IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

EVADING FIREWALL USING Nmap TOOL

NOBLE JONES S , NILESH SHINDE , KARTHIGEYAN S

1 Student, Dept of Computer science engineering, Dr . M.G.R Educational and Research Institute, Chennai, Tamil Nadu, India

2 Student, Dept of Computer science engineering, Dr . M.G.R Educational and Research Institute, Chennai, Tamil Nadu, India

3 Student, Dept of Computer science engineering, Dr . M.G.R Educational and Research Institute, Chennai, Tamil Nadu, India

Abstract

The primary goal of firewall penetration testing is to prevent unauthorized internet access to your organization's internal network, or check to make sure your security policy is doing what you think it's doing. In order to successfully test your organization's firewall, you must think like the adversary. Collecting intelligence on the network, such as operating system and firewall type, are important to know in order to proceed with the penetration test.

A firewall penetration test's success is determined by a number of factors. Making sure firewall policies and rules are properly configured can greatly limit the success of attacks and prevent the majority of unauthorized connection attempts. The first step in firewall penetration testing is to find the firewall. Nmap, a popular open-source tool for network discovery and auditing, can be used to accomplish this. This tutorial will demonstrate how nmap can be used for firewall penetration testing to evaluate and improve the security of your network.

Introduction

There are several opportunities to test network penetration. These penetration tests are typically carried out by businesses in order to ascertain whether or not their network and all of the devices that are connected to their internal network are secure and up to date in accordance with the policies that they have established.

Imagine that a firm has hired you to conduct a network-based penetration test for them, but all you have is a list of IP addresses, and even then, the corporation isn’t entirely sure how many IP addresses are used internally because there is always the possibility that there are more.

As soon as you have access to the services that are operating, you will be able to individually search for vulnerabilities and attempt to exploit them. But now things begin to take an unexpected turn. You will probably run into a firewall at some point, and it is possible that it will discard the packets that nmap generates (or any other port scanner).

IMPLEMENTATION

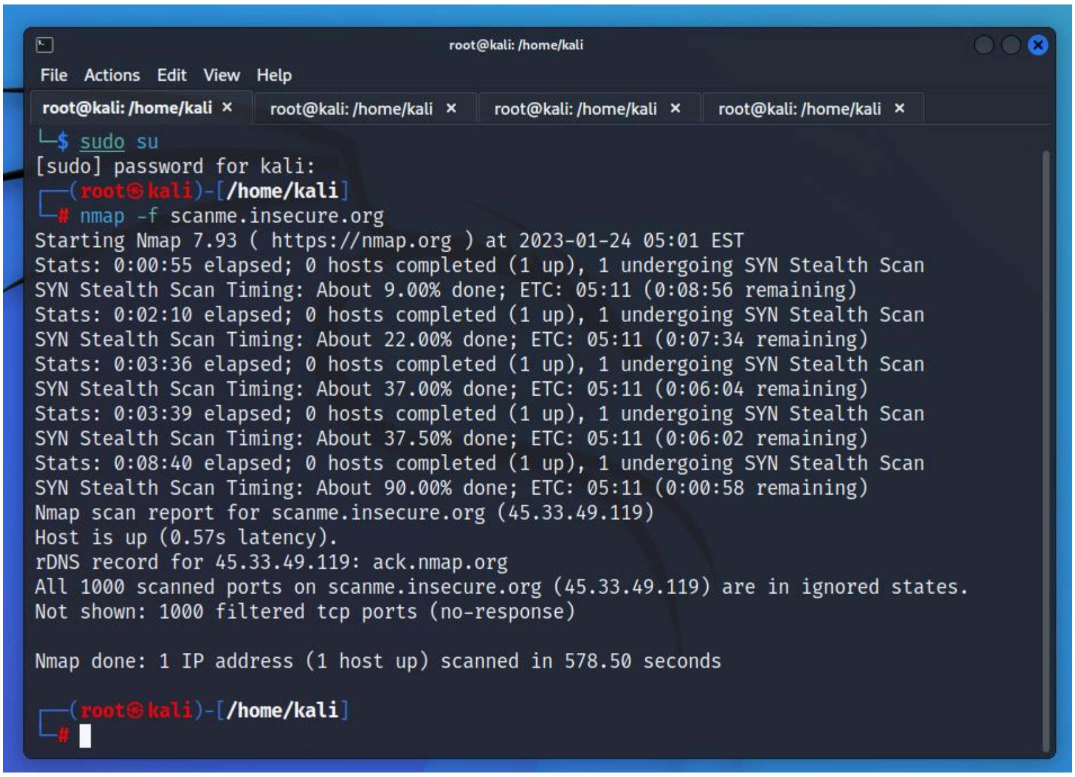
<u>Overview of Firewall Evasion Techniques</u>

