Volume 7, Issue 5, May 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Design and Deployment of Secure Enterprise Network Framework

Komal
Department of CSE, Amity University, Haryana,
India

DOI: 10.23956/ijarcsse/V7I5/0102

Abstract— Network Security has always been the concern of the world since the invention of communication devices and computers. The absolute prevention of network attacks has not been successful till date. Several tools have been developed in order to detect possible intrusion attacks and network traffic monitoring such as Wireshark and Solarwinds, software and hardware firewalls, Intrusion Detection system (IDS) and Intrusion Prevention System (IPS). Besides this, the software that runs on the network hardware and possibly weak technical specifications and misconfigurations can be exploited for vulnerabilities. The paper aims to design and implement security concepts and tools which will enable enterprises and organizations to secure their networks from various threats and unauthorized access using traffic analysis and penetration testing

Keywords— Enterprise Network, Attacks, IDS, IPS, Traffic analysis, Firewalls, Penetration testing.

I. INTRODUCTION

In today's world of technological advancement, various technologies are being developed and implemented globally at an alarming rate. Most of these are implemented in Enterprises, Organizations and Institutions and for personal use by individuals. Each of the above stated categories seeks to connect or communicate with the other branches of their own situated or located at various parts of the world, for coordinating and delivering the desired output. This has contributed to the need for a network to connect them together for easy communication, sharing and transfer of data and information across the globe.

An enterprise network is a network that connects all resources and hosts in a large business organization to interconnect its various company sites (such as production sites, offices and shops) that spans across multiple geographic locations in order to share computer resources. The sharing of information and data is a necessity in day to day activities for an enterprise network. Some of the information shared is very sensitive and when gotten into the wrong hands can cause a lot of harm which makes it very important to secure the network with which it is shared. Networks should be able to provide the usability, reliability, integrity, and safety of the network and data [1]. A secure network seeks to defend and protect whatever goes into it, comes out of it, detect a variety of threats and stops them from having access or entering and spreading on the network.

When there is a secured network infrastructure in place, there are many benefits attributed to it. The company or enterprise is protected against disruptions in work and business, which increases employee's productivity. Network security also enables the organization to meet mandatory regulatory compliance. Since secured networks protect customers' data and other sensitive information, it reduces the risk of legal action from data theft. Ultimately, the reputation of the organization is protected, which is one of its most important assets.

This paper is structured as follows. Section 2 presents the design of enterprise network security framework. Section 3 highlights the vulnerabilities of current security framework by using traffic analysis tools and penetration testing. Section 4 concludes the paper with necessary findings.

II. DESIGN OF SECURITY FRAMEWORK FOR ENTERPRISE NETWORK

The initial requirements that are derived in the planning phase are used to drive the activities for the network security design. The network security design is a detailed design that meets current organizational and technical requirements, and also incorporates specifications to support availability, reliability, security and performance. The security design specification is the basis for the implementation activities. In the modular framework design and for maximum security of an organizational network, a topology based on the CCIE standard is designed as shown in fig. 1.

The designed network topology is a hub and spoke which consists of three sites which include one headquarters and two branch sites of an organization. The branches are communicating with the headquarters and each other over a public network or internet. At the headquarters, there are two firewalls. One is the default and the other acts as a failover. In case the default firewall goes down, the failover is supposed to take over the functions of the default with no delay. Two switches are used to connect the firewalls with the hub and edge router at the headquarters for effective routing purposes.

There are three edge routers one for each site which is responsible for routing the packets to the desired destination and also for some filtering purposes. The other two routers (known as the spokes) at the branch sites act as a server and clients respectively.

