1st International Conference on Computational Intelligence and Sustainable Engineering Solution(CISES-2022)

An Analysis of Vulnerability Scanners in Web Applications for VAPT

2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) | 978-1-6654-8004-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/CISES54857.2022.9844365

Ashish Joshi
Security Consultant
Bosch
Banglore, India
a.joshicse1986@gmail.com, 0000-0002-0302-2569

Aditya Raturi
Security Consultant
Bosch
Banglore , India
Addy3177@gmail.com,0000-0002-0986-0248

Santosh Kumar
Security Consultant
Bosch
Banglore,India
santosh51623z@gmail.com,0000-0001-9819-6758

***Abstract*—Though the development in cybersecurity for protecting the websites and applications are growing rapidly, the attacks on these crucial websites are still happening. Irrespective of the development of society, third-party attacks would always increase correspondingly. To protect these websites and web applications, the developers would always use defensive mechanisms to survive third party attacks. But the reliability of the website's strength against third party attacks depends on several factors. Intruders are now using automated structures in form of BOTS, AI, ML, to perform these attacks.**

Need of security arises from the initial stages of planning and development. As part of SEP (Security Engineering Process) defined by individual vendors and companies for securing the system and performing risk analysis, Vulnerability Analysis are essential as part of standard procedures. Apart from SEP, VAPT (Vulnerability Analysis and Penetration Testing) now forms the standard operating measures for prevention of intrusion activities. We hereby focus on various vulnerability analysis tools forming basis for vulnerability analysis and Penetration testing (VAPT) for short and try to analyze the various impact with respect to stages of penetration testing.

Keywords— Vulnerability Analysis, Reconnaissance, foot printing, spoofing, enumeration, Sniffing, NIST 800-300, CVSS

I. INTRODUCTION AND BACK GROUND

Vulnerabilities are the gateways through which threats arise. Vulnerabilities are security flaws in a system's architecture. It's the flaws that come with systems, web apps, and even network design. Vulnerabilities provide an opportunity for system exploitation.[1]

Vulnerability and threat to a system especially web applications may result in leakage of sensitive information measure of parameters affected are in form of *confidentiality* (disclosure of information to untrusted parties), *availability* (data readily available as and when required by authorized users), *integrity* (data to be protected from unreliable and unauthorized amendments) [2]. An external entity like hacker, cracker, hacktivist may try to exploit the various vulnerabilities inside the system and try to compromise the system for personal interest and sometimes for knowledge.

As a result, safeguarding web apps is one of the most important assignments at the present time: according to an Acunetix survey, 60% of discovered vulnerabilities affect web applications. Searching for and eliminating vulnerabilities on web is the most common approach of safeguarding them. Safe online application development, as well as implementing intrusion prevention system and/or prevention technologies, are examples of additional ways to secure web applications. [5,6].

Vulnerability Scanning and penetration testing (VAPT for short) now forms an essential component of improving the quality and security of your product. The product quality is nowadays emphasised on security parameters as well regarding of what the end product will look alike whether it is hardware software and web application or any another form but due to increase in attacks and also connectivity security audits on all of them the need to be performed before going live on any platform.

Due to such increase in attacks the compliance related parameters and Laws for affecting the privacy of personal data and other sensitive information like medical history and phone number email and have significantly been changed and will be possible to amended in near feature too depending on the attack factors. We as an Author try to highlight some of the general issues which can be encountered by using some of the open-source tools only. [3,4]

Our paper will be focused on Vulnerability assessment and penetration testing techniques although vulnerability analysis seeks information about vulnerabilities in known packages and software and penetration testing tries to exploit weakness in structure or environment there are many of the sources available to perform such actions. An attacker may use any of the known mechanisms to exploit those or may include his/her own mechanism to perform actions as spoofing denial of Service etc. thinking of such a changing scenario, we consider this field as quite an emerging one and important to consider.

