

Windows Firewall Bypassing Techniques: An Overview of HTTP Tunneling and Nmap Evasion

O. Igbekele Emmanuel[1(✉)], A. Adebiyi Ayodele[1], A. Marion Adebiyi[1], and B. Francis Osang[2]

[1] Landmark University, Omu-Aran, Kwara, Nigeria
{igbekele.emmanuel,ayo.adebiyi,marion.adebiyi}@lmu.edu.ng
[2] National Open University, Abuja, Nigeria
fosang@noun.edu.ng

Abstract. Internet technology has brought about significant improvement in economical drive thereby making automated processes the new norm. With this new technological drive comes the upsurge in criminal activities as technology has proved to be a densely crime-perpetrated territory. Operating Systems (OS) have had their fair share of this debacle with significant updates being pushed out regularly to mitigate threats. Particularly, the windows OS has the firewall feature which has been a huge success in Intrusion Prevention and Detection systems. The Windows 10 version of the OS will always have significant patches and updates regularly to mitigate security threats. However, there have been several techniques and experiments that proves that firewalls are not sufficient enough for system protection. Advanced techniques in firewall evasions are new generation firewall mechanisms with a combination of techniques usually used to bypass standard security tools, such as intrusion detection and prevention systems, which might detect a protection mechanism. This singular fact that the use of multiple combinations of simpler components is possible, hundreds of thousands of potential Advanced Evasion Techniques exists. This paper therefore takes an overview two of the most significant techniques when it comes to bypassing firewalls - HTTP Tunneling and Nmap Evasion. A comparative study of both techniques helps us look at their similarities and differences and future works.

Keywords: IDS/IPS · OS · Firewalls · HTTP tunneling · Nmap

1 Introduction

1.1 Background

Modern day technological wave has overtime incorporated essential services to further strengthen the concept of security within its usage [1, 2]. The Operating Systems (OS) upon which these services are layered also possess their own security layer which gives users without in-depth knowledge of security protection a level of safety with its usage. The Windows OS has enjoyed wide and significant acceptability because of its

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12957, pp. 546–556, 2021.
https://doi.org/10.1007/978-3-030-87013-3_41

user-friendly environment, but this has made the OS the target of security vulnerability explorers. Connectivity of computing systems has brought security of operating systems under intense scrutiny [3]. Windows 10, most recent version of the Microsoft OS was released in 2015, precisely on July 29 to succeed Windows 8. It is described to be the most secure version of Windows. Most of the numerous challenges that faces Windows 10 ranges from privacy challenges to usability challenges as well as psychological challenges all categorized as either technical or non-technical challenge [4].

While these challenges have been prevalent over the years, different measures, in form of services are being released in updates that seeks to further reduce these risks. Windows 10 has incorporated some of these services believing that privacy is a fundamental right of everyone using their product [5] as well as requirements and maintaining user productivity and data protection [6].

Services ranging from anti-virus, network monitoring, firewall protection, and wireless security are some of the essential services on the Windows 10 OS that helps form extra layers of defense leading to an effective protection strategy. The importance of having a standard network system being protected using a firewall is a necessity, and effectively determines the happenings within the system network. It also can be the difference between safety of the network and possibility of being vulnerable to hacking [7].

Even with the vast reach of innovation, new applications and handsets, the industry technology can be often ignored and become the nest of vipers, and gaining access to mobile networks has always been a honeypot for attackers [8]. The bulk of the research on evasions focuses on how these bypassing techniques and their implementations act within a network. The actual effectiveness of evasion techniques against network defenses has been less explored.

2 Literature Review

2.1 Conceptual Issues

One of the sole aim of network hackers is to be on the lookout for users with little or no security measure in place and therefore making them vulnerable. They use this as a channel to enter networks by processes such as IP spoofing to steal data. There have been several identified ways through which these attackers get packets through firewalls, with IP addresses spoofing being a major channel [9]. With access to network traffic, they can cause a lot of damage ranging from password hijacking attacks, Trojan attacks, registry attacks, and so on, which can be disastrous for any organizations' network.

