Inspection Report: Strength of Different types of Firewall

Prepared for:

Leann Nicholson

Prepared by:

Niladri Sengupta

Computer Technologist

Date of Submission:

December 2,2016

Introduction

The purpose of this report is to check the vulnerability of the computer systems taken with and without the use of different types of firewall.

There are 4 different computer systems taken into account System A, System B, System C and System D. All systems have the same specifications excluding the firewall. The variance in levels of security achieved using different settings of firewall is the main focus of the inspection.

Included in this report are our findings, as well as pictures of the equipment, accompanied by analysis of the damage done to the systems along with its solutions.

There are several terms that are used in the report which are outlined below:

|  |  |
| --- | --- |
| **Glossary** | |
| **Term** | **Definition** |
| VPN/Proxies | Virtual Private Network (VPN) is a way to connect to the internet via a remote and/or private server instead of using your own machine as the connected system. |
| TOR | The Onion Router (TOR) disguises the identity of the user by moving traffic across different TOR servers. It encrypts all the traffic such that the it cannot be traced. |
| WPA2-PSK (AES) | Wi-Fi Protected Access 2 Pre-Shared Key with Advanced Encryption Standard. |
| WEP | Wired Equivalent Privacy (WEP) is a security protocol that follows the IEEE Wireless standard. |
| Routers | A device and/or software that determines the best way to deliver a packet to the destination. |
| Packets | A packet is the unit of a data is routed between the source and destination of the internet or other packet-switching switching [9]. |
| Trojan Backdoor | A certain type of virus that knowing for its malicious software programs that performs a number of different things. |
| Anti-virus | Anti-virus is a program that detects and prevents malicious infections and/or attempts in a system. |

Background

Utilizing 4 systems with the same specifications, we check the strength of three different types of firewalls. Namely the WEP firewall in one system, WPA/WPA2 firewall in another as well as VPN/Proxies, TOR and WPA/WPA2 mix of firewall in the final system.

**WEP** was create in 1999 as a basic network security for wired networks. After being widely used for years, it was clear that its security was extremely lacking with the FBI publicly demonstrating how it could be hacked in minutes.

**WPA2-PSK (AES)** is the second version of the WPA with AES encryption. WPA/WPA2 was an upgrade from the older and more vulnerable WEP [5].

**TOR** disguises the identity of the user by moving traffic across different TOR servers. It encrypts all the traffic and moves it to different TOR servers such that the it cannot be traced back to the original user [8].

**VPN** is built using public wires connected to a private network [7]. It allows the user to browse the internet off a separate network leaving the user’s system safe and secure.

**The need for Firewall:**

Having an active internet connection leaves, you vulnerable to hackers who will attempt to access your personal and financial information stored on your system [1]. Hackers sometimes hijack your network connection and flood the system with malicious viruses and worms crashing or disabling your system.

A firewall acts as a shield or fortification between your computer system and the internet [4]. When connected, and accessing the internet, the system is in a constant state of uploading and downloading information. All information entering the system pass through the firewall which examines each small packet of information and blocks those that do not meet the security criteria [2].

Standards Used

For this inspection, we used a NIST SP 800-41 standard created by the National Institute of Science and Technology under the Federal Information Security Management Act (FISMA) of 2002 [10]. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.

This standard has been prepared for use by Federal agencies. It may be used by non-governmental organizations on a voluntary basis.

There are several types of firewalls, each with varying capabilities to analyze network traffic and allow or block specific instances by comparing traffic characteristics to existing policies [11]. Understanding the capabilities of each type of firewall, and designing firewall policies and acquiring firewall technologies that effectively address an organization’s needs, are critical to achieving protection for network traffic flows

“New firewalls should be tested and evaluated before deployment to ensure that they are working properly.”[10]

The criterion that will be used for this inspection:

1. **Connectivity**

Users can establish and maintain a connection through the firewall with no errors or complications arising.