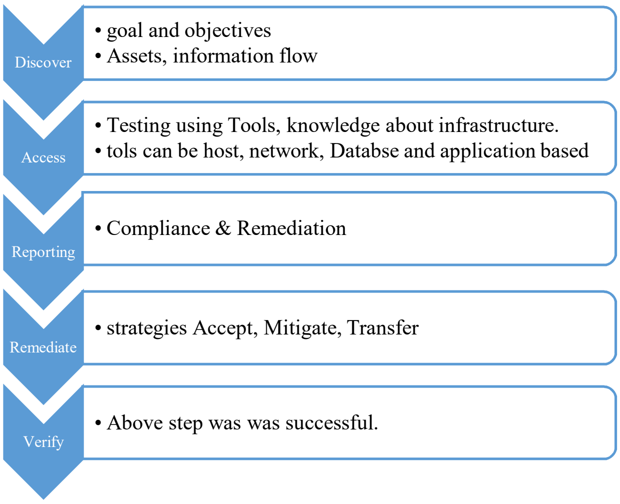
The tools mechanisms for vulnerability detection or pen test discussed here can be in either of the following phases and falls under the scope of our discussion in our Research study conducted. The zones/ phases discussed here are taken as general (who are likely to be there inside any organization) but they are not limited to for the same usage. They can have addition layers which we consider as out of scope for our discussion.

1. **External:** here we are connected to external network any firewall misconfiguration or usage of outdated components can lead to exposure to exploitation of certain vulnerabilities.
2. **Demilitarized Zone:** in this zone generally the web servers etc are placed.

3. **Internal:** This phase covers information extraction through social engineering techniques or computer worms. These are considered as basically insiders who have some concern about their organization and are trying to harm their organization itself.

II. METHODOLOGY AND SCOPE FOR VULNERABLITY ANALYSIS

Vulnerability analysis tries to find out the known Vulnerability inside the system it is one of the most critical components in performing wonder ability assessment and penetration testing. [11,12,13,14,15] To sum up we can divide the process of Vulnerability analysis in following Phases: -


Discover
• goal and objectives
• Assets, information flow
Access
• Testing using Tools, knowledge about infrastructure.
• tols can be host, network, Databse and application based
Reporting
• Compliance & Remediation
Remediate
• strategies Accept, Mitigate, Transfer
Verify
• Above step was was successful.

a. **Discover:** it involves determine the scope of vulnerability analysis (VA) also forms basics for Penetration test activities.

b. **Access:** In this step we use various tools like ZAP, Burp and can perform an automated scan of our target can be done in either of forms like

c. **Black Box** (no access to target), Black box testing, also known as Dynamic Analysis Security Testing (DAST test), is a critical component of application security. Black box evaluation is done out in real time, identifying vulnerabilities that an adversary could exploit while the programme is in use.

d. **White Box** (authorized access to whole of infrastructure and code) the tester in this case will be authorized to see or use the resources available in web applications (in our case)

e. **Grey box** (limited access to resources) in grey box testing method the tester have some access to limited resources to the system unlike to white box and black box testing mechanisms this term has much wider and practical relevance to internal pentesters.

f. **Reporting:** this step involves the exhaustive summary of the above step including the compliance like OWASP ISO to be filter out. Remediation measures to be provided in this step

g. **Remediate:** after having the remediate step you can perform either of the following:

1. **Accept:** this can be followed if some of cost-based parameters are involved or risk of exploiting the vulnerability is quite high.
2. **Transfer:** may involve transfer to a third-party application if involved or any other internal party.
3. **Mitigate:** try to remove the vulnerability within the system. Possible mitigations here include fixing vulnerability via patch level update or upgrading the version etc.

h. **Verify:** Verify all the remediation steps are successful and implemented. Verification is quite important as it provides you the feedback of the mitigation measures.

There are many of open-source tools like Zap Burp available to perform vulnerability scan and provide the mitigation measures [7,8,9].

III. PENETRATION TESTING PT

Penetration testing as term suggests we try to exploit vulnerabilities in network, computer systems, applications for penetration testing vulnerability scanning might be considered as it facilitates the pen testing process. As penetration testing may involve lot of legal issues its quite important to note here that we have form a general agreement between the connected parties eg the pen testers and the client on which the pen testing has to be performed [10,16]. We can broadly classify the Phases of pen testing as follows *figure 1*: -