2.2 Windows 10 Security Issues

As with most OS, Windows 10 has had its share of vulnerabilities in the past. No sooner than its launch, it became the cybercriminals choice for carrying out their attacks. Some of these vulnerabilities include:

Information Disclosure. In exploiting this vulnerability, an attacker simply tricks a user into surfing a malicious website and clicking on some links [10].

Cold Boot Attack. This attack thrives by gaining physical access to the computer's hardware tools. For individuals who store highly-sensitive information on their personal computers, or for high-ranked government officials or top businessmen, the effect of this can be catastrophic.

Remote Code Execution. This vulnerability surfaced as a result of improper input validation by Microsoft.NET framework. This attack is not geographically bound as attacker gain remote access to user's computer without being physically present.

Privilege Elevation. This vulnerability exists as a weakness in authentication requests on the Windows OS. It usually comes into fore when the Windows kernel improperly handles objects in memory [11] (Table 1).

Table 1. Summary of Windows 10 vulnerability impact based on the CIA triad.

Criteria	Confidentiality breach	Integrity breach	Availability breach
Information disclosure	*Partial*	*None*	*None*
Code boot	*Complete*	*Complete*	*Partial*
Remote code execution	*Complete*	*Complete*	*Complete*
Privilege elevation	*Partial*	*Partial*	*Partial*

2.3 Firewalls

Firewalls are defense mechanisms designed with the sole aim of preventing unauthorized access into or from a network. They can be implemented either software or hardware, or a combination of both. Essentially, owners of private networks using the internet utilize firewalls to block unauthorized access to such networks, especially intranets (Fig. 1).

Firewalls are implemented in three basic forms:

- Packet Filters: sieves network access by controlling inbound and outbound network packets
- Stateful Inspection: analyses packet headers and the current state of the packets at the network layer of OSI
- Proxy Servers: acts as message filters in the application layer of the OSI.

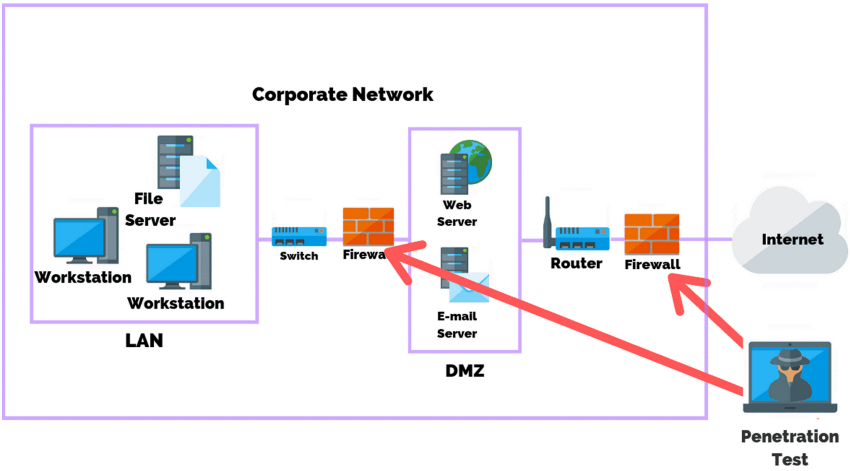

Fig. 1. Corporate Network Architecture showing firewall placements [12]

Firewall bypassing is a technique used by attackers in manipulating the attack sequence to mask themselves over the network to avoid being detected by the underlying security firewall [13]. Usually, firewalls operates on some predefined set of rules, and by extensive skills, such an attacker can bypass the firewall by exploring various firewall bypassing techniques.

Previous works of authors such as [14–17] have focused solely on firewall security as well as that of VPNs, leaving out attack mechanisms or threats on firewalls. The work of [18] was very extensive as regards the loopholes that have been overlooked in years past as regards firewalls. The authors highlighted packet-filtering, application proxy and stateful inspection as the major working principles on which firewalls thrive.

