Wireless Router Security Potentials and CLI Network Commands: A Vulnerability Protections

Jeffrey John R. Yasay

Faculty, Department of Computer Studies
College of Engineering and Technology
Tarlac Agricultural University, Camiling Tarlac, Philippines

Abstract: This article examines the fundamental parts and standards of wireless routers as defined by the Institute of Electrical and Electronics Engineers (IEEE). Several commands were given using command line interface (CLI) to evaluate the capabilities of certain commands in the network. Vulnerability in the wireless router causes network attacks; it also distinguished the various forms of wireless protection as characteristics in the wireless network equipment. The study has found out that the security potentials have a significant influence in the network growth through proper planning and implementation.

Keywords **– Security, vulnerability, CLI, network.**

I. INTRODUCTION

In the twenty-first century, the ubiquitous network—an entirely new network that can achieve person-to-person, person-to-object, and object-to-object communication anytime and anywhere—and ubiquitous computing are becoming a reality and gradually entering use, driven by rapidly developing new technologies such as wireless access, RFID, network applications, and man-machine interaction [1]. Wireless routers connect with users' PCs using IEEE802.11 protocols. The IEEE (Institute of Electronic and Electrical Engineers), a non-profit organization, created these standards. IEEE has created a plethora of communication standards to ensure that devices from various suppliers can interact with one another. The original design was started in 1990 and took 7 years to finish. It communicates through the 2.4 GHz radio frequency. In most countries, users do not require a license to utilize this band. This is one of the reasons why this standard has gained popularity. The standard defines the interaction between wireless clients and access points. It also specifies the usage of encryption as an option [2].

Wireless connections between computers, routers, or digital video devices are growing so popular that manufacturers have begun to produce increasingly better and more affordable systems. After many years of proprietary devices and ineffectual standards, the industry has chosen to support a single set of wireless networking standards: the IEEE 802.11 family. These standards specify wireless Ethernet, often known as wireless LAN (WLAN) or Wi-Fi (Wireless Fidelity) [3].

II. WIRELESS ROUTER STANDARDS

The most used wireless network adapters and access points use the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification. Most wireless devices are based on this specification and are therefore Wi-Fi certified [4].

There are several different IEEE 802.11 specifications:

1. **802.11a** – Wireless speeds of up to 54 Mbps may be achieved utilizing the 5GHz transmission band, with practical interior ranges ranging from 25 to 75 feet depending on barriers.

2. **802.11b** – Wireless speeds of up to 11 Mbps are possible when using the 2.4GHz transmission band, with practical indoor ranges ranging between 100 and 150 feet. 802.11b is backwards compatible with 802.11g at 11 Mbps.

3. **802.11g** – Wireless speeds of up to 54 Mbps are possible when utilizing the 2.4GHz transmission band, with effective indoor ranges of 100 to 150 feet. At 11 Mbps, 802.11g may coexist with 802.11b.

4. **802.11n** – Wireless speeds of up to 600 Mbps may be achieved utilizing either 2.4GHz or 5GHz transmission frequencies, with an effective interior range of 200 to 300 feet. 802.11n can communicate at 11 Mbps with 802.11b and 54 Mbps with 802.11g. 802.11n is the most recent wireless networking standard, and it improves on prior standards by incorporating multiple-input multiple-output (MIMO).

III. WIRELESS NETWORK SETUP

Configure the Router

While setting up a wireless network, you'll need to use your computer to change the default settings on your router. This entails assigning a unique name and password to your wireless network.

a. Enter the router's default IP address into the address bar of your web browser, then press Enter. The instructions for your router should give this information, but some of the most frequent addresses are 192.168.0.1, 192.168.1.1, and 192.168.2.1.

b. The router's sign-in page will be shown. Again, your router's instructions should provide the specific sign-in information, although most routers utilize a conventional user name and password combination, such as admin and password.

c. The settings page for your router will display. Locate and pick the Network Name option, then provide a distinct network name.

d. Locate and pick the Network Password option, and then select an Encryption option. There are numerous forms of encryption available, it is recommended to use WPA2, which is often regarded as the most secure.

e. Enter the required password here. Use a strong password to assist ensure that no one else can access your network.

f. To save your settings, locate and pick the Save option.

g. Locate your computer's network settings and search for Wi-Fi networks in your area.

h. Select your network, and enter your password.

i. If the connection is successful, use your web browser and navigate to a website such as www.google.com. If the website loads, your Wi-Fi connection is operating properly.