1. **Ruleset**

Traffic that is specifically allowed by the security policy is permitted. All traffic that is not allowed by the security policy is blocked. REF

1. **Management**

Administrators can configure and manage the traffic going through the systems with the help of the effectively and securely.

1. **Performance**

Firewall’s should be able to provide adequate performance during the normal and peak usage. This is very important in the performance and security of the firewall during a DoS attack.

1. **Additional Features**

Additional features that will be used by the firewall—such as VPN and antimalware capabilities—should be tested to ensure they are working properly.

Inspection Method

With the help of a 3rd party anti-virus software(Avira) we scan the infected system using a complete and thorough system scan. Noting down the number of files infected and the damage done to the system along with the actions that will be needed to take place to fix the system [12]. Using these results, we rank the effectiveness of the firewall on the respective systems.

The inspection was done using a few items, mainly

* An average network router (Linksys AC1900)
* 4 identical computer systems (Aspire E5-773G\_0985\_1.05 all running Windows 10)
* Anti-virus software (Avira)
* A controlled Malware (Trojan backdoor)
* High speed Lan connection (100 mbps down 50 mbps up)

The Trojan backdoor is given a period of 1 hour with the specific systems and their firewalls. The antivirus system scan runs at an average of 180-200 minutes.

The inspection was evaluated based on the NIST SP 800-41 standard and the main areas of focus were

* **Detection Capability:** The ability of the firewall to detect and isolate the Trojan backdoor being used to cause the infection.
* **Performance Check:** The performance of the system was checked and compared to its performance before the attack.
* **Data Usage Privileges:** The ability of the firewall to block the use/change of data that should be accessible only to the administrators.
* **System Recovery:** The amount of work that is needed to bring the system to its performance levels before the attack.

Location

Location was a closed and secure workplace environment. The inspection was performed using only a power outlet alongside the required units and systems. This inspection can be done close to anywhere and hence location used is irrelevant for this inspection.

Results

**System Results:**

**System - A:** To use again, complete reformat, hardware changes recommended

**System - B:** An operating system reformatting required

**System - C:** Full system anti-virus run cleanup required

**System - D:** Little to no action required.

**Final Inspection Report:**

* **Detection Capability**
  + **System A**

No firewall, hence no malware detection capabilities

* + **System B**

Limited detection capabilities, only detected malware after system 32 was infected.

* + **System C**

Malware was detected but not isolated. Led to few files being corrupted, but no system 32 files damaged.

* + **System D**

At introduction of Trojan, malware was detected by firewall. Malware was isolated and awaiting instructions for deletion.

* **Performance Check:**
  + **System A**

Full system crash after allocated malware spread time.

* + **System B**

System performance was significantly lowered, attempts at reformatting were hampered due to low performance.

* + **System C**

Performance was affected, but not unrecoverable. Performance was restored to pre-malware infection.

* + **System D**

Performance was not affected. Full system running at stable levels.

* **Data Usage Privileges:** 
  + **System A**

All files were accusable to malware infection.

* + **System B**

Data usage authorization was initiated late, after data was infected.

* + **System C**

Main system files were protected along with private data.

* + **System D**

No files other than user inputted infected files were accessed.

* **System Recovery:** 
  + **System A**

System was not recoverable. After considerable effort was system reusable.

* + **System B**

System was damaged but not unrecoverable. There was loss of data.

* + **System C**

System was lightly damaged and fully recoverable. Close to no loss of data

* + **System D**

System was not damaged. All files were useable. No recovery was needed.

Observations and Recommendations for Improvement

**System - A:**

* Malware infected all files accessed by user after the Trojan was introduced. Along with almost all system accessed files being infected as well.
* Computer was inaccessible for first few attempts at start-up. Only after repeated attempts was system recovery possible with system damage.
* Full computer reformat along with reinstallation of close to all system drivers. Hard disk was damaged and even after reformat was functioning with a lower performance (recommend replacement). Installation of high level firewall recommended for prevention of future attacks.