[19] identified some weaknesses in firewalls as displayed in the table below (Table 2)

Table 2. Five kinds of firewalls and their weaknesses [20]

SN	Firewall Type	Security Weakness
1	Personal Firewall	Inability to control and observe multiple communication simultaneously
2	Web Application Firewall	Restricted user range
3	Packet-filtering Firewall	Very difficult in its configuration
4	Network address Firewall	Helpless against attacks and threats from within the system
5	Dynamic detection Firewall	Causes delays in network connection

Although firewalls have weaknesses, they are very much active in protecting users from various forms of attack some of which are listed below from the in-exhaustive list [21]:

- Eavesdropping
- Password Guessing
- Service Denial
- Host Attacks
- Social Engineering
- Protocol Based attacks

These therefore signify the strengths of firewalls especially as it concerns places and organizations. Private networks that are connected to a public network will require firewall protection [22]. Also, individuals connected through the use of Internet modems to will require a personal firewall software. Dial-up internet users usually assume they are safe from illegitimate users, however, these users have fallen victim of attacks and in the process losing significant data [23]. Firewall is also required by these users to avoid such attacks.

[24] posited that next generation firewalls will incorporate integrated signature-based intrusion prevention system mechanism which particularly filters the intrusions received for its reporting system. Also, these firewalls will possess the ability to embed information from outside the system, including white records, index based arrangements, etc.

2.4 Tunneling

Tunneling, just as it appears in real world, is a passage way created where there exists none. It is a method of data transfer over a network protocol that is naturally not supported by the network. This method thrives by embedding small pieces of data inside other packets for reassembling at the destination in a process known as encapsulation. Often used in Virtual Private Networks, tunneling also helps set up secure and efficient connections between networks allowing users to bypass firewalls. This technique allows users to remotely access and connect to various network resources in form of Corporate Home Gateways or Internet Service Providers through external networks. Generally, tunnels established through these external network are done though a multipoint passage and connects a remote user to some resource at the far end of the tunnel.

There are basically four (4) Tunneling protocols, they are:

1. Point-to-point Tunneling protocol (PPTP)
2. Secure Socket Tunneling Protocol (SSTP)
3. Layer 2 Tunneling Protocol (L2TP)
4. Virtual Extensible Local Area Network (VxLAN)

HTTP Tunneling is a relatively more efficient technique involving the use of HTTP. It is a known fact that network administrators usually grant HTTP traffic access through their network boundaries albeit with the aid of application level proxies and a firewall.

The wide acceptance of this evasion technique is largely due to its effectiveness which makes it easy for users with legitimate motives, or worse still, spyware, adware and viruses, ability to bypass the established network security policies implemented at the proxy/firewall. This is done by incorporating just any protocol into what looks like a normal web browsing activity. What is essentially needed is an external host accepting HTTP connections, configured as a tunnel exit point and redirecting packets to the "true" destination, i.e., to the actual destination of the protocol.

2.5 Nmap

Network Mapper, commonly referred to as Nmap is a free, open source tool, available under Unix GPL as published by the Free Software Foundation. It is a network administration tool used by IT security professionals to scan enterprise networks, looking for live hosts, specific services, or specific operating systems details. Nmap was created with firewall subversion purpose and it has always been a very useful tool in staying abreast of network and operating systems updates that impact the scanning capabilities of the tool.

Usually activated from the command-line, Nmap works simply by calling the application (nmap or nmap.exe) and padding the command with the appropriate parameters or switches. Also, new network users use the tool for advanced configuration having the help instructions close-by. These can be easily accessed from the command-line by typing nmap –h.