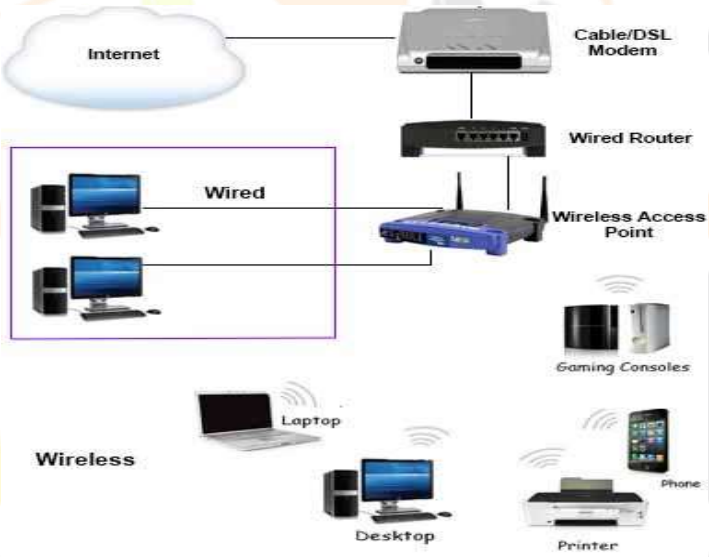

Figure 1. Initial Setup of Wireless Router [5].

IV. WIRELESS ROUTER SECURITY POTENTIAL

Wireless mesh networks have the ability to provide Internet broadband access, wireless local area network coverage, and network connection for fixed or mobile hosts at cheap cost to network operators and customers alike. The basic technology consists of a network of wireless routers relaying packets in a multi-hop form. Many variations in targeted applications and implementation options provide various potential for emerging enterprises in this emerging sector [6].

Aside from altering the default administrator credentials and enabling WPA encryption for Wi-Fi network, there are a few simple steps you can do to help safeguard home router. These include using an OpenDNS server rather than the one maintained by the Internet service provider; disabling remote administrative access (if it's enabled by default); ensuring that your network name, or SSID, contains no hints about the router model or manufacturer; and updating the manufacturer's firmware. Even better, change the firmware with a more secure open-source solution [7].

V. NETWORK VULNERABILITY SCANNER

The operation of the network vulnerability scanner is included in the pricing of proprietary products such as the FortiAnalyzer solution. A FortiGuard subscription service is necessary to obtain an up-to-date list of network application-service vulnerabilities.

To begin a network vulnerability scan, perform the following steps in the correct order:

1. Define an asset to be scanned under Network Vulnerability Scan->Assets Definition. This could be a single or range of hosts' definition. In addition, Microsoft Windows or Unix authentication can be defined to provide more granular host level access to conduct further system level logging and vulnerability assessments.

2. Define when and how to perform the scan for the defined asset created in the above step. This is created under Network Vulnerability Scan->Scan Schedule. Select "create new" to start the Scan Schedule definition which would involve selecting the asset(s) to scan as defined in step 1, choosing the vulnerability scan mode of Quick, Standard, or Full then defining whether to schedule the scan or run it on-demand.

The scan progress can be seen for each scan scheduled under Network Vulnerability Scan → Scan Schedule. Once the scan is completed, the report is produced under Network Vulnerability Scan → Vulnerability Results [8].

VI. BASIC TEST NETWORK DOS COMMANDS

Ping Command

A request/response protocol used to detect whether another IP address is reachable. The requestor issues a ping request message to a certain IP address. If the ping message is delivered, the interface utilizing the destination IP address sends a ping response message to the source IP address. The responding ICMP module replicates the ping request's information into the ping response so that the requestor may match replies to requests. Pings are used by the requestor to determine the roundtrip time to a destination, among other things [9].

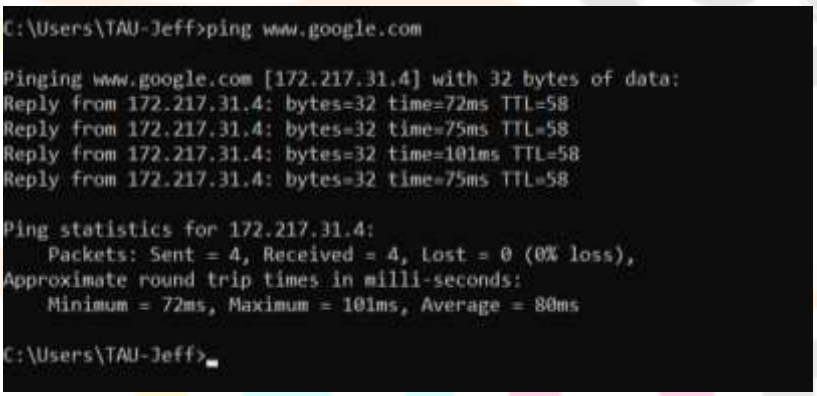

Figure 2. The ping Command Using Command Line Interface

ipconfig Command

Verify that the IP address, subnet mask, default gateway, and other parameters are accurate with this command [10].

