**LAB PROGRESS REPORT NO. 4**

Name:  ERIC WEBB

Lab Progress Report Due Date: 06/09/19

Current Week Since Start Date: Week 5

Reporting Week:  06/03/19 to 06/09/19

**Progress achieved in reporting week 5:**

|  |
| --- |
| 4.1.1 Physical Security |
| 4.1.2 Tailgating and Piggybacking |
| 4.1.3 Physical Security Facts |
| 4.1.4 Implement Physical Security |
| 4.1.5 Practice Questions |
| 4.2.1 Hardware Security Guidelines |
| 4.2.2 Breaking into a System |
| 4.2.3 Hardware Security Facts |
| 4.2.4 Practice Questions |
| 4.3.1 Physical Network Protection |
| 4.3.2 Physical Network Protection Facts |
| 4.3.3 Practice Questions |
| 4.4.1 Environmental Controls |
| 4.4.2 Securing Environmental Systems |
| 4.4.3 Environmental Control Facts |
| 4.4.4 Fire Protection Facts |
| 4.4.5 Practice Questions |

**Progress not achieved in the reporting week that is needed to be addressed during the next reporting week:**

All progress was achieved.

**Progress expected to achieve in the next reporting period:**

|  |
| --- |
| 5.1.1 Reconnaissance |
| 5.1.2 Performing Reconnaissance |
| 5.1.3 Reconnaissance Facts |
| 5.1.4 Denial of Service. |
| 5.1.5 DoS Attack Facts |
| 5.1.6 UDP Flood Attack |
| 5.1.7 Practice Questions |
| 5.2.1 Session and Spoofing Attacks |
| 5.2.2 Session-Based Attack Facts |
| 5.2.3 Performing ARP Poisoning |
| 5.2.4 Spoofing Facts |
| 5.2.5 DNS Attacks |
| 5.2.6 DNS Attack Facts |
| 5.2.7 Examining DNS Attacks |
| 5.2.8 Prevent Zone Transfers |
| 5.2.9 Practice Questions |
| 5.3.1 Security Solutions |
| 5.3.2 Security Zones |
| 5.3.3 Security Zone Facts |
| 5.3.4 All-In-One Security Appliances |
| 5.3.5 Security Solution Facts |
| 5.3.6 Configuring Network Security Appliance Access |
| 5.3.7 Configure Network Security Appliance Access |
| 5.3.8 Practice Questions |
| 5.4.1 Demilitarized Zones |
| 5.4.2 Configuring a DMZ |
| 5.4.3 Configure a DMZ |
| 5.4.4 DMZ Facts |
| 5.4.5 Practice Questions |
| 5.5.1 Firewalls |
| 5.5.2 Firewall Facts |
| 5.5.3 Configuring a Perimeter Firewall |
| 5.5.4 Configure a Perimeter Firewall |
| 5.5.5 Practice Questions |
| 5.6.1 Network Address Translation |
| 5.6.2 Configuring NAT from the CLI |
| 5.6.3 Configuring NAT on an NSA |
| 5.6.4 NAT Facts |
| 5.6.5 Practice Questions |
| 5.7.1 Virtual Private Networks (VPNs) |
| 5.7.2 Configuring a VPN |
| 5.7.3 Configuring a VPN Client |
| 5.7.4 Configure a Remote Access VPN |
| 5.7.5 Configure a VPN Connection iPad |
| 5.7.6 VPN Facts |
| 5.7.7 VPN Protocol Facts |
| 5.7.8 Practice Questions |
| 5.8.1 Web Threat Protection |
| 5.8.2 Configuring Web Threat Protection |
| 5.8.3 Configure Web Threat Protection |
| 5.8.4 Web Threat Protection Facts |
| 5.8.5 Practice Questions |
| 5.9.1 Network Access Protection |
| 5.9.2 Implementing NAC with DHCP Enforcement |
| 5.9.3 NAP Facts |
| 5.9.4 Practice Questions |
| 5.10.1 Wireless Networking Overview |
| 5.10.2 Wireless Antenna Types |
| 5.10.3 Wireless Networking Facts |
| 5.10.4 Wireless Encryption |
| 5.10.5 Wireless Encryption Facts |
| 5.10.6 Configuring a Wireless Connection |
| 5.10.7 Configure a Wireless Network |
| 5.10.8 Practice Questions |
| 5.11.1 Wireless Attacks |
| 5.11.2 Wireless Attack Facts |
| 5.11.3 Using Wireless Attack Tools |
| 5.11.4 Detecting Rogue Hosts |
| 5.11.5 Configure Rogue Host Protection |
| 5.11.6 Practice Questions |
| 5.12.1 Wireless Security Considerations |
| 5.12.2 Wireless Authentication |
| 5.12.3 Wireless Authentication Facts |
| 5.12.4 Hardening a Wireless Access Point |
| 5.12.5 Harden a Wireless Network |
| 5.12.6 Configure WIPS |
| 5.12.7 Configuring a Captive Portal |
| 5.12.8 Wireless Security Facts |
| 5.12.9 Practice Questions |

