## Final Exam Essay Questions

Each short answer essay question is worth 10 points each.

NAME:

Natnael kebede

1. **Create the following 5 ACL rules by filling in the table below:**
   1. **Allow all HTTP traffic to a web server with an IP Address of 123.456.78.9**
   2. **Allow all HTTPS traffic to a web server with an IP Address of 123.456.78.9**
   3. **Allow all DNS queries to a DNS server with an IP Address of 987.654.32.1**
   4. **Deny all FTP transfers to an FTP server with an IP Address of 333.22.1.1**
   5. **Apply the standard “implicit default deny” rule to all traffic**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Rule** | **Protocol** | **Source IP** | **Source Port** | **Target IP** | **Target Port** | **Action** |
| **1** | TCP | ANY | ANY | 123.456.78.9 | 80 | Allow |
| **2** | TCP | ANY | ANY | 123.456.78.9 | 443 | Allow |
| **3** | UDP | ANY | ANY | 987.654.32.1 | 53 | Allow |
| **4** | TCP | ANY | ANY | 333.22.1.1 | 21 | Deny |
| **5** | TCP | ANY | ANY | ANY | ANY | Deny |

1. **Define “split-tunneling” as it relates to a standard VPN connection. Describe 2 benefits or advantages for allowing split-tunneling. Describe 2 security risks or disadvantages by allowing split-tunneling.**

Split tunneling is a configuration setting that allows a remote VPN user to simultaneously access both an untrustworthy network such as a home network or public network such as the internet, and a secured VPN network connection which allows the individual to access resources hosted on the VPN.

Two benefits or advantages that can occur by allowing split tunneling includes:

1. It reduces bottlenecks and conserves bandwidth since Internet traffic does not have to pass through the VPN server.
2. It enables strict separation of corporate Internet traffic and private Internet use.

On the other hand, two security risks or disadvantages that can occur by allowing split tunneling includes:

1) It provides an attacker access to an internal network from anywhere on the internet if the client machine gets compromised by a virus that permits remote control of the system by an attacker.

2) It potentially opens a door into a network that can’t be controlled. That is, it introduces Hairpinning, allowing malicious code to enter from a non-secure network making a hairpin or sharp turn and entering the secure network without any trouble by entering from a secure and verified endpoint.

1. **Identify and briefly describe 5 key differences between IPv4 and IPv6.**

Five key differences between IPv4 and IPv6 include:

1. Address Space: IPv4 address supports approximately 4.3 billon addresses with less than 10 percent of the total IPv4 address currently remaining. On the other hand, IPv6 provides an increased address space supporting 340 undecillion IP addresses for network devices.
2. Security: IPv6 protocol has solved some of the security problems found in IPv4 networks. One example of this scenario is the inclusion of IP Security (IPsec) in the IPv6 protocol to provide native information security framework, making it fundamentally more secure than the older IPv4 standard.
3. Management Requirements: IPv6 is a more robust protocol that requires less management. In contrast, IPv4 required a significant management due to new requirements after the introduction of the protocol.
4. Routing: The routing functionality of IPv6 has been enhanced by requiring fewer hops between network nodes, allowing multicast (Substantial packet streams sent to multiple destinations at the same time distributing loads and saving bandwidth), and smoother end-to-end functionality (the host generating part of the address to speed up the process) in comparison to IPv4.
5. Configuration of Hosts: By querying the local routers with multicast message, IPv6 permits hosts to automatically configure themselves when they connect to an IPv6 network. If this configuration mechanism isn’t supported for a specific environment or application, support is also available for an IPv6 version of DHCP all of it making it different when compared to IPv4.
6. **List and explain 5 different security controls to reduce the risk of a standard Denial of Service (DoS) attack against an Internet facing system.**

Five different security controls to reduce the risk of a standard Denial of Service (DoS) attack against an internet facing system is summarized in the table below.

|  |  |
| --- | --- |
| **List of Security Controls** | **Explanation of Security Controls** |
| 1. Firewalls | A firewall can detect and discard DoS by utilizing its filtering service to prevent the DoS traffic from breaching the network’s perimeter and affecting internal systems. |
| 1. In-Cloud Scrubbing Services | Given that most DoS attacks can be volumetric attacks, cloud scrubbing services inspect large volumes of traffic and remove malicious traffic before allowing it to enter corporate networks. As a result, they deliver a high degree of effectiveness with advanced mitigation and protection. |
| 1. Regular Patching | By regularly patching and infrastructure and installing new software versions, it is possible to close doors to attackers that utilized loopholes in outdated systems to launch DoS attacks. |
| 1. Security Awareness | Engaging in strong security practices can keep business networks from being compromised. Secure practices such as complex passwords that change on a regular basis, anti-phishing methods, and secure firewalls that allow little outside traffic all provide a critical security foundation. |
| 1. Security Checklists | Incorporate into a security checklist the assumption that you may become a victim of a DoS attack since every communication is vulnerable to such attack. This mechanism allows the maintenance of effective security overtime despite any change, accidents, and human nature. |

1. **List and explain 5 different security controls that should be implemented in order to secure guest wireless access to the Internet from inside a corporate office.**

Five different security controls that should be implemented to secure guest witless access to the internet from inside a corporate office is summarized in the table below.

|  |  |
| --- | --- |
| List of Security Controls | Explanation of Security Controls |
| 1. Access Controls | Only allow authorized individuals to access the guest network. Additionally, restrict access to the network by filtering devices based on their MAC address.  Furthermore, grant wireless access to guests on a separate wireless channel with a different password, while maintaining the privacy of your primary credentials. |
| 1. Encryption | Encrypt wireless data using encryption protocols such as Wireless Protected Access (WPA2 and WPA3) to prevent anyone who might be able to access your network from viewing it. |
| 1. Protect the Service Set Identifier (SSID) | Avoid publicizing the SSID. That is, Wi-Fi routers allow users to protect their device’s SSID, which makes it more difficult for attackers to find the network.  Additionally, change default SSID to avoid any potential attacker from identifying the type of router and possibly exploiting vulnerabilities. |
| 1. Firewall | Install a firewall directly on the wireless devices (a host-based firewall). That is, attackers who can directly tap into the wireless network may be able to circumvent the network firewall, but a host-based firewall will add a layer of protection to the data on the computer. |
| 1. Regular Patching | Keep your access point software patched and up to date. The manufacturer of the wireless access point will periodically release updates to and patches for a device’s software and firmware.  Be sure to check the manufacturer’s website regularly for any updates or patches for the device. |