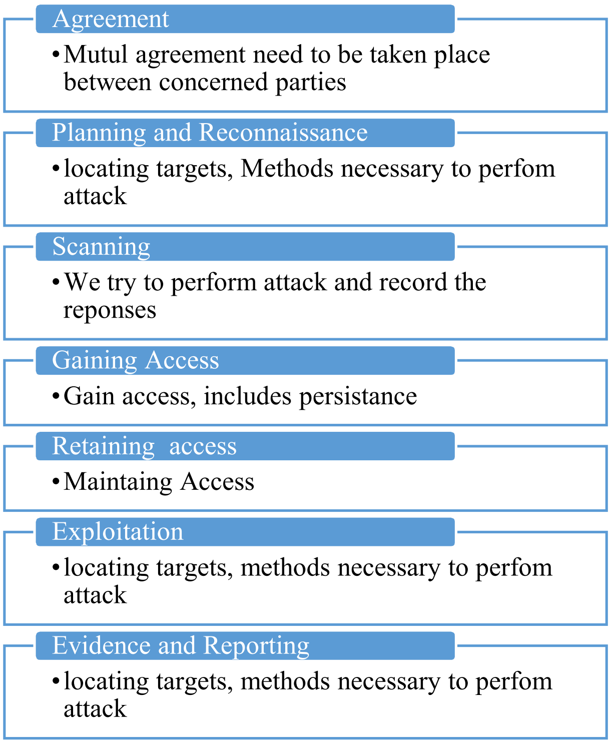

Agreement
• Mutul agreement need to be taken place between concerned parties
Planning and Reconnaissance
• locating targets, Methods necessary to perfom attack
Scanning
• We try to perform attack and record the reponses
Gaining Access
• Gain access, includes persistance
Retaining access
• Maintaing Access
Exploitation
• locating targets, methods necessary to perfom attack
Evidence and Reporting
• locating targets, methods necessary to perfom attack

Fig 1: All Phases of Penetration Testing

1. **Agreement:** As Penetration testing may involves lot of offensive approaches an agreement between the connected parties needs to be come out.
2. **Planning and Reconnaissance** involve information collection

a. Physical location of target

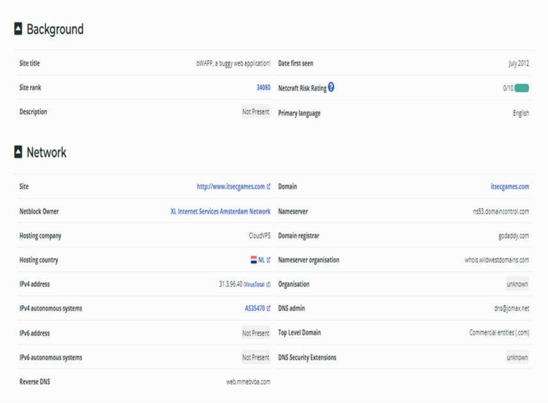
b. Data OS, hardware configuration

c. Services, Phone list

d. Sniffing

e. Information extraction through social engineering (include Impersonation, intrusion reverse social Engineering), Dumpster Diving internet foot printing, search Engines as shown in Figure 2,3.

Planning and reconnaissance phase mainly focus on information gathering about the target can be used as source of exploitation.


Background

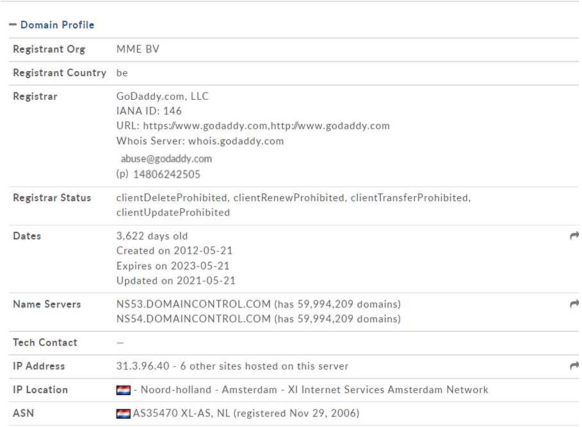
Site title	bWAPP, a buggy web application!	Date first seen	July 2012
Site rank	34080	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network

Site	http://www.itsecgames.com	Domain	itsecgames.com
Netblock Owner	XL Internet Services Amsterdam Network	Nameserver	ns53.domaincontrol.com
Hosting company	CloudVPS	Domain registrar	godaddy.com
Hosting country	NL	Nameserver organisation	whois.wildwestdomains.com
IPv4 address	31.3.96.40 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS35470	DNS admin	dns@jomax.net
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	web.mmebvba.com		

Fig2. Net craft showing site information for information gathering.

