

DCS22104

Lesson 11: Evading IDS, firewalls, and honeypots

Department of Computing

Course outline

Week	Topic
1	Introduction to ethical hacking and reconnaissance
2	Network enumerators and system vulnerabilities
3	Malware
4	Social engineering attacks
5	Hacking web servers and web applications
6	Session hijacking
7	Script injections
8	Hacking wireless network
9	Buffer overflow attacks
10	Cryptography
11	Evading IDS, firewall, and honeypot
12	Penetration testing

Assessments

#	Components	Marks(%)	Week
1	Test 1 (Topics 1 to 5)	10	DONE
2	Midterm examination	20	DONE
3	Test 2 (Topics 1 to 11)	20	12
4	Final examination	50	Exam week

Reviews on Lesson 9

- DoS a denial of service attack, where user could not perform normal tasks in a computer.
- Smurf attack: Broadcast ping request to a network, servers in the network will relay, and ping replies to the target server.
- Ping of death: Flood incoming ping request and outgoing ping replies will going to malicious party server.
- SYN flood: Send SYN requests to target server which exceeded the number of SYN-received, end up response only to malicious party.
- Others: Echo chargen, teardrop, DNS attack, and DDoS attack.

Reviews on Lesson 9

- Intrusion detection system.
- Components of an IDS are anomaly, audit, profiling, intrusion, and misuse.
- Four modes of operations for an IDS involved:
- Signature-based: Detect know type of attacks. But unknown signatures will not be detected.
- Anomaly-based: Only allow permitted behaviour in a system.
- Heuristic-based: It constructs model of a normal system behaviour.
- Hybrid: a combination of three operations of IDS.

Topic learning outcomes

1. Describe the role of cryptography in information security.

2. Identify the major types of cryptographic algorithms and typical applications.

3. Describe how digital signatures are performed and the role of digital certificates.

Reviews on Lesson 10

Vulnerabilities for a password.

- ✓Brute force attack possible, which consisted of trials and errors to crack the password.
- ✓Common passwords, malicious party can easily guess.
- ✓Social engineering attack where malicious party could ask the user for their password.
- ✓Weak password which does not contain the combination of alphabets, numbers, and special characters.
- ✓Input key logging.
- ✓Search for system password file.

Reviews on Lesson 10

The requirements for a strong password?

✓It must have at least 8 characters long.

✓It must include numbers, alphabets, and symbols.

Topic learning outcomes

1. Explain the role of firewall in a computer network.

2. Explain the mechanism of an intrusion detection system (IDS).

Lesson 11: Lecture and lab session

Start time	End time	Topics
1:00pm	1:30pm	Reviews on Lesson 10
1:30pm	2:00pm	Lecture 1: **Purposes of computer network and firewalls**
2:00pm	2:15pm	Break time
2:15pm	2:45pm	Lecture 2: **Honeypots**
2:45pm	2:50pm	References

Lecture 1
Purposes of computer network and firewalls

Terminology

Terms	Descriptions
Node	A single conceptual computing device connected to the network (Server).
Host	An actual physical computing device involved in a node.
Link	A connection between two hosts.

Advantages of a computer network

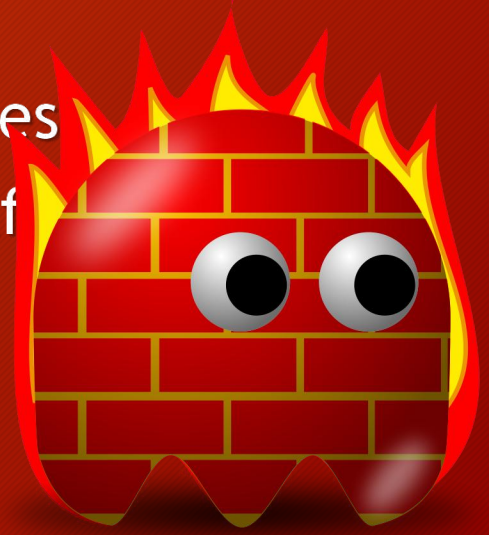
- Resource sharing
- Distribution of workload
- Increased reliability
- Expandability
- Scalability

Network vulnerabilities

- Anonymity
- Many points of attacks
- Resource and workload sharing
- System complexity
- Unknown boundary

Firewall

- It is a network security system.
- It lies on transport and network layers.
- It prevents unauthorized outside users from accessing a network or workstation.
- Set security policies and permissions.
- Set proxy to deny access, while allow certain computers to acces
- It allows individual to inspect inbound or outbound network traf



Packet filters

- It is a first generation firewall created in year 1988.
- It inspects data packets (TCP or UDP) between computers on the Internet.
- If a packet does not match a set of rules, packet filter will drop or reject the packet.
- Also, it will send error responses to the source.

Stateful filters

- It also refers to circuit-level gateways.
- The second generation firewall.
- It records all connections and classifies the states into
  - (a) new connection,
  - (b) part of existing connection,
  - (c) not part of any connection.
- The fake connection packets will be denied from entering the layer 4 (Transport layer).

Application layer

- A third generation firewall.
- It is a firewall toolkit.
- It recognizes FTP, DNS and HTTP protocols.
- It detects unwanted services in those protocols.

Exercise 1 (10 minutes)

1. State two purposes of a firewall.

2. State two vulnerabilities for a computer network.

Break time

Duration: 15 minutes.

Lecture 2: Honeypot

Honeypot

- A tool to learn from the attacks.
- Honeypot architecture is designed to trap attackers.
- Early detection and prevention.
- Learn motives from attackers.

Exercise 2 (10 minutes)

1. What is the first generation firewall?
2. What is the second generation firewall?
3. What is the third generation firewall?
4. State two purposes of a honeypot.

References

- CEHv11 course materials, EC-Council.
- Ethan, T (2019). Kali Linux: Simple and Effective Approach to Learn Kali Linux. Independently published.
- Jason, K (2019). Kali Linux: A Comprehensive Step by Step Beginner's Guide to Learn the Basics of Cybersecurity and Ethical Computer Hacking, Including Wireless Penetration Testing Tools to Secure Your Network. Independently published.