3 Procedural Comparison

3.1 HTTP Tunneling

It is common knowledge that attackers are always on the lookout for users whose account and access can be easily compromised, so that they tailgate into the networks using IP spoofing for the purpose of data theft. Attackers can readily access data packets through firewalls using this spoofing method [25]. If successful, damage can be perpetrated by causing Trojan attacks, password hijacking attacks, amongst many others, which can be disastrous for organizations' network. A simple HTTP Tunneling attack undergoes some of these procedures:

1. Ensure firewall is turned on in the target machine
2. Ensure the Internet Information Service (IIS) admin and WWW Publishing services are disabled on the target machine
3. Install any HTTP tunneling software (e.g. HTThost) on the target machine
4. After successfully blocking the attack machine IP address, leave target machine running and navigate to the attack machine
5. On target machine, ensure all FTP sites are stopped
6. Open Control Panel and Launch Firewall settings
7. Ensure firewall is turned on and set outbound rules to block all remote Ports and Protocols

8. Test rule by disabling and testing the ftp site on the target machine (ftp IP Address) – Access will be granted
9. Now, re-enable rule and check to see that access is denied.
10. Next, we perform tunneling using an application called HTTPort to establish a connection with the FTP site located on our target machine.
11. After successful installation, on the HTTPort main window, on the Proxy tab, enter the Host name or IP address of the target machine where HTThost is running. Enter the Port number 80.
12. Under Miscellaneous options, Bypass mode, select Remote host from the drop-down list. Under Use personal remote host at (blank = use public), re-enter the IP address of target machine and port number 80.
13. Select the Port mapping tab, and click Add to create a New Mapping, right-click the New Mapping node, and click Edit. Right-click the node below Local port, then click Edit, and enter the port value as 21. Right-click the node below Remote host, click Edit, and rename it as attack machine IP Address. Right-click the node below Remote port, then click Edit, and enter the port value as 21.
14. Now, switch to HTTPort Proxy tab and click Start to begin the HTTP tunneling. HTTPort intercepts the ftp request to the local host and tunnels through it. HTTHost installed in the target machine to connect you to the attack machine. This means you may not access ftp site directly by issuing ftp IP Address in the command prompt, but you will be able to access it through the local host by issuing the command ftp 127.0.0.1.

HTTP Tunneling Risks. Tunnels are very herculean to detect essentially because they work by bypassing HTTPS traffic, whereas HTTPS traffic should naturally undergo end-to-end encryption thereby preventing inspection [26]. This singular mechanism gives rise to a whole lot of risks, some of which are:

- Service interruptions when an insider uses internet bandwidth for personal or inappropriate gains.
- Tunneling allows behaviors or conduct outside of the security or organizational polices.
- Law suit risks when organizational network is used to access copyrighted materials.
- Intellectual property rights issues

3.2 Nmap Evasion

Nmap has achieved global acceptance from both systems and network administrators, security and network engineers, firewall administrators, incident response teams, pen-testers, desktop administrators, and indeed anyone who works around systems and networks in a secure environment. Job function that revolves around locating a system, looking out for open ports, determining what services running on a given port, or identifying the operating system that a particular server uses, has looked to Nmap to help fulfill these service needs [27]. A simple Nmap Evasion attack undergoes some of these procedures:

1. Ensure firewall is turned on on the target machine
2. Open Control Panel and Launch Firewall settings
3. Ensure firewall is turned on and set inbound rules to block all remote Ports and Protocols and IP Address of the attack machine
4. On attack machine, perform a different kinds of network scans (Basic nmap scan e.g. nmap IP Address, SYN scan e.g. nmap -sS IP Address, INTENSE scan e.g. nmap -T4 -A IP Address) – Result: No access as all scanned ports are filtered due to firewall restrictions.
5. However, a PING Sweep scan on the network subnet (e.g. nmap -sP IP Address/24) – Result: A revelation of the live machines on the network is returned.
6. Finally, a Zombie scan on any of the detected live hosts on the network will reveal the open ports on the network.

