International Journal of Research in Engineering, Science and Management
Volume-3, Issue-6, June-2020
www.ijresm.com | ISSN (Online): 2581-5792

Study and Comparison of Networking Tools Used by Industries in Real World Applications

Harshit Pandey*
Student, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
*Corresponding author: harshit.pandeyofficial@gmail.com

***Abstract*: The cyber security is one of the most booming fields right now. Now more than ever industries are focusing on using various tools to keep their applications secure. Every day industries faces various vulnerabilities on real world applications for which they use different tools. In this study we will focus on three of the most important tools used by these industries and make a comparative conclusion for the same. Specifically, these tools are often used by the Cyber security specialists of these industries which helps them to detect various vulnerabilities which are affecting the security of the particular application. We will be using tools line Nmap, SQLMap and Acunetix on a particular problem and analyse their advantages and disadvantages over the other tools.**

***Keywords*: Cyber, Security, Nmap, SQLMap, Acunetix.**

1. Introduction

Cyber security has been used interchangeably for information security, where later considers the role of the human in the security process while former consider this as an additional dimension and also, focus person has a potential target [1]. As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude of activities whose loss would all but cripple these organizations. As a consequence, cybersecurity issues have become national security issues. Protecting the Internet is a difficult task. Cybersecurity can be obtained only through systematic development; it cannot be achieved through haphazard seat-of-the-pants methods. Applying software engineering techniques to the problem is a step in the right direction. However, software engineers need to be aware of the risks and

security issues associated with the design, development, and deployment of network-based software. This paper introduces some known threats to cybersecurity, categorizes the threats, and analyzes protection mechanisms and techniques for countering the threats. Approaches to prevent, detect, and respond to cyber-attacks are also discussed [2]. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc. also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing [3]. Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber-form [3]. There will benew attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security [3].

2. Nmap Security Tool

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping) [4]. The output from Nmap is a list of scanned targets, with

supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state [5]. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open filtered and closed filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (**-sO**), Nmap provides information on supported IP protocols rather than listening ports [5]. In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

3. SQLMap Penetration Tool

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections. SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection [6].

4. Acunetix Security Tool

Website security is today's most overlooked aspect of securing an enterprise and should be a priority in any organization. Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites. A victim's website can be used to launch criminal activities such as hosting phishing sites or to transfer illicit content, while abusing the website's bandwidth and making its owner liable for these unlawful acts.Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits. The hacking community is also very close-knit; newly discovered web application intrusions, known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. Postings are updated daily and are used to propagate and facilitate further hacking. Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data.

If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyber-attacks are done at the web application level.