Tools like Nmap are not intended to be able to accurately depict the systems that intrusion prevention and firewalls are meant to protect. Nmap consists of a variety of features created to get over these barriers. The many evasion methods that Nmap includes are covered in this section.

“We are going to try different methods to evade the target server. Th target server we are going to use in this project is scanme.insecure.org. This server is designed to intake attacks. This server has firewall configured. We will use all the evasion techniques on this server. We are going to pull more information from this server by using the above methods.”

1. Fragment Packets
2. Specify a Specific MTU
3. Use a Decoy
4. Idle Zombie Scan
5. Manually Specify a Source Port
6. Append Random Data
7. Randomize Target Scan Order
8. Spoof MAC Address
9. Send Bad Checksums

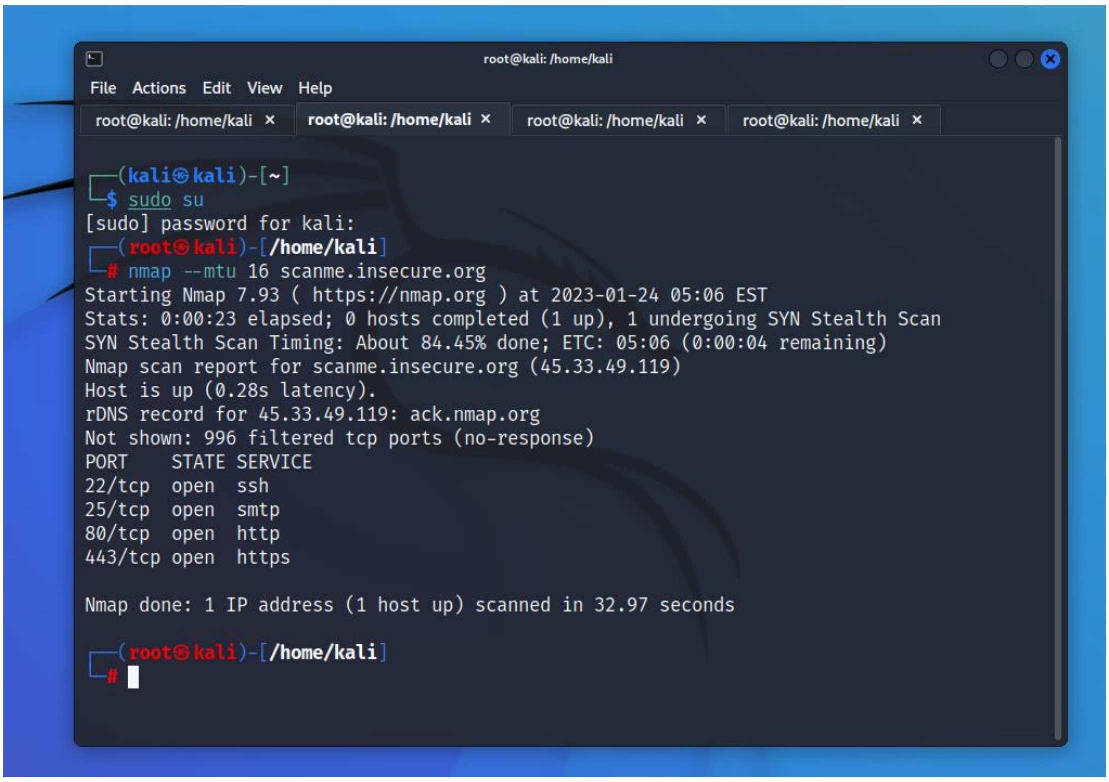
“From using all these methods,



```
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -f scanme.insecure.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 05:01 EST
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.00% done; ETC: 05:11 (0:08:56 remaining)
Stats: 0:02:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 22.00% done; ETC: 05:11 (0:07:34 remaining)
Stats: 0:03:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.00% done; ETC: 05:11 (0:06:04 remaining)
Stats: 0:03:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.50% done; ETC: 05:11 (0:06:02 remaining)
Stats: 0:08:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.00% done; ETC: 05:11 (0:00:58 remaining)
Nmap scan report for scanme.insecure.org (45.33.49.119)
Host is up (0.57s latency).
rDNS record for 45.33.49.119: ack.nmap.org
All 1000 scanned ports on scanme.insecure.org (45.33.49.119) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 578.50 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap --mtu 16 scanme.insecure.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 05:06 EST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.45% done; ETC: 05:06 (0:00:04 remaining)
Nmap scan report for scanme.insecure.org (45.33.49.119)
Host is up (0.28s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 32.97 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

Conclusion