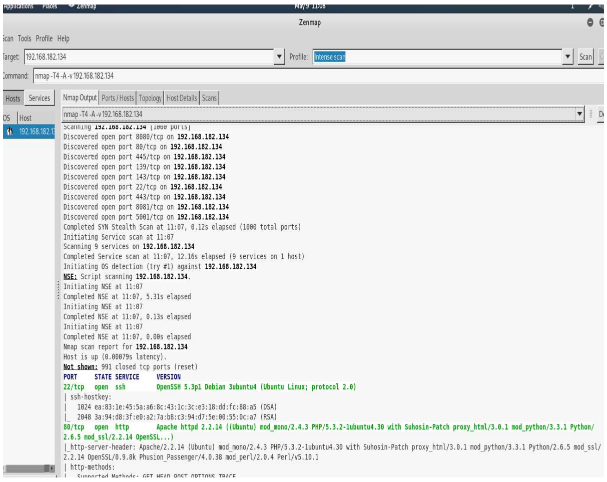
Tools like netcraft (*figure 2*) can be of great practical importance as it provides hosting/ network details as well as the background of the target. Apart from this netcraft can we used to wide range of attacks related to cybercrime and threat level scenarios.


Domain Profile

Registrant Org	MME BV
Registrant Country	be
Registrar	GoDaddy.com, LLC IANA ID: 146 URL: https://www.godaddy.com,http://www.godaddy.com Whois Server: whois.godaddy.com abuse@godaddy.com (p) 14806242505
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	3,622 days old Created on 2012-05-21 Expires on 2023-05-21 Updated on 2021-05-21
Name Servers	NS53.DOMAINCONTROL.COM (has 59,994,209 domains) NS54.DOMAINCONTROL.COM (has 59,994,209 domains)
Tech Contact	–
IP Address	31.3.96.40 - 6 other sites hosted on this server
IP Location	- Noord-holland - Amsterdam - XI Internet Services Amsterdam Network
ASN	AS35470 XL-AS, NL (registered Nov 29, 2006)

Fig 3 who is domain showing same site information

Whois *figure 3* another tool can be used as same the netcraft and can provide the reliable information on the target in who is websites you will be able to see information as IP owner information.



Target: 192.168.182.134
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.182.134

```
nmap -T4 -A -v 192.168.182.134
Scanning 192.168.182.134 [1000 ports]
Discovered open port 8080/tcp on 192.168.182.134
Discovered open port 80/tcp on 192.168.182.134
Discovered open port 445/tcp on 192.168.182.134
Discovered open port 139/tcp on 192.168.182.134
Discovered open port 143/tcp on 192.168.182.134
Discovered open port 22/tcp on 192.168.182.134
Discovered open port 443/tcp on 192.168.182.134
Discovered open port 8081/tcp on 192.168.182.134
Discovered open port 5001/tcp on 192.168.182.134
Completed SYN Stealth Scan at 11:07, 0.12s elapsed (1000 total ports)
Initiating Service scan at 11:07
Scanning 9 services on 192.168.182.134
Completed Service scan at 11:07, 12.16s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 192.168.182.134
NSE: Script scanning 192.168.182.134.
Initiating NSE at 11:07
Completed NSE at 11:07, 5.31s elapsed
Initiating NSE at 11:07
Completed NSE at 11:07, 0.13s elapsed
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Nmap scan report for 192.168.182.134
Host is up (0.00079s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/
2.6.5 mod_ssl/2.2.14 OpenSSL...)
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/
2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
```

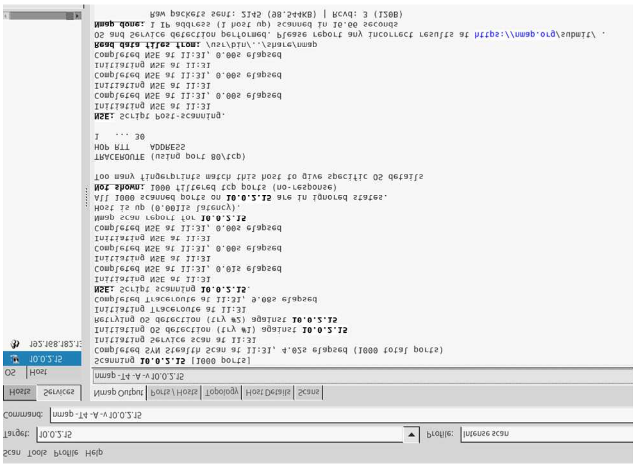
Fig4: Zen Map used to list out various discovered ports and other details in OWASP Broken Web APPS machine

Zenmap as shown in *figure 4* and *figure 5* is very useful tools in gaining information in terms of Network Exploitation and open ports including the Host details. It is more refined version of Nmap an open-source tool for network exploration and security auditing. It uses the UI features for Nmap also it provides an tool for running Nmap commands

It can also be used for various reasons such as: -

a. Operating system and versions
b. List of open ports
c. Services
d. Monitoring
e. Network inventory kind of tasks

