Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By:Mohammed Abde

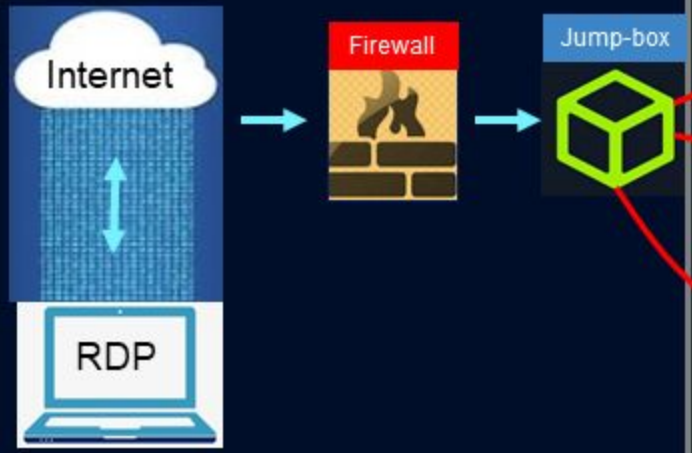
Table of Contents

This document contains the following sections:

Network Topology

Network

IP Range: 192.168.1.0/16
Broadcast: 192.168.1.255
Gateway: 192.168.1.1



VM-Capstone
192.168.1.105
OS: Windows
Victim server

VM-ELK
192.168.1.100
OS: Linux
Log/Attack monitoring

VM-Kali
192.168.1.8
OS: Linux
Hacker's machine

Hyper-V

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	Monitors network and collects logs to be analyzed using Kibana
Capstone	192.168.1.105	Victim Machine
KALI	192.168.90	Attacker Machine
HYPER-V-Manager	192.168.1.1	Virtuals machines used to attack, defend, monitor activity.