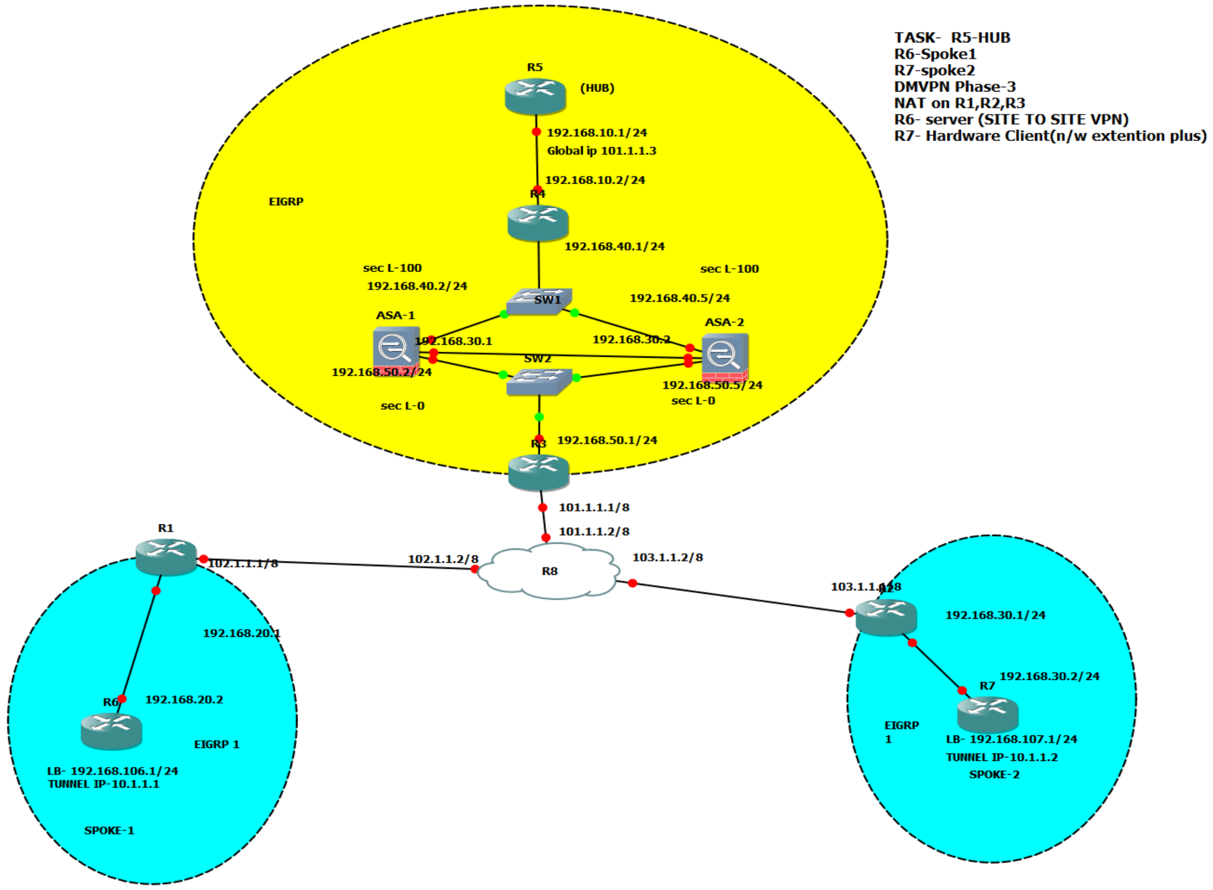


Fig. 1 Topological design of Enterprise Network Security Framework

A. *Branch Sites (Spokes)*

The two sites connect to each other over a public network. Site to site VPN is configured between the two to enable remote connection from one to another. Site to Site VPN connects LAN to LAN when an organization wants to connect multiple remote connections in one private network. The edge routers (spokes) have Access Control lists (ACLs) configured to specify which traffic to allow or deny based on port numbers and protocols. Pinging is blocked using the ACLs to prevent ping sweeps. It requires large scale encryption and dedicated equipment. Hence, Advanced Encryption standard (AES) and MD5 (Message Digest) hash algorithm is to be used.

B. *Headquarters (HUB)*

The edge router at the headquarters (hub) has Access Control lists (ACLs) configured to specify which traffic to allow or deny based on port numbers and protocols. Only telnet traffic has been permitted to flow through the edge routers. Network Address Translation (NAT) is configured on the edge router to protect the networks IP address from discovery by hackers.