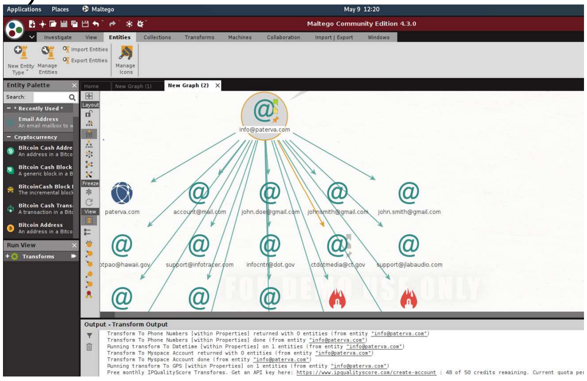
Nmap is very powerful is considered as essential for performing basic scanning it uses basic set of input parameters and has proven to be fast and accurate.



Target: 10.0.2.15
Profile: Intense scan
Command: nmap -T4 -A -v 10.0.2.15

```
nmap -T4 -A -v 10.0.2.15
Scanning 10.0.2.15 [1000 ports]
Completed SYN Stealth Scan at 11:31, 4.02s elapsed (1000 total ports)
Initiating Service scan at 11:31
Initiating OS detection (try #1) against 10.0.2.15
Retrying OS detection (try #2) against 10.0.2.15
Initiating Traceroute at 11:31
Completed Traceroute at 11:31, 9.08s elapsed
NSE: Script scanning 10.0.2.15.
Initiating NSE at 11:31
Completed NSE at 11:31, 0.01s elapsed
Initiating NSE at 11:31
Completed NSE at 11:31, 0.00s elapsed
Initiating NSE at 11:31
Completed NSE at 11:31, 0.00s elapsed
Nmap scan report for 10.0.2.15
Host is up (0.0011s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using port 80/tcp)
HOP RTT    ADDRESS
1   ... 30

NSE: Script Post-scanning.
Initiating NSE at 11:31
Completed NSE at 11:31, 0.00s elapsed
Initiating NSE at 11:31
Completed NSE at 11:31, 0.00s elapsed
Initiating NSE at 11:31
Completed NSE at 11:31, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.66 seconds
           Raw packets sent: 2145 (98.544KB) | Rcvd: 3 (120B)
```

Fig5: ZenMap used to list out various discovered ports and other details in Bulldog machine



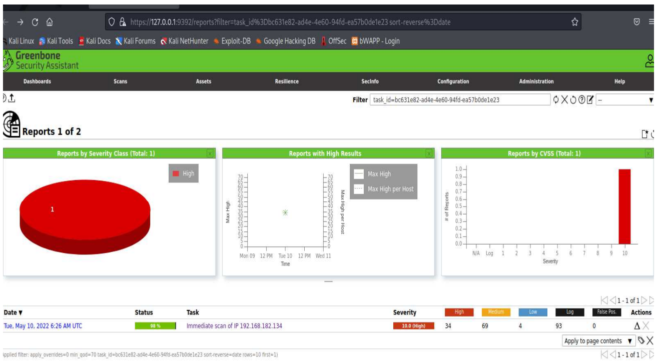
```
Transform To Phone Numbers [within Properties] returned with 0 entities (from entity "info@paterva.com")
Transform To Phone Numbers [within Properties] done (from entity "info@paterva.com")
Running transform To Datetime [within Properties] on 1 entities (from entity "info@paterva.com")
Transform To Myspace Account returned with 0 entities (from entity "info@paterva.com")
Transform To Myspace Account done (from entity "info@paterva.com")
Running transform To GPS [within Properties] on 1 entities (from entity "info@paterva.com")
Free monthly IPQualityScore Transforms. Get an API key here: https://www.ipqualityscore.com/create-account : 48 of 50 credits remaining. Current quota per
```

Fig 6: Maltego used to exploit using email address

Maltego *figure 6* another open-source tool and commercial version (for the study purposes we use open source version) uses OSINT (Open Source Security Intelligence) and used graphical link analysis for connection related information. Maltego is available on wide list on platforms as Windows, Linux etc and is efficient against connected information. The connected information may be in terms of email, phone numbers.

3. **Scanning:** This phase includes details gathered in reconnaissance and scan the network may be considered as active reconnaissance but involves vulnerability scanners port scanners etc to perform attack. In addition to that scanning network form a quite important and crucial role in identifying packets format eg. TCP or IP, communication.

