Bethany Hooten

NDG NETLAB+®

NISGTC

The National Information, Security & Geospatial Technologies Consortium

CompTIA Network+® Lab Series
Network Concepts

Lab 10: Network Security - Firewalls

Objective 5.5: Given a scenario, install and configure a basic firewall

Document Version: 2015-09-18

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

5 Create a Firewall Rule (iptables) within Linux

In the previous tasks, you examined host-based firewalls and implemented firewall rules, or *exceptions,* using a graphical user interface in the Windows OS. In this task, you will use a command-line interface (CLI) based firewall called *Uncomplicated Firewall* (ufw) to implement a host-based firewall in Linux.

The Windows Firewall, Windows with Advanced Security, and Uncomplicated Firewall in Linux are front-end applications that use predefined firewall rules that can be loaded into the program. They also have initial firewall rule settings automatically applied when the firewall is enabled. In the Windows OS, these are called *exceptions* and in the Linux OS, they are called *iptables*.

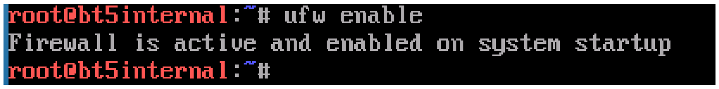
5.1 Enable a Firewall Rule

In current versions of Windows, the firewall is enabled at boot up and default firewall rules are set to block all incoming traffic that does not match an exception and to allow all outbound traffic. In many Linux distributions, the firewall does not run automatically at boot up and needs to be added to the startup configurations to enable it at boot up. For Linux, when the firewall starts, it is configured to allow all inbound and outbound traffic, so even though the firewall is on, it is not filtering.

When preparing to use a firewall in Linux, the first step is to enable the firewall. The next step is to apply the rules to block all incoming traffic that does not match an exception and allow all outbound traffic. Most firewalls allow users to apply rules that are specific to the needs of their situation. In this task, you will enable the Uncomplicated Firewall (ufw) on the Linux Backtrack 5 r3 system and then enable the predefined rules, as well as configure a firewall rule to block outbound telnet traffic, all using the CLI.

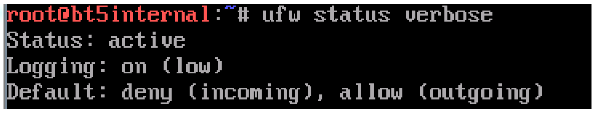
1. On the Backtrack 5 R3 machine at the root@bt5internal:~# prompt, type **ufw enable**. This is the command to activate the uncomplicated firewall program in Backtrack 5 R3.

Keep in mind that Linux commands are case sensitive.



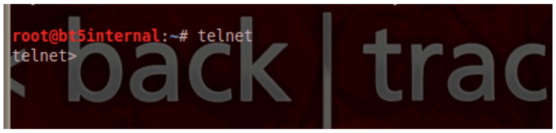
```
root@bt5internal:~# ufw enable
Firewall is active and enabled on system startup
root@bt5internal:~#
```

2. At the root@bt5internal:~# prompt, type **ufw status verbose.** This command shows the status of the firewall and ufw managed rules.



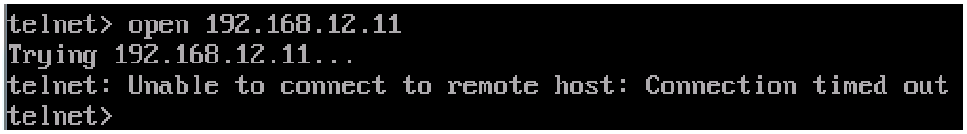
```
root@bt5internal:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
```

3. At the root@bt5internal:~# prompt, type **telnet**. Your prompt will change because you have just opened the telnet utility. Telnet is a TCP/IP utility that allows remote access to computers that are running the telnet service. You will attempt to remotely access the Windows 2k8 R2 Internal 2 machine using telnet. Telnet was a commonly used remote access method in the past, but because it is not a secure program, it has been replaced on many networks by more secure alternatives.



