JINNAH UNIVERSITY FOR WOMEN

Department of Computer Science & Software Engineering

Information Security CSS 4292

Assignment 2

**Instructions:**

* The assignment must be submitted on JUW LMS. Email submission will not be accepted.
* Each student should solve the assignment individually.
* You are advised to go through the related topics before solving the assignment.
* Make your work clear and understandable.
* Plagiarism may lead to marks deduction.
* Use references where necessary.

**Question No.1**

1. How is an application layer firewall different from a packet-filtering firewall? Why an application layer firewall is sometimes called a proxy server?

|  |  |
| --- | --- |
| **Application Layer Firewall** | **Packet-Filtering Firewall** |
| It works at Application layer. | It is implemented at Network layer. |
| Inspects header as well as payload or data. | Inspects source and destination IP address, port number and protocols to make decision about packets. |
| Comparatively slower because of processing overhead. | Simple security measures make it bit faster. |

**Application Layer Firewall as Proxy Server:**

A **proxy server** is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources (Wikipedia).

Application layer firewall, instead of providing direct connection between the protected-network to the one from which it is being protected, provides a checkpoint for data exchange. This way it resonates the concept of proxy, thus also called proxy server.

1. What is DMZ network? What types of systems would you expect to find on such networks? Illustrate with the help of network diagram.

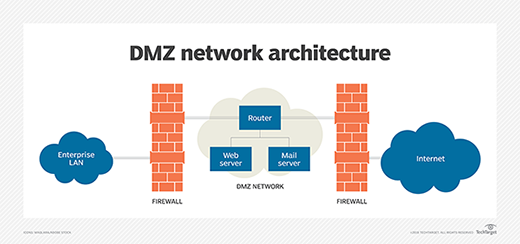


Figure 1: DMZ Network (source: techtarget)

**DeMilitarized Zone Network:**

It is a physical or logically partitioned network that provides an interface separating protected environment from untrusted external network (usually internet) while keeping internal or private network unexposed to threats.

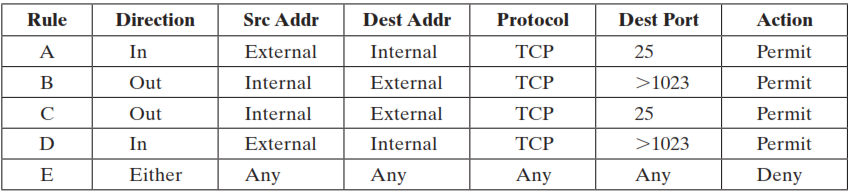
Enterprise LAN (protected resources) in Fig. 1 is separated with the help of a security gateway (firewall) from DeMilitarized Zone (outward interacting resources). This way there is least threat for protected network for being compromised through any outside attack.

**Types of Systems in DMZ:**

This zone includes all possible components that communicate with external environment such as users or hosts interacting with outside space or web servers and data servers, etc. Following are some of external-facing services and resources that are placed in DMZ network:

* File Transfer Protocol
* Mail Servers
* Proxy Servers
* Web Servers
* Domain Name Server (DNS)
* Voice over Internet Protocol (VoIP)

1. SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set. Describe the effect of each rule.



* Inward traffic from any external source for destination port 5 will be permitted.
* Outward response from destination port greater than 1023 will be permitted.
* Outward traffic from port 25 for any external destination is allowed.
* For any destination port above 1023, external response will be accepted.
* Rule E is default rule that discards all the traffic that does not fit the given set of rules i.e. A, B, C or D. It has by-default ‘deny’ policy for all.

**Question No.2**

1. Assume your organization is at high risk for malware-based attacks. Use the risk management steps discussed in lecture to convince your supervisor to support your request for funding to implement an employee training program to reduce malware infections”.

**Risk Identification**

This step is further divided into three smaller ones i.e.

*Identification of Inventory Assets:* All resources in the inventory, whether hardware or software, will be reviewed in order to evaluate the impact of attack i.e. malware based attack so that to go for prioritization of assets as well as risks.

