**FAITH SADERA**

**20-1015**

**ACS 251 ASSIGNMENT 2**

1. Distinguish between authorization and authentication in network security and how they are applied.

**Authorization is the process whereby a server checks and determines if a client has permission to access a resource or a file.**

**In Authorization, a server determines whether a user has access to a resource.**

**Authorization relies on the process of authentication so that the server can know who the user requesting access is.**

**Authentication is the process of verifying who a user/client is.**

**Authentication in network security is the process of verifying the identity of a user/client when that user logs into a computer system.**

**Authentication by a server requires the user to input username and password. Other methods of authentication include cards, voice recognition, fingerprints etc.**

**Authentication only identifies and verifies who the user is but does not determine which level of access to data and files an individual has.**

1. Discuss how Risk, Threats and Vulnerability affect network Security.

* **PRIVATE DATA LEAKING**

**Computer virus is an example of a security threat that can disable security settings, corrupt or steal data including personal information such as passwords. This means in case one computer in a network is infected, the entire network is vulnerable and sensitive data running through the network might leak or end up on unauthorized hands.**

* **MAKING REQUIRED INFROMATION INACCESSIBLE**

**DDoS (distributed denial-of-service) attack is one whereby an attacker attempts to make a resource unavailable to the intended users by indefinitely disrupting or suspending the services of its hosting server.**

* **MAKING THE NETWORK SLOW.**
* **MAKING THE NETWORK INOPERABLE**

1. Discuss Intrusion Detection in Network Security. Explain how the need of Web Security.

**An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.**

**An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance).**

**IDS was originally developed this way because at the time the depth of analysis required for intrusion detection could not be performed at a speed that could keep pace with components on the direct communications path of the network infrastructure.**

**As explained, the IDS is also a listen-only device. The IDS monitors traffic and reports its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device.**

**Explain the need of web security:**

**Web security means the protective protocols an organization/online network adopts to protect the network from attackers and threats that use the web channel.**

**Need of web security:**

* **It is critical to business continuity and data protection.**
* **Protecting websites from unauthorized access of resources.**
* **Deny possibility of an attacker to modify or destruct or disrupt the website.**

1. Discuss the various types of threats and attacks in Network Security?

* **Malware – This term is used to describe malicious software including viruses, ransomware and worms. Malware gets its way inside a network when a user clicks a dangerous link or email attachment that then it installs.**
  + - **Malware can:**
* **Deny access to key features of the network.**
* **Obtain information being transmitted through the network.**
* **Make the entire network inoperable.**
* **Phishing - The act of attackers sending corrupt communications that appear to be legitimate with an aim of obtaining sensitive data like credit card and login information.**
* **SQL injection**

**Sql injection happens when an attacker inputs malicious code into a server that uses SQL and tricks the server into revealing information it normally would not.**

* **DNS tunneling**

**This is a method of cyber-attack that encodes the data of a program in DNS queries and responses. It often includes data that can be added to a targeted server and used to control a remote server.**

* **Denial-of-service attack**

**This kind of attack floods the server /Network with heavy traffic to a point of exhausting resources. As a result, the system is unable to meet legit requests.**

1. Discuss based on the previous question, how these infiltrations can be prevented or averted.

* **Malware**
* **Keeping the network security software up to date.**
* **Avoid clicking suspicious links.**
* **Phishing**
* **Protecting your account using the multi-factor authentication.**
* **SQL injection**
* **Using parameterized statements where available.**
* **DNS tunneling**
* **A tool used to identify suspicious domains and IP addresses might be installed. DNS traffic that is sent to known malicious endpoints is blocked at the perimeter.**
* **Denial-of-service attack**
* **Use of firewalls and Intrusion Prevention Systems (IPS)**

1. Discuss the major challenges of a Network Security Administrator.

* **Poor network performance. There’s no question that poor network performance is a top challenge for network engineers. There isn’t simply more total traffic; there’s more traffic in all directions. Without the right equipment at endpoints and midpoints along the way, it’s impossible to provide the high-speed communication needed by today’s applications. Plus, performance isn’t just about speed; it’s about reliability, too. Network designs need to handle spikes in load and provide alternate routes to enable communication to continue even when a link fails. 24×7 online business requires 24×7 network availability.**
* **Security. Security is another top challenge. Because the perimeter of today’s network is unclear, blocking unauthorized outside traffic from the internal network isn’t adequate for protecting data. Many threats make it into the network when employees respond to a phishing email. Denial of service attacks only need to attempt connections to succeed. Encryption helps protect traffic, but encryption can also make it harder to monitor network activity. There are many tools that can be used to improve network security, but ensuring they work together and provide a comprehensive solution is difficult. In addition, multiple tools require increased monitoring and management.**
* **Configuration management. As networks increase in size, overseeing the network configuration increases in difficulty. Devices can conflict with each other. It becomes challenging to keep the rules in firewalls up to date, and manually applying policies leads to errors and inconsistencies.**
* **Cost. Available budget almost never meets the need for network services, especially when the network now needs to support not just traditional IT applications but also conventional business services like telephony (in the form of VoIP) and videoconferencing that require new levels of network quality.**
* **Growth. All the other challenges would be easier to address if the network would stay the same, but it doesn’t. There’s a constant increase in the number of devices attached to the network, with every additional connection an additional potential point of failure.**
* **Vendor lock-in. Yesterday’s reasonable decision means today your architecture is built around the assumptions and capabilities of yesterday’s vendor. Bringing in the best solutions from today’s vendors means figuring out how to interoperate, integrate, and support multiple solutions, or figuring out how to tear out all of the old equipment without tearing down the entire network at the same time.**