Dynamic multipoint VPN (DMVPN) [2] is configured for the remote access and communication between the headquarters and the two branch sties. DMVPN is an effective solution for dynamic secure overlay networks. It is cisco’s answer to increasing demands of enterprise companies being able to connect branch offices with head offices and between each other whiles keeping costs low. It is a combination of various technologies which includes

- Multipoint GRE tunnel [3]: It allows a tunnel to have multiple destinations
- Next hop resolution protocol (NHRP) [4]
- Support for Dynamic routing protocols (EIGRP, RIP, OSPF, BGP)
- Cisco Express forwarding (CEF) [5]

The network security framework design has been built according to, with the goal of integrating hardware and software where relevant without disrupting the existing enterprise network functionality or creating points of vulnerability.

In the network, Enhanced Interior Gateway protocol (EIGRP) is used for all the routing between the headquarters and its branches. EIGRP is chosen due to its several benefits over other routing protocols such as RIP. These benefits includes fast convergence time, hybrid routing protocol, works better in large networks and efficient neighbor discovery.

III. TRAFFIC ANALYSIS AND PENETRATION TESTING

Operational phase is the final test of the appropriateness of the design. The operational phase involves maintaining network security health through day-to-day operations, including maintaining high availability and secure transmission of data and information. Some of the tools that were used for finding vulnerabilities in a network and also for traffic analysis on routine basis include:

A. Wireshark

Wireshark [7] is a free of cost and open source software used for analyzing packets. It is used for troubleshooting of network(s) , traffic analysis, and development of communications protocols in education sector. Wireshark uses QT widget, in current releases to implement its user interface and is cross-platform, and via the makes use of pcap to capture packets and can run on various operating systems like Windows ,Linux, , BSD, macOS, Solaris, and some other Unix-like operating systems, There is also a Non-GUI version which is terminal-based and is called TShark.

B. Metasploit pen test tool

The Metasploit pen test tool [6] is an open source computer security tool that entails information about security breaches and aids in penetration tests and Intrusion Detection Systems signature creation.Its proprietary and most important Metasploit Framework, is a tool for exploiting code versus a remote target machine. Other important systems encompasses the shellcode archive ,Opcode Database and related research.

C. Putty software

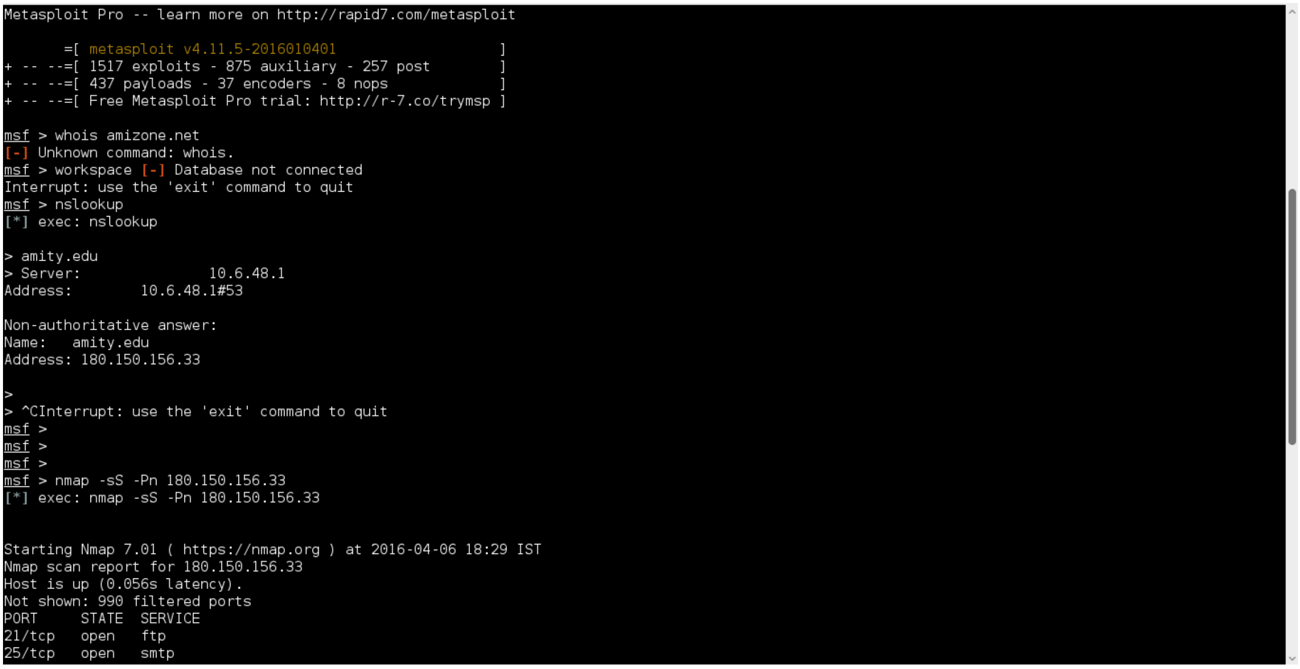
Putty [8] is another free and open-source software that acts as terminal emulator and network file transfer application. It provides support for number of network protocols, including SSH, Telnet and many variations of SSH too. It can also connect to a serial port and provides user control over the SSH encryption key and provides local, remote, or dynamic port forwarding with SSH.