Nmap Evasion Risks. Although with proper usage, Nmap is a formidable network security against invaders, however with improper usage, Nmap can (in rare cases) result in complicated legal issues. Hence, it is important to reduce risks by reading available legal guides before using Nmap. This singular mechanism gives rise to a whole lot of risks, some of which are:

- Scanning a network without permission
- Loose scans not tightly targeted
- Doing controversial things using your organization's network
- Performing scans without any legitimate reasons.
- Using version scanning on portly written applications
- Scanning multiple ports and machines on a network

3.3 Similarities in Both HTTP Tunneling and Nmap Evasion Techniques

While both processes and procedures as firewall evasion techniques are distinct, there exist a measure of similarities between them [28], some of which are listed below:

1. They both use the pcap library routines in providing an interface which enables applications detect raw packets from the network.
2. They both have a software that helps with user interface to monitor network packets
3. They both possess network scanning capabilities which helps in discovering active hosts, ports, services, and operating systems on which the target system operates.
4. No server modification required for its operations.

3.4 Differences Between HTTP Tunneling and Nmap Evasion

The following Table gives a comparison of the significant differences between both techniques (Table 3).

Table 3. Differences between HTTP tunneling and Nmap evasion.

Criteria	HTTP tunneling	Nmap evasion
Operating Systems Platform	Windows Platform	Platform Independent
Scanning Option	Direct and Concise	Varying options available – in-depth knowledge is needed
Client Modification	Modification to help wrap the connection with the HTTP header	No additional modification required after installation
Multiple Connections	Each connection to a remote TCP port requires a distinct tunnel	A single connection can carry out multiple activities
Variances	Simple, VPN, etc. are variances	No variance of Nmap
Integrated timing policies	No timing policy integrated	Integrated timing policies that vary from T0 (very, very slow) to T5 (extremely fast)
DNS resolution issues	Cannot perform DNS resolution	The –n option allows this action to be performed

4 Conclusion

In this study, an overview has been done on firewalls and its components with a special focus on techniques that aids bypassing the security layer. It is clear and evident that firewalls on its own is not a guaranteed security layer as the concept of absolute security has been thwarted overtime. HTTP Tunneling and Nmap Evasion techniques were the two firewall evasion techniques compared and although there are a couple of similarities in their deployment mode, there also exists a few difference in their setup and inadvertently, their mode of operation.

The study reveals that although firewalls as a form of Intrusion Detection/Prevention Systems is widely accepted in systems deployment, its workability, performance, accuracy and security is not solely based on the rules and specifications put to use, but also a function of the additional security layer harnessed with the system and how the hybrid techniques are combined. This paper would create an awareness on the weakness of firewalls as a singular IPS and possible improvements on some of the existing evasion techniques.

The next-generation firewalls will require an improved detection of encrypted applications and inclusion of prevention services, hence modern threats like application-layer attacks or web-based malware attacks have an unignorably negative effect on these threat areas [29]. Moving forward, it is the best network security systems that can be used to block and quarantine attacks/threats according to the security policies [30].

