Kohl Johnson

CST-321

01-26-2025

Activity 7 Coversheet

# Applying Basic Security

**Part 1**

**A screenshot of a computer

Description automatically generated**

**Part 2**

**A screenshot of a computer

Description automatically generated**

**Part 3**

**A screenshot of a computer

Description automatically generated**

**Theory of Operation:** Did not convert it to a bash script. But, this is my first step.

**Part 4**

The first step to hardening a linux server would be to user a secure shell protocol (SSH) to enable a secure connection to our network services over an unsecured network. In addition to SSH, we could use IPTables to restrict access from known IPs only, used key-based authentication instead of password-based, and keep client keys encrypted to prevent their use in case of theft. We could also disable the Internet Control Message Protocol (ICMP) which allows internet hosts to notify other hosts about errors/issues to aid in troubleshooting. While this is a great tool, it can be exploited in the form of ping sweeps (used to identify all hosts on a network) and ping floods (involves sending ICMP messages in quick succession causing the exhaustion of bandwidth).

# Working with OpenSSL

**Step F Screenshot**

A screenshot of a computer

Description automatically generated

**Step I Screenshot**

**A screenshot of a computer

Description automatically generated**

**Step N Screenshot**

**A screenshot of a computer

Description automatically generated**

# Working with Network Utilities

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| **Command** | **Purpose** |
| Hostname | Finds the hostname of computer |
| Ifconfig -a | Lists all network interfaces |
| Netstat -a | Lists all open connections |
| Netstat -tnl | Check the listening connections |
| Sudo netstat -itpe | Get connections with process name/id and user id |
| Netstat -i | Prints network interfaces |

# Ethical Hacking

Some groups of hacking are Website, Network, Email, Password, Computer, and Ethical Hacking. Website hacking involves taking unauthorized control over a web server and/or associated software like databases and interfaces. Network hacking covers the gathering of information about a network using tools like TelNet, NS Lookup, Ping, Tracert, Netstat, and others with the sole intention of harming the network and disabling its operation. Email hacking includes unauthorized access to an email account without first getting the consent of the owner. Password hacking involves the same but is more centered around recovering secret passwords from data that is stored or transmitted from a computer system. Computer hacking relates to the stealing of a computers ID and password and getting unauthorized access to the said computer. Ethical hacking relates to the finding of weaknesses in a system with the sole goal of providing a fix and increasing the overall security of a said system.