D. Penetration testing[9]

This phase involves proactive management of the network security. The goal of proactive management is to identify and resolve issues before they affect the organization. Reactive fault detection and correction (troubleshooting) is needed when proactive management cannot predict and mitigate failures. Performing penetration vulnerability scanning on daily basis will prevent the network from succumbing to various threats. Following tools and commands can be used for penetration testing:

- **Passive Information Gathering-**

By using passive and indirect information gathering, you can discover information about targets without touching the systems. By using nslookup tool, the detailed non –authoritative information about a network which includes server IP address or mail exchanger address depending on the type of server as shown in fig. 2

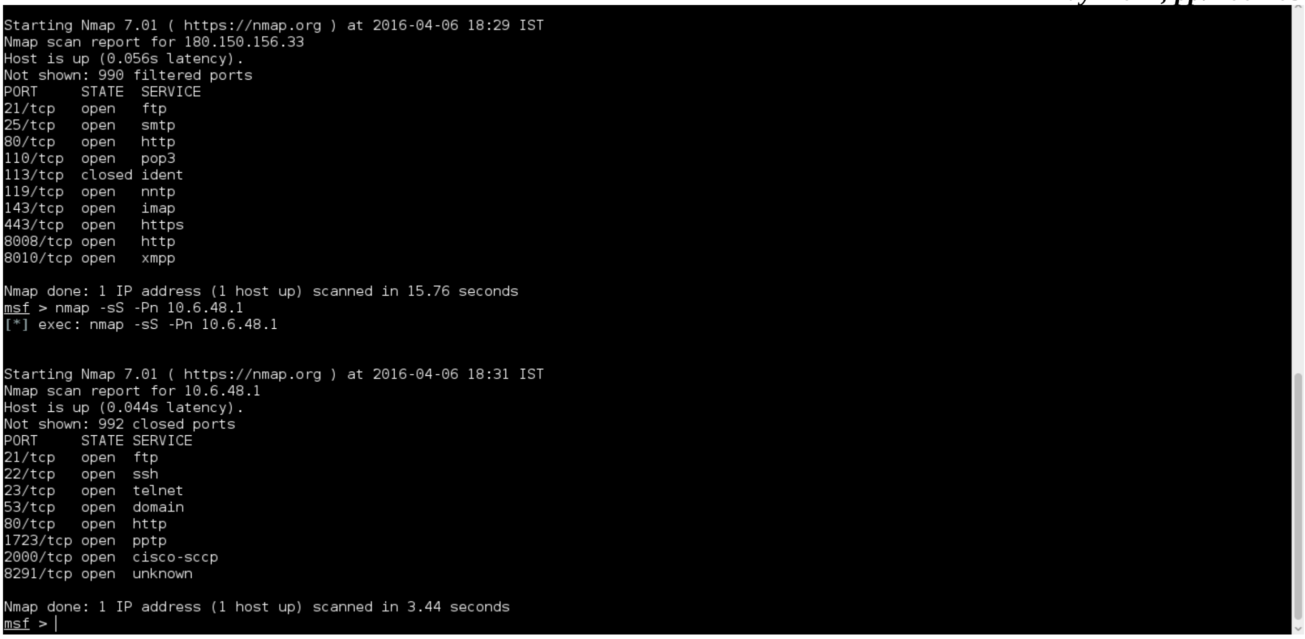


```
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > whois amizone.net
[-] Unknown command: whois.
msf > workspace [-] Database not connected
Interrupt: use the 'exit' command to quit
msf > nslookup
[*] exec: nslookup

> amity.edu
> Server:               10.6.48.1
Address:        10.6.48.1#53

Non-authoritative answer:
Name:   amity.edu
Address: 180.150.156.33

>
> ^CInterrupt: use the 'exit' command to quit
msf >
msf >
msf >
msf > nmap -sS -Pn 180.150.156.33
[*] exec: nmap -sS -Pn 180.150.156.33


Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-06 18:29 IST
Nmap scan report for 180.150.156.33
Host is up (0.056s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
```