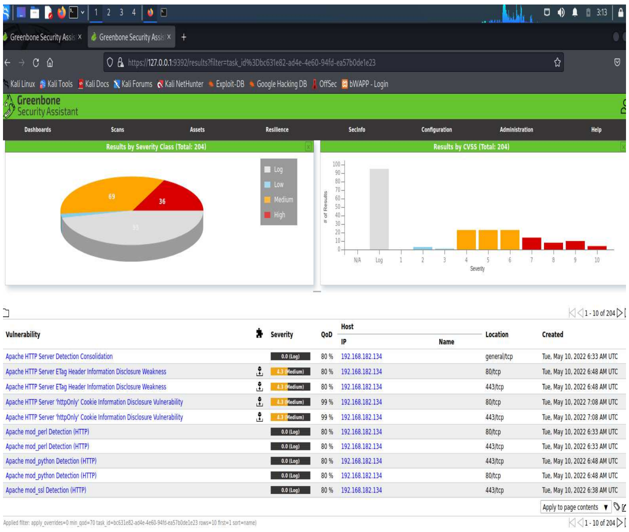
   Greenbourne from 2006 has developed a full feature vulnerability scanner known as Open VAS *figure 7* and *figure 8* for testing vulnerabilities inside a web application or web server. The database here is updated on feed provided by open VAS also it supports the authenticated crawl and auditing actives like as used in burp suite.



Date ▾	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Tue, May 10, 2022 6:26 AM UTC	98 %	Immediate scan of IP 192.168.182.134	10.0 (High)	34	69	4	93	0	

Applied filter: apply_overrides=0 min_qod=70 task_id=bc631e82-ad4e-4e60-94fd-ea57b0de1e23 sort-reverse=date rows=10 first=1)

Fig 7: Vulnerability scan report using open VAS scanner denoting the severity

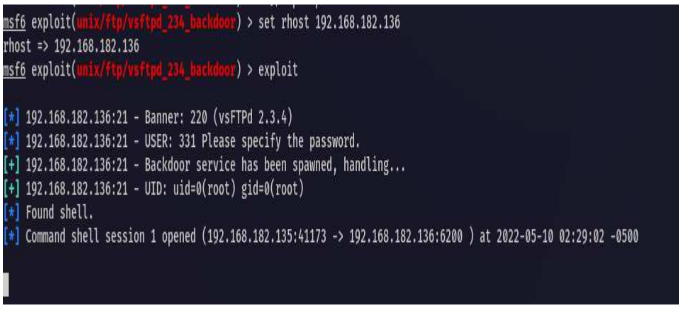


Vulnerability		Severity	QoD	Host IP	Host Name	Location	Created
Apache HTTP Server Detection Consolidation		0.0 (Log)	80 %	192.168.182.134		general/tcp	Tue, May 10, 2022 6:33 AM UTC
Apache HTTP Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80 %	192.168.182.134		80/tcp	Tue, May 10, 2022 6:48 AM UTC
Apache HTTP Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80 %	192.168.182.134		443/tcp	Tue, May 10, 2022 6:48 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99 %	192.168.182.134		80/tcp	Tue, May 10, 2022 7:08 AM UTC
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99 %	192.168.182.134		443/tcp	Tue, May 10, 2022 7:08 AM UTC
Apache mod_perl Detection (HTTP)		0.0 (Log)	80 %	192.168.182.134		80/tcp	Tue, May 10, 2022 6:33 AM UTC
Apache mod_perl Detection (HTTP)		0.0 (Log)	80 %	192.168.182.134		443/tcp	Tue, May 10, 2022 6:33 AM UTC
Apache mod_python Detection (HTTP)		0.0 (Log)	80 %	192.168.182.134		443/tcp	Tue, May 10, 2022 6:48 AM UTC
Apache mod_python Detection (HTTP)		0.0 (Log)	80 %	192.168.182.134		80/tcp	Tue, May 10, 2022 6:48 AM UTC
Apache mod_ssl Detection (HTTP)		0.0 (Log)	80 %	192.168.182.134		443/tcp	Tue, May 10, 2022 6:38 AM UTC

Applied filter: apply_overrides=0 min_qod=70 task_id=bc631e82-ad4e-4e60-94fd-ea57b0de1e23 rows=10 first=1 sort=name)

Fig 8: Vulnerability scan report using open VAS scanner denoting the severity -detailed assessment

4. **Gaining Access:** attacker use output received form step 2 and 3 to get into the system and network. several of the existing mechanisms are WEP cracking, ARP request replay All the Exploitation mechanisms seems to be beyond the scope of the current research but several of the tools like Metasploit are found eligible to gain access to certain specified network. *figure 9*