*Classification and Prioritization of Assets:* This step will clear out what to protect foremost on critical basis i.e. most sensitive and paramount assets will be secured first and assets of lesser value or those that don’t need much protection will be handled afterwards.

*Identification and Prioritization of Threats:* Not only assets, threats too need to be prioritized i.e. which one to alleviate first. In this case, threats sabotaging the availability of services of organization will be mitigated first.

**Risk Assessment**

*Identify Vulnerabilities in Assets and Threats:*

This step includes mapping of vulnerabilities associated with threats. Here it will be examined how malware based attack can harm the assets. Assets, threats and their agents are prioritized to clear out the critical nature of action plan.

*Identification and Quantification of Assets Exposure:*

Here risk is determined and calculated on the basis of probability of threat attack (how likely it is that threat will harm asset), value of information asset, mitigation by current controls (how equipped organization is for said attack) and uncertainty of each threat. Quantitative Risk Assessment is also done to calculate Annualized Rate of Occurrence (ARO), Annual Loss Expectancy (ALE), etc.

**Risk Control**

* Here strategy to tackle risk is devised which is followed by justifying appropriate controls and then implementation of both.
* In case of Malware based attack, combination of predefined strategies i.e. defense and mitigation will be formulated to protect assets.
* This will be followed by planning for controls. Here in this case, as mentioned in the description, one of control would be training of personnel to reduce malware infection.
* Final step would be actual implementation of whole approach formulated in earlier steps**.**

1. As part of a formal risk assessment of the IT system of your university, you have identified the asset “integrity of stored file and database information of all the students and faculty stored on the server” and the threat “corruption, theft, loss of information from server.” Suggest reasonable values for the items in the risk register (given below) for this asset and threat with justifications for your choice.

|  |  |
| --- | --- |
| **Asset** | Integrity of stored file and database information of all the students and faculty stored on the server |
| **Thread/ Vulnerability** | corruption, theft, loss of information from server |
| **Existing Controls** | Access Controls  (Files are accessible for defined authorized individuals only to protect data from unauthorized circulation)  File encryption |
| **Likelihood** | 0.2  (If access controls are defined and implemented efficiently then it’s unlikely that file will be modified or corrupted |
| **Consequences** | File exposure or unauthorized modification  (if any unauthorized person gains access then records and data can be modified) |
| **Level of Risk** | High  (loss of personal data in case of attack can have serious consequences) |
| **Risk Priority** | High |

1. Suppose ABC company owns an information asset X that has a value score of 60 and has one vulnerability. Vulnerability 1 has a likelihood of 1.0 with no current controls. Estimate shows that assumptions and data are 90 percent accurate. Evaluate the risk associated with asset X

**Risk Assessment:**

P: Probability of threat attack = 1

V: value score = 60

M: Mitigation by current controls = 0%

U: Uncertainty of vulnerability = 100 – 90 = 10%

R = P \* V – M + U

R = (1 \* 60) – 0 + 10 =

(60 \* 1.0) – ((60 \* 1.0) \* 0.0) + ((60 \* 1.0) \* 0.1)

60 – 0 + 6 = 66

**Question No.3**

ABC Company is worried about the misuses of the database components. Company’s manager is asking you to recommend an intrusion detection system to help identify misuses. Would you use anomaly-based or misuse-based intrusion detection? Justify your answer

Both methods have some positive and negative aspects. Although both are capable of resolving the issue, Anomaly-based Intrusion Detection seems better choice for the given scenario for following reasons:

* It uses deviations from normal usage patterns to identify intrusions or suspicious behavior. System is trained first to understand the normalized baseline and then compare activities against those definitions.
* It is efficient for detection of zero-day exploits as slightly deviated behavior from normalized one will trigger warnings and alarms.
* However, chances for false positives are higher in this method, which are less common in misuse based or signature based detection.