5. Results

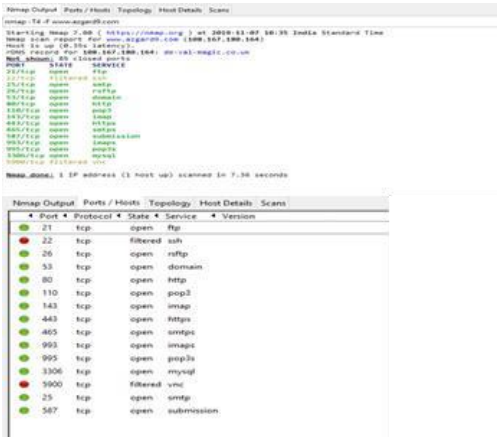

Fig. 1. Nmap Tcp/Ip call

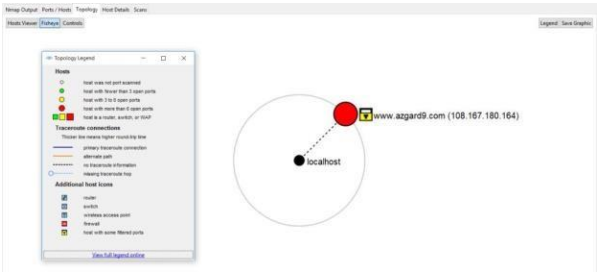

Fig. 2. Nmap topology

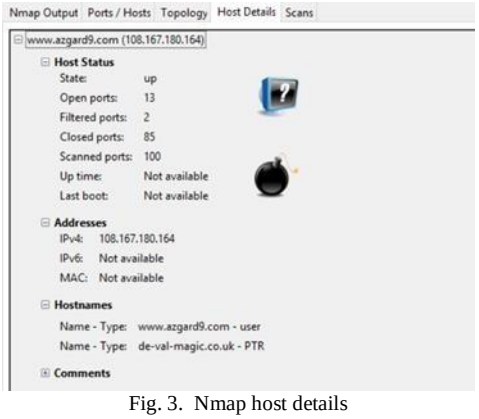

Fig. 3. Nmap host details

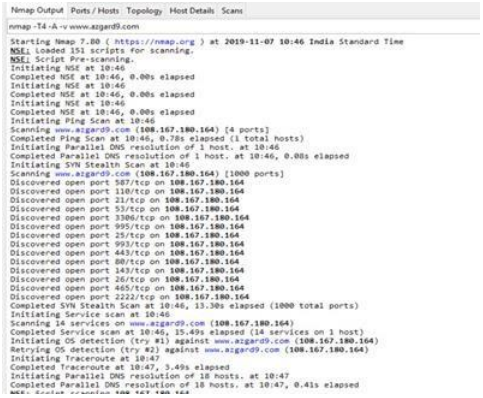

Fig. 4. Nmap intense scan output

Fig. 5. Nmap intense scan output

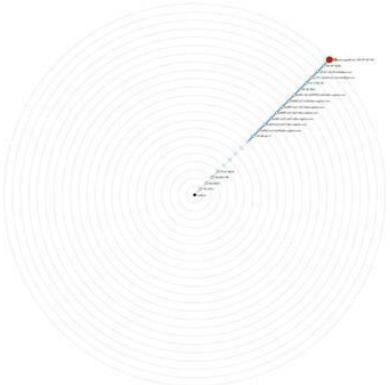

Fig. 6. Nmap topology map

Fig. 7. SqlMap Introduction

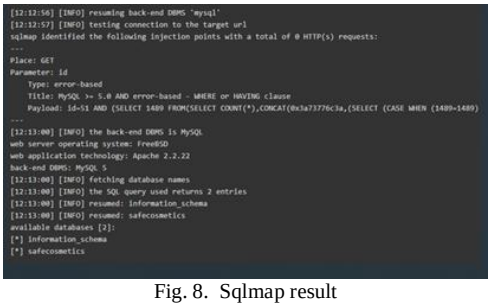

Fig. 8. Sqlmap result

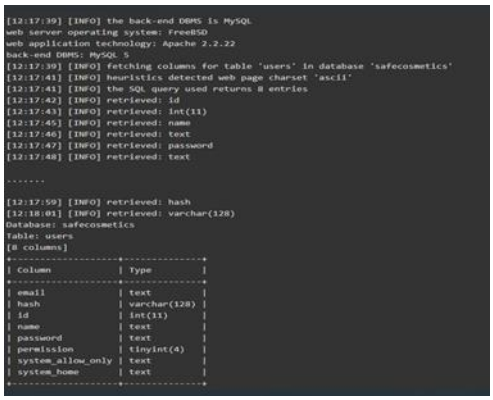

Fig. 9. Sqlmap result

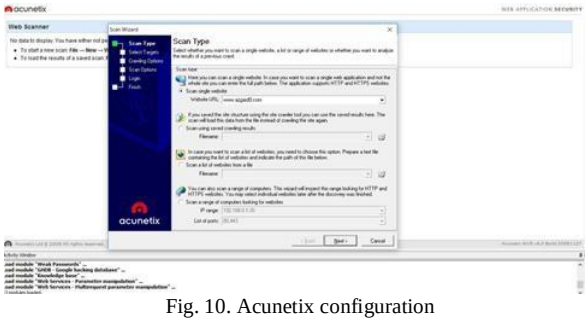

Fig. 10. Acunetix configuration

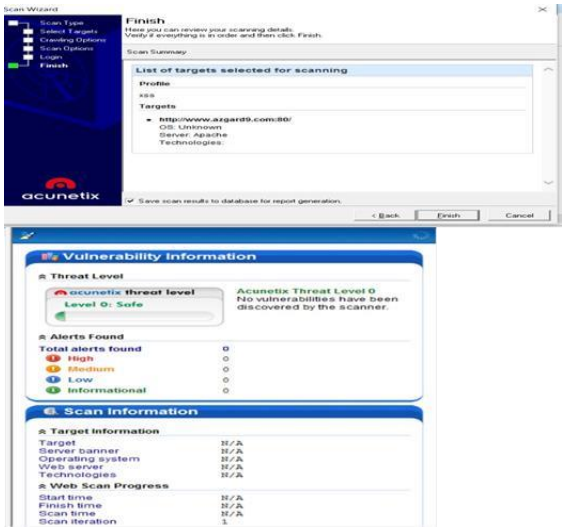

Fig. 11. Acunetix report

6. Conclusion

From the above results of the cyber security tools used by industries we come to a conclusion where Acunetix is the clear winner among all. Its fast and easy to use which can not only be used by industries but also by various individuals who are working as freelancers. So Acunetix is clearly the best among them and also in the market with other tools.

References

[1] W. R. Bevier, "Kit: a study in operating system verification," in *IEEE Transactions on Software Engineering*, vol. 15, no. 11, pp. 1382-1396, Nov. 1989.

[2] R. A. Kemmerer, "Cybersecurity,"*25th International Conference on Software Engineering, 2003. Proceedings.*, Portland, OR, USA, 2003, pp. 705-715.
[3] Gade, Nikhita Reddy and Reddy, Ugander, "A Study of Cyber Security Challenges and its Emerging Trends On Latest Technologies," 2014.
https://nmap.org/
[4] https://www.systutorials.com/docs/linux/man/1-nmap/
[5] https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/
[6] https://www.acunetix.com/support/docs/introduction/