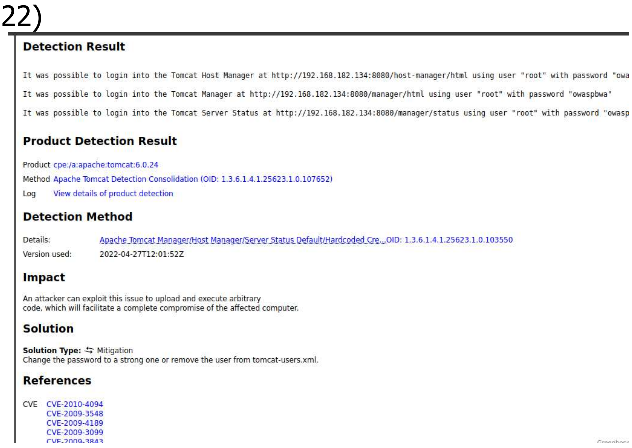
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.182.136
rhost => 192.168.182.136
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.182.136:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.182.136:21 - USER: 331 Please specify the password.
[+] 192.168.182.136:21 - Backdoor service has been spawned, handling...
[+] 192.168.182.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.182.135:41173 -> 192.168.182.136:6200 ) at 2022-05-10 02:29:02 -0500
```

Fig 9: using Metasploit for gaining access to system using payload options

5. **Maintains access** Attacker try to maintain access over a longer duration of time and try to explore more resources inside the systems.

6. **Exploitation:** Exploitation can be done using burp suite Metasploit, Wireshark (for network packets), Hydra, Burp Suite etc. as shown in *figure 9*

7. **Evidence and Reporting:** This phase highlights the number of vulnerabilities listed in previous steps. Helps to provide a mitigation measure to appropriate levels of organization as shown in *figure 10.*



Detection Result