References

1. Ansalem Ez, A., Igbekele, E.: Cloud computing research in Nigeria: a bibliometric and content analysis. Asian J. Sci. Res. **12**(1), 41–53 (2019). https://doi.org/10.3923/ajsr.2019.41.53
2. Khu-Smith, V.: Enhancing the security of electronic commerce transactions (2003). http://dig irep.rhul.ac.uk/items/e42a99f4-78e1-69a3-87fd-6ac743f828ca/1/
3. Alhazmi, O., Malaiya, Y., Ray, I.: Vulnerabilities in Major Operating Systems (2004)
4. Goretsky, A.: Microsoft Windows 10 Security and Privacy. An ESET White Paper, pp. 1–34 (2017). https://www.welivesecurity.com/wp-content/uploads/2016/06/windows-10-security-privacy.pdf
5. Microsoft: Windows and the GDPR: Information for IT Administrators and Decision Makers, 05 October 2018. https://docs.microsoft.com/en-us/windows/privacy/gdpr-it-guidance
6. Rogers, M.: Windows resources to help support your GDPR compliance, 5 September 2017. https://blogs.windows.com/windowsexperience/2017/09/25/windows-resources-to-help-support-your-gdpr-compliance/#17Jy0ZeZXv4dH6Gl.97
7. Igbekele, E., Adebiyi A., Ibikunle, F., Adebiyi, M., Olugbara, O.: Research trends on CAPTCHA: a systematic literature review. Int. J. Electr. Comput. Eng. (IJECE), **11**(5), 4300–4312 (2021). https://doi.org/10.11591/ijece.v11i5
8. R. Roaming Consulting Company Ltd.: Signalling Firewall Vendor Performance Report 2018, pp. 1–31 (2018)
9. EC-Council: Ethical Hacking and Countermeasures. Reproduction, pp. 1–19 (2008)
10. NIST: National Vulnerability Database. Published January 2019. https://nvd.nist.gov/vuln/detail/CVE-2019-0582
11. CVE Details: Microsoft Windows 10: List of security vulnerabilities - CVE Details. https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html
12. Stankovic, S.: Firewall Penetration Testing: Steps, Methods, & Tools (2019). https://purplesec.us/firewall-penetration-testing/
13. Jiang, C.: Research on computer network security technology and firewall technology. Ability Wisdom 235 (2017)
14. Sun, K.: Concrete application of firewall technology in computer network security. Sci. Technol. Econ. Guide **17**, 38 (2017)
15. Sahin, M., Sogukpinar, I.: An efficient firewall for web applications (EFWA). In: 2017 International Conference on Computer Science and Engineering (UBMK), pp. 1150–1155 (2017)
16. Ma, L., Liang, H.: Application of firewall technology in computer network security. Comput. Knowl. Technol. **10**, 3743–3745 (2014)
17. Su, J., Yuan, J.: Firewall technology and its development. Computer Eng. Appl. 147–149 (2004)
18. Yang, Z., Cheng, Q.: Research of immune-based technology for the firewall system security. Microcomput. Inf. **21**, 9–3
19. Boukari, N., Aljane, A.: Security and auditing of VPN. In: Proceedings of Third International Workshop on Services in Distributed and Networked Environments, pp. 132–138, 6 Aug 1996
20. Jingyao, S., Chandel, S., Yunnan, Y., Jingji, Z., Zhipeng, Z.: Securing a network: how effective using firewalls and VPNs are? In: Arai, K., Bhatia, R. (eds.) FICC 2019. LNNS, vol. 70, pp. 1050–1068. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-12385-7_71
21. Zhang, T.: Design and implementation of firewall based on content filtering software. University of Electronic Science and Technology (2012)

22. Zeng-gang, X., Xue-min, Z.: Research and design on distributed firewall based on LAN. In: Computer and Automation Engineering (ICCAE), pp. 517–520. IEEE, Singapore (2010). E-ISBN 978-1-4244-5586-7, Print ISBN 978-1-4244-5585-0, INSPEC Accession Number: 11259785. https://doi.org/10.1109/ICCAE.2010.5451596
23. Chopra, A.: Security issues of firewall. Int. J. P2P Netw. Trends Technol. **22**(1), 4–9 (2016). https://doi.org/10.14445/22492615/ijptt-v22p402
24. Chakravarthi, M.R., Meenakshi, N.: Next generation firewall- a review. Int. J. Comput. Sci. Inf. Technol. **7**(3), 1212–1215 (2016)
25. Alman, D.: Information Security Reading Room HTTP Tunnels Though Proxies (2021)
26. Pack, D.J., Streilein, W., Webster, S., Cunningham, R.: Detecting HTTP tunneling activities. In: Proceedings of the 2002 IEEE Workshop on Information Assurance, pp. 1–8 (2002)
27. Nmap: Chapter 2 Introducing Nmap Solutions in this chapter (2013). http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introducing-Nmap.pdf
28. EC Council: Certified Network Defense (CND) Outline, pp. 1–26 (2021)
29. Saurav, P.J.: A brief survey on next generation firewall systems over traditional firewall systems. Int. J. Sci. Eng. Res. **11**(1), 795–800 (2020). http://www.ijser.org
30. Next-generation firewalls: Imperial J. Interdiscip. Res. (IJIR) 2(5) (2016). ISSN 2454-1362