**Question No.4**

Your organization is offering a web-based application and worried about potential cyber-attacks where the attacker would supply specially crafted input to corrupt the application, such as SQL injection, buffer overflow. Discuss at least four different types of attacks and how would you address these attacks.

**SQL Injection Attack:**

Attackers inject malicious SQL scripts in web applications to gain access to backend or database. This attack is commonly carried out by inserting SQL queries in html forms fields.

SQL Injection attack can be avoided by restricting input to desired one i.e. by allowing user to enter valid strings only.

**Denial of Service Attack:**

This type of attack is intended to make system unavailable for legitimate users by requesting services and resources repeatedly. This type of attack has no benefit for attacker except the fact that victim’s services get affected.

These attacks appear as unsurmountable most of the times. Defensive responses to denial-of-service attacks typically involve the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate.

**Man-in-the-Middle Attack:**

In this type of attack, a third person intervenes the communication between two parties unlawfully and disguises as the other party. Session Hijacking is type of MitM attack in which attacker hijacks session between trusted client and network server. Similar approach is followed in Replay attacks where intruder intercepts and tries to gain trust on the basis of previously exchanged data.

Encryption and digital certifications are used to prevent this type of attacks as there is no single strategy effective enough to defend all Man-in-the-Middle attacks.

**Cross-site Scripting (XSS) Attack:**

Attackers inject payload with malicious JavaScript into website’s database in this attack. When victim requests infected page, that malicious script is transmitted as part of HTML body. This lets attackers easily steal cookies which can be exploited for session high jacking.

Data entry sanitization can help in preventing this type of attack.

**Question No.5**

Assume you are a midlevel systems administrator for one section of a larger organization. You try to encourage your users to have good password policies and regularly run password-cracking tools to check that those in use are not guessable. You have become aware of a burst of hacker password-cracking activity recently. In a burst of enthusiasm, you transfer the password files from a number of other sections of the organization and attempt to crack them. You find that in one section for which you used to work, something like 40% of the passwords are guessable (including that of the vice-president of the section, whose password is “president”!). You quietly sound out a few former colleagues and drop hints in the hope things might improve. A couple of weeks later you again transfer the password file over to analyze in the hope things have improved. They haven’t. Unfortunately, this time one of your colleague’s notices what you are doing. He notifies senior management, and that evening you find yourself being arrested on a charge of hacking and thrown out of a job. Did you do anything wrong? Briefly indicate what arguments you might use to defend your actions in the light of ethical behavior

The act of finding flaws in password was laudable and demand of job. However, carrying out job without going through proper channel and without following prescribed method is illegal act.

* Job responsibilities give job holder the excuse of finding out extent of vulnerabilities in the system.
* No harm was made even after knowing the password which makes clear that intentions behind the act were of benefit of organization.

**Question No.6**

* Security has become a major area of concern for every organization. Due to increase in cyber-crimes, organizations are now more vulnerable to security threats. One way to protect from these threats is to develop a strong security policy. You are required to develop any two organizational security policies (e.g. Password policy, Internet usage policy, software installation pol/icy, IT equipment usage policy etc.)

Policies are formulated with definition of overview, purpose and guidelines usually in accordance with the formats and standards accepted across industry. This definition may include legal terms depending upon the nature of policy.

**Password Policy:**

***Overview:*** Passwords are foremost protection for privacy of users which need to be as much secure as possible.

***Purpose:*** Establishment of criterion for strong passwords.

***Policy:***

Users will get suggestion of strong password while signing up.

Passwords can’t be reused.

Password must be changed after 90 days.

**Internet Usage Policy:**

***Overview:*** Onsite internet usage is need of employees which must be under specific criterion to prevent irreversible consequences.

***Purpose:*** Access to the Internet through company resources is a privilege but all employees must adhere to the policies concerning Computer, Email and Internet usage.

***Policy:***

Employees are expected to use internet responsibly for job accomplishment, not for personal use.

All usage is logged and is considered as official data.

Devices and equipment is property of organization and aren’t permitted to take outside premises until asked.