Figure 3. The ipconfig Command Using Command Line Interface

Hostname Command

A label that identifies a network hardware device or host. Hostnames are used in both local networks (LANs) and wide area networks (WANs) such as the Internet [11].

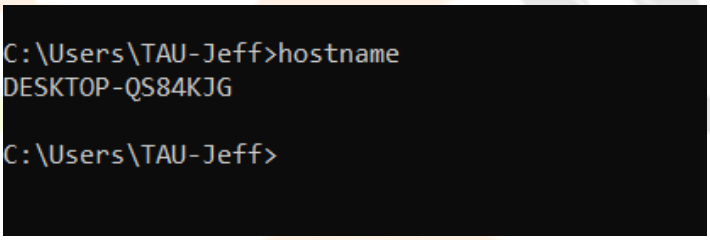

Figure 4. The hostname Command Using Command Line Interface

getmac Command

Can be useful when entering the MAC address into a network analyzer or when determining which protocols are currently in use on each network device on a computer [12].

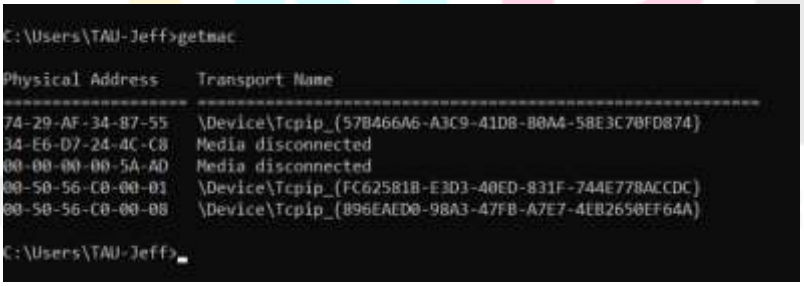

Figure 5. The getmac Command Using Command Line Interface

arp Command

Displays and modifies the Address Resolution Protocol (ARP) cache. An ARP cache is a straightforward mapping of IP addresses to MAC addresses. When a computer's TCP/IP stack uses ARP to identify the Media Access Control (MAC) address for an IP address, the mapping is saved in the ARP cache to speed up subsequent ARP lookups [13].

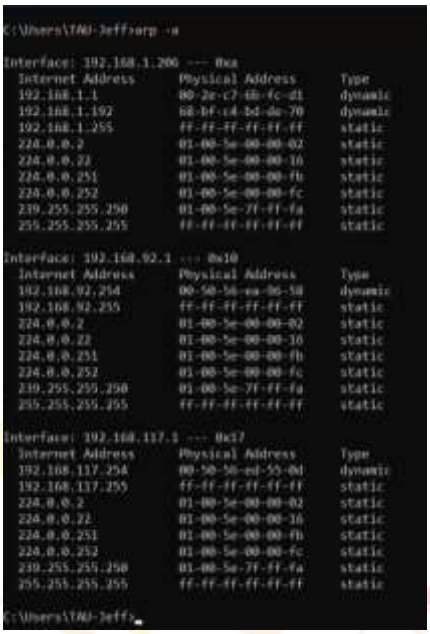

Figure 6. arp Command Using Command Line Interface

NSlookup Command

DNS queries may be highly useful for obtaining many types of information such as mail exchange server information, authoritative information, doing reverse lookups, and so on. Nslookup is fairly simple to use in Windows' command prompt [14].

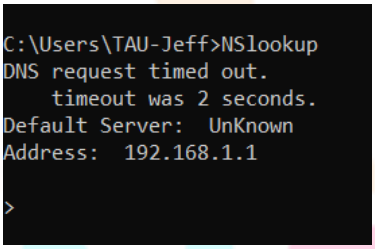

Figure 7. NSlookup Command Using Command Line Interface

NbStat Command

Windows command-line tool that displays NetBIOS over TCP/IP statistics. These activities will show you how to use the nbtstat command [15].

