Operation Diamondhouse

Technical Guide

FOR AUTHORIZED PERSONNEL ONLY

TABLE OF CONTENTS

-

NETWORK INFORMATION

FOB Bravo has a broad network for various operations, but the majority of its computers draw their security configurations from two machines: **PC1** and **PC2**.

PC1 has an IPv4 address of 10.0.0.1. It is the computer that you have direct access to.

PC2 has an IPv4 address of 10.0.0.2. It is the computer that you will have to SSH into, as it does not have a graphical interface to work with.

On both of these computers, a user called **cyberops** has been configured. The password for it is **BestCode123!**. Use this when logging in or using SSH.

For security reasons, these two computers are not directly connected to the Internet. They are, however, connected to each other and to other computers on the local network, which could leave them vulnerable if an attacker gains access to any of those devices.

SSH

The **ssh** command in Linux is used to manage remote systems. Using it will give you a command line terminal as if you were physically accessing the machine. Included below are basic instructions for its usage.

1. To use SSH, the command must be told which machine to access. This should be done through an **IPv4 address**.
    a. **Note:** There are also IPv6 addresses used with modern technologies like 5G wireless networks for cell phones, but the computers in FOB Bravo do not use them.
    b. An IPv4 address typically takes the form of four numbers separated by bullet points, each between 0-255. An example would be **8.8.8.8**, a well-known Google server on the Internet.
2. When accessing a machine, SSH must also be told which user it will be logging in as.
3. The final format of an SSH command, with both an IPv4 address and a user, is as follows:
    a. ssh user@IPv4Address
    b. EXAMPLE: **ssh user1@127.21.30.244**
4. SSH will then prompt you for a password. However, for security purposes, SSH will not spell out the password on the screen as you type it. Write the password normally, then hit Enter. If the username and password are correct, you will be given access to the computer.

IPTABLES

The **iptables** software is a firewall that is used on Linux computers. All traffic that goes into and out of these computers will be checked by the firewall. If they do not match any of the rules, they will be allowed through by default. However, if they do match one of the rules, then that traffic will be accepted or dropped, depending on the rule. Included below are basic instructions on its usage:

1. The iptables command requires elevated permissions to use. BEFORE every iptables command, you must write **sudo** to indicate that you wish to run the command with these elevated permissions.
2. When writing an iptables rule, you must ALWAYS identify two things: the direction, and the action.
    a. The direction is which way the traffic is going. In an iptables rule, these are written as **INPUT** (going into the computer) and **OUTPUT** (going out of the computer).
    b. The action tells iptables what to do if a piece of traffic matches the rule. It can either **ACCEPT** the traffic and let it continue, or **DROP** the traffic and not allow it to pass.
3. There are many ways an iptables rule can be written. Here, you only need to know two of them: **filtering ports**, and **filtering IP addresses**. Write them exactly as you read them, all as one line, but do NOT include the brackets.
    a. To filter a port, you must identify a port number. Key differences between input and output are underlined.

sudo iptables -A INPUT -p tcp <u>--dport</u> [port number] -m conntrack --ctstate <u>NEW,ESTABLISHED</u> -j [ACCEPT/DROP]

sudo iptables -A OUTPUT -p tcp <u>--sport</u> [port number] -m conntrack --ctstate <u>ESTABLISHED</u> -j [ACCEPT/DROP]

b. To filter an IP address, you must identify the IP address.

sudo iptables -A [INPUT/OUTPUT] -s [IP address] -j [ACCEPT/DROP]

i. **Note:** IPv4 addresses are used by **iptables**. IPv6 addresses are used by **ip6tables**. If you need to filter an IPv6 address, write the command as normal but change “iptables” to “ip6tables”.

sudo ip6tables -A [INPUT/OUTPUT] -s [IPv6 address] -j [ACCEPT/DROP]

4. To see what rules you have written, use the following command:

sudo [iptables/ip6tables] -L

NMAP

The nmap software is a tool that is used to analyze networks. In the scope of Operation Diamondhouse, it will be used as the method of verifying whether or not firewall rules are working. Included below are basic instructions on its usage:

1. To use nmap to scan individual ports, use the following format:

nmap -p [port number] [IP address]

2. When the command is complete, the command will print output that tells you whether or not the firewall rules are working as you intended. Simply look under the STATE column to tell you what is happening.
    a. If they are dropping traffic, you will see the following:

PORT	STATE	SERVICE
##/tcp	**filtered**	[word or phrase to describe the service]

    b. If they are not dropping traffic, you will see the following:

PORT	STATE	SERVICE
##/tcp	**open**	[word or phrase to describe the service]

3. **Note:** You can target your own computer with this command as well. Just change the IP address based on which computer's firewall rules you want to test.