```
It was possible to login into the Tomcat Host Manager at http://192.168.182.134:8080/host-manager/html using user "root" with password "owa
It was possible to login into the Tomcat Manager at http://192.168.182.134:8080/manager/html using user "root" with password "owaspbwa"
It was possible to login into the Tomcat Server Status at http://192.168.182.134:8080/manager/status using user "root" with password "owasp
```

Product Detection Result

Product cpe:/a:apache:tomcat:6.0.24
Method Apache Tomcat Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.107652)
Log View details of product detection

Detection Method

Details: Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Cre...OID: 1.3.6.1.4.1.25623.1.0.103550
Version used: 2022-04-27T12:01:52Z

Impact

An attacker can exploit this issue to upload and execute arbitrary
code, which will facilitate a complete compromise of the affected computer.

Solution

Solution Type: Mitigation
Change the password to a strong one or remove the user from tomcat-users.xml.

References

CVE CVE-2010-4094
CVE-2009-3548
CVE-2009-4189
CVE-2009-3099
CVE-2009-3843

Fig 10 a sample of result obtained by using open VAS tool.

IV. Results and Discussions

Vulnerability scan tools provide a great help in finding the vulnerability. However, the occurrence of false positives, Mitigation measures quality of detection classifying one vulnerability into high medium low is a big concern to provide a solution to vulnerability. A mixture of automatic and manual analysis is to be taken into consideration.[18,19}

We can consider the following points as conclusion for our conducted research

1. *Selection of tools:* Initial stages of penetration testing require identification of different vulnerabilities so identification of relevant scanning tool will make quite a lot of difference here many of the tools are including the false positives and does not provide a wider scope for search. At the initial stages vulnerability, you might consider all the possible one which is inside the system but during the assessment phase it might be difficult for you to filter out many of the possible false positives it requires lots of manual testing process for verification and validation purposes and may be hard to diagnose if the list is quite large. The selection of tools also differs since your target annual compliance for example OWASP so here we consider all of the compliance related parameters and the possible results obtained after performing a Vulnerability scan

2. *Scoring for threat:* vulnerabilities scanning tools may produce some form of output on the basis of severity of a particular threat for example, you may consider it in the form of high medium low etc but there might be cases where you don't have any specific categorization of any threats for example if we consider like a website itself so suppose availability scan produces output in the form of high threat but during the manual testing process you found that particular threat is not validated, you conclude from the result that this thread is not relevant at this particular state of time so either it's in false positive category or it might be relevant after that particular product has gone to release phase or updated, so here you want to update that possible threat from high to low so this thing types of scenarios you have to take into consideration as well. A common vulnerability scoring Like CVSS can also be taken into consideration.

3. We only limit our discussion to two of major tools used in vulnerability scanning however there are other tools like Nessus Nexpose highly efficient in exploring the software level network level vulnerabilities.

V. Future Scope

Current Vulnerability assessment mechanisms provide a great way to handle vulnerabilities. Although it remains a open field to gather new vulnerability inclusion of modern approaches like machine learning Artificial intelligence. Although some of research areas currently its considered but consideration of false positive and correctness remains well in scope for future refinement and implementations [17]

References

[1] Abd Rahman, Nor Azlina, et al. "Millennial Psychology Towards Hacking Activities." Journal of Applied Technology and Innovation (e-ISSN: 2600-7304) 6.2 (2022): 22.

[2]

[3] [2] S. Shah and B. M. Mehtre, “An overview of vulnerability assessment and penetration testing techniques,” Journal of Computer Virology and Hacking Techniques, vol. 11, no. 1, pp. 27–49, Nov. 2014, doi: 10.1007/s11416-014-0231-x.

[4]

[5] [3] Wardana, Wasis, Ahmad Almaarif, and Adityas Widjajarto. "Vulnerability Assessment and Penetration Testing On The Xyz Website Using Nist 800-115 Standard." Syntax Literate; Jurnal Ilmiah Indonesia 7.1 (2022): 520-529.

[6]

[7] [4] Aljebry, Amel F., Yasmine M. Alqahtani, and Norrozila Sulaiman. "Analyzing Security Testing Tools for Web Applications." International Conference on Innovative Computing and Communications. Springer, Singapore, 2022.

[8]

[5] S. Mishra, S. K. Sharma, and M. A. Alowaidi, "Analysis of security issues of cloud-based web applications," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 7051-7062, 2021.

[6] M. Rennhard, D. Esposito, L. Ruf, and A. Wagner, "Improving the effectiveness of web application vulnerability scanning," International Journal on Advances in Internet Technology, vol. 12, pp. 12-27, 2019.

[7] A. Tedyyana and O. Ghazali, "Teler Real-time HTTP Intrusion Detection at Website with Nginx Web Server," JOIV: International Journal on Informatics Visualization, vol. 5, pp. 327-332, 2021.

[8] F. Fathurrahmad and E. Ester, "Automatic Scanner Tools Analysis As A Website Penetration Testing: Automatic Scanner Tools Analysis As A Website Penetration Testing," Jurnal Mantik, vol. 4, pp. 1138-1144, 2020.

[9] W. Wardana, A. Almaarif, and A. Widjajarto, "Vulnerability Assessment and Penetration Testing On The Xyz Website Using Nist 800-115 Standard," Syntax Literate; Jurnal Ilmiah Indonesia, vol. 7, pp. 520-529, 2022.

[10] J. Yomas and C. Kiran, "Critical analysis on the evolution in the e-payment system, security risk, threats and vulnerability," Communications on Applied Electronics, vol. 7, pp. 21-29, 2018.

[11] M. A. Ali, "Does the online card payment system unwittingly facilitate fraud?," Newcastle University, 2019.

[12] K. Dennis, M. Alibayev, S. J. Barbeau, and J. Ligatti, "Cybersecurity Vulnerabilities in Mobile Fare Payment Applications: A Case Study," Transportation Research Record, vol. 2674, pp. 616-624, 2020.

[13] M. Yu, J. Zhuge, M. Cao, Z. Shi, and L. Jiang, "A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices," Future Internet, vol. 12, p. 27, 2020.

[14] K. Kritikos, K. Magoutis, M. Papoutsakis, and S. Ioannidis, "A survey on vulnerability assessment tools and databases for cloud-based web applications," Array, vol. 3, p. 100011, 2019.

[15] H. S. Abdullah, "Evaluation of open source web application vulnerability scanners," Academic Journal of Nawroz University, vol. 9, pp. 47-52, 2020.

[16] Aljebry, Amel F., Yasmine M. Alqahtani, and Norrozila Sulaiman. "Analyzing Security Testing Tools for Web Applications." International Conference on Innovative Computing and Communications. Springer, Singapore, 2022.

[17] Antonelli, Diego, et al. "Leveraging AI to optimize website structure discovery during Penetration Testing." arXiv preprint arXiv:2101.07223 (2021).

[18] Wang, Liwei, et al. "An empirical study on vulnerability assessment and penetration detection for highly sensitive networks." Journal of Intelligent Systems 30.1 (2021): 592-603.

[19] Pohorila, Victoriia. Application penetration test and its necessity in 2021. Diss. National Aviation University, 2021.