Fig. 2 Passive Information gathering using "nslookup"

- **Active information gathering-**

After getting the target IP from the passive information gathering, the system is interacted with directly to get more information about it. Port scanning using Nmap tool is used to scan for vulnerabilities like open ports as in fig. 3.



```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-06 18:29 IST
Nmap scan report for 180.150.156.33
Host is up (0.056s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
80/tcp   open   http
110/tcp  open   pop3
113/tcp  closed ident
119/tcp  open   nntp
143/tcp  open   imap
443/tcp  open   https
8008/tcp open   http
8010/tcp open   xmpp

Nmap done: 1 IP address (1 host up) scanned in 15.76 seconds
msf > nmap -sS -Pn 10.6.48.1
[*] exec: nmap -sS -Pn 10.6.48.1


Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-06 18:31 IST
Nmap scan report for 10.6.48.1
Host is up (0.044s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
1723/tcp open  pptp
2000/tcp open  cisco-sccp
8291/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds
msf > |
```

Fig. 3 Active Information gathering using “nmap”

IV. CONCLUSIONS

The framework proposed for securing enterprise networks has been found successful for identifying vulnerabilities within the network technology implementation device configurations, open ports and for traffic analysis using penetration testing and other ethical hacking tricks. The framework provides clear understanding of all security measures and technologies to be used for establishing secure communication over an enterprise network infrastructure. Network security will continue to be a major area of concern. With new deployments and upcoming technologies, enterprises need to be abreast with all of them. Security Policies must be renewed or updated at required intervals without neglecting securing network devices physically and logically.

REFERENCES

[1] Komal, *Compromised Security of Wireless Ad-hoc Networks & its implications*, International Journal of Computer Applications, Cognition 2015, pp.25-30, 2015.

[2] *Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T*, Cisco Systems, 2017.

[3] (2017) The Cisco website [Online]. Available:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15_0_sy_swcg/L2omGRE.pdf.

[4] (2017) The Cisco website [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html

[5] (2017) The Cisco website [Online]. Available: http://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-3/addr_serv/configuration/guide/b_ipaddr_cg43xcrs/b_ipaddr_cg42crs_chapter_011.pdf.

[6] D. Kennedy, J. O’Gorman, D. Kearns and M. Aharone, *Metasploit the penetration testers guide.*

[7] (2017) The Wireshark website [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/Chapter Introduction.html.

[8] (2017) The Wikipedia website [Online]. Available: https://en.wikipedia.org/wiki/PuTTY

[9] G. Weidman, *Penetration Testing*, No starch Press, San Fransico, 2014.