**System – B:**

* Trojan infected sizeable portion of the system files (system32), including private files and documents. Drivers were not damaged. Warning were given about unauthorized execution of files at system files level. Warnings were given at regular intervals.
* Computer was accessible but could not perform at maximum levels. System restore was used to recover settings. System reformat recommended.
* Installation of higher grade firewalls along with education on how to not introduce viruses to system would be ideal in maintenance of system performance.

**System - C:**

* System files and drivers were damaged, but close to all of the data was recoverable although private files may have been breached.
* Warnings were given along with protection of certain levels of system files.
* Packets was stopped at the router of the system and the user was asked to either drop or keep the packet.
* Recommend full system scan by anti-virus, along with windows system restore.

**System - D:**

* Full system was shielded.
* Warnings were given at the introduction of the malware. Immediate action was taken by the firewall in isolating and then deleting the malware once confirmation on type of malware was found.
* Only files accessed by the user on purpose for testing of system with the Trojan Backdoor were found to be infected and needed a quick system fix.
* No action recommended. Firewall performs perfectly.

Outcome

System A was a **failure** and performed the duty of lowest possible protection level possible in a computer system.

System B was a **failure**, as the firewall did not protect the system 32 files along with private data. Amount of information that could be stolen in such an attack is unacceptable in a modern computer system.

System C was a **close pass**, most files were undamaged and main system 32 files were not changed or damaged. Private data was protected but if private data was accessed by the user during the infection period it could have been stolen or corrupted.

System D was a **success**, with no files being harmed other than those accessed by the user using the Trojan. System ran at stable performance even during the attack. Ideal system for higher security computer systems.

# Bibliography

|  |  |
| --- | --- |
| [1] | M. Rouse, "Firewall," Search Security, November 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/firewall. [Accessed 1 December 2016]. |
| [2] | V. Beal, "Firewall," Webopedia, [Online]. Available: http://www.webopedia.com/TERM/F/firewall.html. [Accessed 1 December 2016]. |
| [3] | "What is firewall?," Paloalto, [Online]. Available: https://www.paloaltonetworks.com/documentation/glossary/what-is-a-firewall. [Accessed 1 December 2016]. |
| [4] | M. Anicas, "What is a Firewall and How Does It Work?," DigitalOcean, 20 August 2015. [Online]. Available: https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work. [Accessed 1 December 2016]. |
| [5] | V. Beal, "WPA2-PSK," Webopedia, [Online]. Available: http://www.webopedia.com/TERM/W/WPA2\_PSK.html. [Accessed 1 December 2016]. |
| [6] | C. Hoffman, "Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?," How-To Geek, [Online]. Available: http://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/. [Accessed 1 December 2016]. |
| [7] | E. Geier, "How (and why) to set up a VPN today," PCWorld, 19 March 2013. [Online]. Available: http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html. [Accessed 1 December 2016]. |
| [8] | W. Nicol, "A BEGINNER’S GUIDE TO TOR: HOW TO NAVIGATE THROUGH THE UNDERGROUND INTERNET," Digital Trends, 19 January 2016. [Online]. Available: http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/. [Accessed 1 December 2016]. |
| [9] | M. Rouse, "Packet Filtering," SeachNetworking, September 2005. [Online]. Available: http://searchnetworking.techtarget.com/definition/packet-filtering. [Accessed 1 December 2016]. |
| [10] | P. H. Karen Scarfone, "National Institute of Standards and Technology," September 2009. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf. [Accessed 1 December 2016]. |
| [11] | A. D. K. S. M. B. J. M. S. Sotiris Ioannidis, "Implementing a distributed firewall," 2000. [Online]. Available: http://dl.acm.org/citation.cfm?id=353052. [Accessed 10 October 2016]. |
| [12] | A. Wool, "A quantitive study of firewall configuration errors," 21 June 2004. [Online]. Available: http://ieeexplore.ieee.org/document/1306389/. [Accessed 10 October 2016]. |