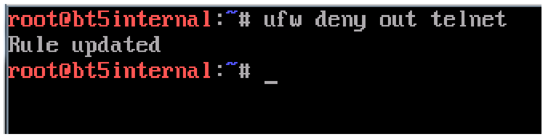
```
root@bt5internal:~# telnet
telnet>
```

4. At the telnet> prompt, type **open 192.168.12.11,** the IP address of the Windows 2k8 R2 Internal 2 machine. Because telnet is no longer installed by default on Server 2008, your attempt to connect will fail.



```
telnet> open 192.168.12.11
Trying 192.168.12.11...
telnet: Unable to connect to remote host: Connection timed out
telnet>
```

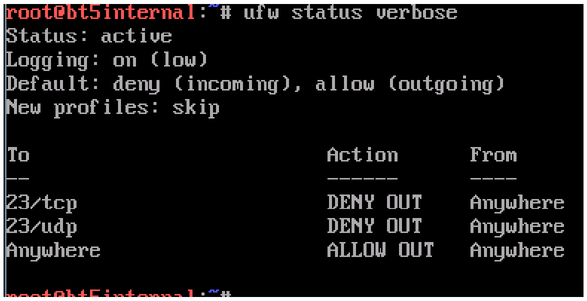
5. You can press ^C or 'q' to exit telnet and get back to the root@bt5internal:~# prompt.
6. At the root@bt5internal:~# prompt, type **ufw deny out telnet**.
   This command will set the firewall rule to deny all outbound telnet traffic. This would prevent users from using telnet on this host. Using an insecure remote access program creates vulnerabilities on the network.



```
root@bt5internal:~# ufw deny out telnet
Rule updated
root@bt5internal:~# _
```

7. At the root@bt5internal:~# prompt, type **ufw status verbose.** This command shows the status of the firewall and ufw managed rules. The **To** column in the output indicates the destination or type of traffic. The Action column indicates how the packet is handled. The **From** column indicates where the traffic is being sourced. A breakdown of the command **ufw deny out telnet:** uncomplicated firewall will examine outbound traffic, if that traffic is generated from tcp/udp port 23 (telnet) then it will deny the packet before it leaves the system. In the

From column, **Anywhere** indicates that regardless of the source, this is how outbound traffic will be controlled.



```
root@bt5internal:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip

To                         Action      From
--                         ------      ----
23/tcp                     DENY OUT    Anywhere
23/udp                     DENY OUT    Anywhere
Anywhere                   ALLOW OUT   Anywhere

root@bt5internal:~#
```

Note: Your output may vary from the above image.

8. At the root@bt5internal:~# prompt, type **telnet**. Your prompt will change because you have just opened the telnet utility.
9. At the telnet> prompt, type **open 192.168.12.11,** the IP address of the Windows 2k8 R2 Internal 2 machine. The connection can't be made because the outbound port is blocked.
10. Type ‘q’ to close telnet.

5.2 Conclusion

There are multiple types of firewalls and most operating systems include a firewall program in the installation. Firewalls all have the same purpose, to block both incoming and outgoing traffic to secure networks and computers while allowing them to be used productively. Differences in the interface and ease of use are big factors in choosing and using a firewall. Firewall configuration ranges from basic to very complex. Understanding TCP ports and protocols is an important part of knowing how to filter traffic and configure firewall rules.

5.3 Review Questions

1. *Compare the ufw status verbose command output with Windows Firewall with the Advanced Security Windows Firewall Properties you investigated in an earlier lab. Describe the major similarities that you observe.*

   Both are front end applications that use prefined firewalls rules and can be automatically applied when enabled

2. *Explain the advantages and disadvantages of having the firewall disabled at start up in the Linux operating system.*

   It depends on the TCP ports and protocols to filter and configure firewall rules

3. *Create and document two firewall rules that you think would be important to include if all outbound traffic is being denied by the firewall rules. Explain your decision.*

   deny telnet because they are an insecure remote access and can create vulnerabilities on the network