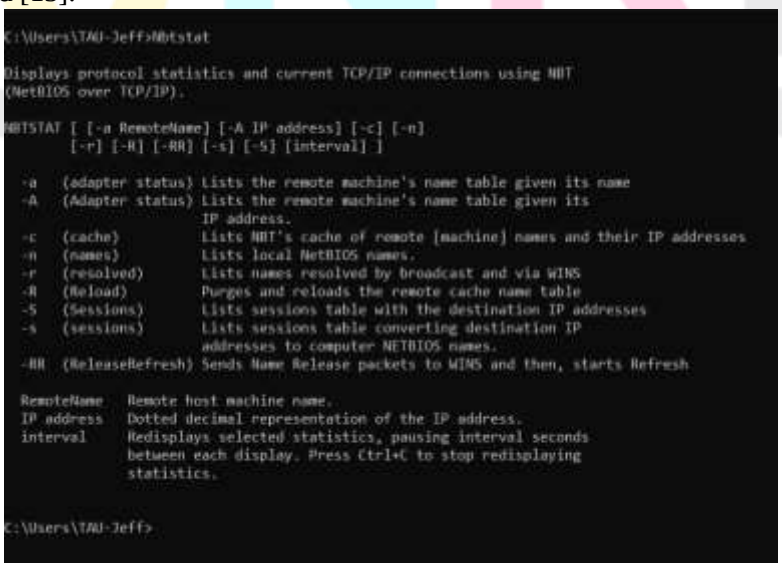

Figure 8. Nbstat Command Using Command Line Interface

Netstat Command

Netstat is a TCP/IP networking software that identifies a computer's listening ports as well as incoming and outgoing network connections. This information can be extremely useful when attempting to address a malware issue or identify a security issue [16].

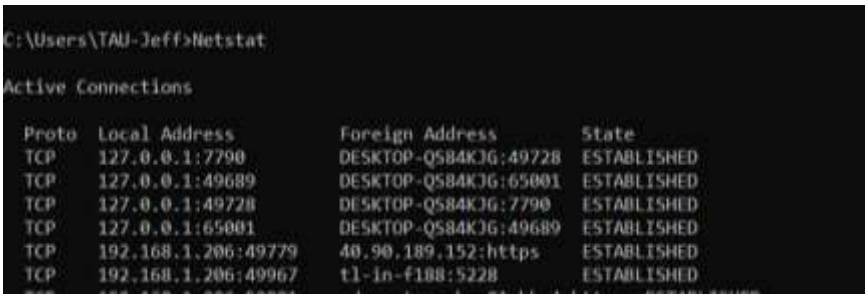

Figure 9. Netstat Command Using Command Line Interface

VII. Wireless Router Capabilities

Password Security

Passwords (together with user account names) are the "keys to the kingdom" in the networking world, granting access to network resources and data. It may sound straightforward to suggest that your complete security strategy should include an effective password policy, but it is a fundamental component that is more difficult to execute than it appears at first look.

To be effective, password policy must require users to choose passwords that are difficult to "crack" but easy for them to remember, so that they do not commit the common security breach of writing the password on a sticky note that ends up stuck to the monitor or prominently displayed in the top desk drawer [17].

MAC Filtering

Network equipment, with a few exceptions, have a physically unique burned-in MAC address. The goal is to give the piece of equipment a unique identify. It is pre-assigned to devices by the manufacturer and is, in principle, absolutely unique. The MAC address is usually 48 bits long. There is a standard format for writing MAC addresses, which are made up of three sets of four hexadecimal numbers separated by dots. The most typical way of writing is to use six sets of two hexadecimal numbers separated by colons or hyphens, such as 00-07-E9-E3-84-F9 [18].

WPA

WPA has been designed to target both enterprise and consumers. Enterprise deployment of WPA is required to be used with IEEE 802.1x authentication, which is responsible for distributing different keys to each user. Personal deployment of WPA adopts a simpler mechanism, which allows all stations to use the same key. This mechanism is called the Pre-Shared Key (PSK) mode [19].

It is also designed to provide a much higher level of security for wireless users than existing WEP standards provide. The WPA specification makes allowances both for network-based authentication for corporate networks, and for a special home mode for use in a SOHO or home-user environment. WPA is capable of interoperating with WEP devices, although in cases of interoperability, the default security for the entire wireless infrastructure reverts to the WEP standard [20].

VIII. Conclusion

In terms of transmission, the usage of a wireless router is rather unusual. It serves as the foundation for all wireless devices. This gadget has security risks and vulnerabilities that must be addressed. The IEEE has discussed ensuring various standards for wireless routers. The capabilities of wireless technology were adapted to enterprise networks in order to meet the needs of this dynamic wireless world, which requires the inclusion of mobile devices and apps in a single, multi user and collaboration infrastructure that seamlessly integrates voice, video, and data while maintaining wireless communication security.

Furthermore, vulnerabilities may arise as a result of system reconfiguration and/or update. As a result, penetration testing and scanning should be performed on a frequent basis, especially following a system reconfiguration or network configuration. The capabilities of password security, MAC filtering, and WPA have greatly aided wireless devices in reducing network vulnerabilities. Different command using Command Line Interface (CLI) in tracing network was also executed to ensure the usefulness of the commands.