This article is an effort to cover the most important aspects of Nmap from beginning to advanced so that everyone can learn even without previous knowledge. This is not the end because Nmap has a lot of features, you can do many things by using Nmap. I recommend you to practice with it every day because practice makes a man perfect.

In the above methods we have used

1. Fragment Packets
2. Specify a Specific MTU
3. Use a Decoy
4. Idle Zombie Scan
5. Manually Specify a Source Port
6. Append Random Data
7. Randomize Target Scan Order
8. Spoof MAC Address
9. Send Bad Checksums

"From using all these methods, we have got more port scanning information about the target. Still this server needs to be improvised. Thus, we have evaded the targeted machine."

REFERENCES

[1] Kahate, A. Cryptography and Network Security. ISBN-13: 978-0-07-064823-4, ISBN-10:0-07-64823-9, McGraw Hill Higher Education.

[2] Forouzan, B. A., & Mukhopadhyay, D. Cryptography and Network Security. ISBN-13:978-0- 07-70208-0, ISBN-10: 0-07-070208-X, Mc Graw Hill Higher Education.

[3] Stallings, W. Cryptography and Network Security Principlesand Practices. ISBN-978-81-775-8774-6.

[4] Tanenbaum, A. S., Watherall, D. J. Computer Networks. ISBN-13: 978-0132126953, ISBN-10: 0132126958, 5th Edition,Paperback, 2010, pp: 34-39.

[5] Rathod, R.H., & Deshmukh, Prof. V.M. (2013). Role ofDistributed Firewalls in Local Network for Data Security.International Journal of Computer Science and Applications, Vol.6, No. 2, Apr 2013, ISSN: 0974-011(open access), pp: 360-364.Retrieved from official website: www.researchpublications.org

[6] Zeng-gang, X., & Xue-min, Z. (2010). Research and Design on distributed Firewall based on LAN. Computer and Automation Engineering (ICCAE), 2010, E-ISBN: 978-1-4244-5586-7, Print

ISBN: 978-1-4244-5585-0, INSPEC Accession Number:11259785, DOI: 10.1109/ICCAE.2010.5451596, Publisher: IEEE,Singapore, pp: 517-520

[7] Patel, H. B., Patel, R. S., & Patel, J. A. (2011). Approach of Data Security in Local Network using Distributed Firewalls.International Journal of P2P Network Trends and Technology

(IJPTT),Vol. 1 Issue 3- 2011, ISSN: 2249-2615, pp: 26-29.Retrieved from: http://www.internationaljournalssrg.org

[8] Avolio, F. Firewalls and Internet Security, the Second Hundred(Internet) Years. The Internet Protocol Journal,Vol.2,No.2.Retrieved from official website of CISCO:http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html