IX. Acknowledgment

This article would not be possible without the assistance of Tarlac Agricultural University.

REFERENCES

[1] Zemin, Jiang (2010). On the Development of China's Information Technology Industry || Development of Our Country's IT Industry in the New Period**Originally published in the Journal of Shanghai Jiao Tong University, No. 10, 2008.. , (), 3–56. doi:10.1016/b978-0-12-381369-5.00001-5

[2] Loo, Alfred W. (2010). [Advances in Computers] Volume 79 || Illusion of Wireless Security. , (), 119–167. doi:10.1016/s0065-2458(10)79003-3

[3] Damjanovski, Vlado (2014). CCTV || Networking in CCTV. , (), 410–477. doi:10.1016/B978-0-12-404557-6.50011-2

[4] Jorge Orchilles, Chapter 6 - Networking and Mobility, 2010, Pages 361-419, ISBN 9781597495615, https://doi.org/10.1016/B978-1-59749-561-5.00006-1.

[5] Set up wireless network tutorial. (2013). Retrieved October 8, 2016, from https://www.computer-networking-success.com/set-up-wireless-network.html#sthash.Eqb5Ai9s.dpbs

[6] J. Jun, M.L. Sichitiu, The nominal capacity of wireless mesh networks, in: IEEE Wireless Communications Magazine, Special Issue on: Merging IP and Wireless Networks, October 2003

[7] Wolff, J. (2015, July 06). Your Wi-Fi Network's Soft Underbelly. Retrieved September 16, 2015, from https://slate.com/technology/2015/07/wireless-router-security-how-to-secure-this-vulnerable-point-of-your-wi-fi-network.html

[8] K. Tam, M. H. Salvador, K. McAlpine, R. Basile, B. Matsugu, J. More, Chapter 8 - Analyzing your Security Information with FortiAnalyzer, 2013, Pages 307-322, ISBN 9781597497473, https://doi.org/10.1016/B978-59-749747-3.00008-9.

[9] Walker, Jesse (2014). Network and System Security || Internet Security. , (), 179–220. doi:10.1016/B978-0-12-416689-9.00007-1

[10] N. Alpern, R. Shimonski, CHAPTER 10 - Network Troubleshooting, 2010, Pages 155-175, ISBN 9781597494281, https://doi.org/10.1016/B978-1-59749-428-1.00009-6.

[11] Christensson, P. (2016, November 12). Hostname Definition. Retrieved November 28, 2016, from https://techterms.com

[12] Archiveddocs. (2016, August 13). Getmac. Retrieved November 20, 2016, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/ff961509(v=ws.11)

[13] Learning made easy. (2016, March 27). Retrieved October 8, 2016, from https://www.dummies.com/article/technology/information-technology/networking/general-networking/network-administration-arp-command-184342

[14] Shekhar, A. (2016, May 21). How to check DNS records using BASIC Nslookup command examples. Retrieved September 08, 2016, from https://fossbytes.com/check-dns-records-nslookup-command-examples/

[15] Computer Networks/Nbtstat. (2016, May 22). Retrieved October 20, 2016, from https://en.wikiversity.org/wiki/Computer_Networks/Nbtstat

[16] Cobb, M. (2009, September 09). How to use a netstat command in Windows to watch open ports. Retrieved September 15, 2016, from https://www.computerweekly.com/tip/How-to-use-a-netstat-command-in-Windows-to-watch-open-ports

[17] T. B. Azad, Chapter 7 - Locking Down Your XenApp Server, Securing Citrix Presentation Server in the Enterprise, 2008, Pages 487-555, ISBN 9781597492812, https://doi.org/10.1016/B978-1-59749-281-2.00007-X

[18] L. Shinder, M. Cross, Chapter 13 - Implementing System Security, 2008, Pages 555-596, ISBN 9781597492768, https://doi.org/10.1016/B978-1-59749-276-8.00013-3.

[19] C. Rong, G. Zhao, L. Yan, E. Cayirci, H. Cheng, Chapter 10 - Wireless Network Security, Network and System Security (Second Edition), 2014, Pages 291-317, ISBN 9780124166899, https://doi.org/10.1016/B978-0-12-416689-9.00010-1.

[20] A. Tiensivu, Chapter 4 - Microsoft Windows Server 2008: Network Security Changes, Securing Windows Server 2008, 2008, Pages 137-170, ISBN 9781597492805, https://doi.org/10.1016/B978-1-59749-280-5.00004-3.