INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 3)
Available online at: www.ijariit.com

WebEnum

Karthik J. Bhat
karthikjbhat.16is@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

Karthik P.
muralidharakarthik64@gmail.com
Sai Vidya Institute of Technology, Bengaluru, Karnataka

Mithun B. L.
mithunbl.16is@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

Nishith B. Rao
nishithbr.16is@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

Dr. Sangeetha
sangeetha.v@saividya.ac.in
Sai Vidya Institute of Technology, Bengaluru, Karnataka

ABSTRACT

When you want to compromise a system or infrastructure, the most critical phase you have to care about is information gathering. Then you enumerate the system using gathered information to get the exact version of protocols or software. Enumeration is one important phase where you extract the user information, network share, banner grabbing and retrieval of network protocol information. Enumeration is so important because one bad move could lure you to a rabbit hole which gives false information using that you can't compromise a system and you waste most of the time in it. So when you spend the most time in this enumeration phase you would get exact information about the system. It will save you some time and it will avoid getting you frustrated. When you are hacking a big network every information you should gather correctly. So some information will help you in further phases like privilege escalation or clearing tracks.

Keywords *— Attack, Enumeration, Hacker, Web-Server*

1. INTRODUCTION

WebEnum[1] is a command-line information gathering tool which retrieves the various type of information about the web application and also finds the vulnerabilities in it.

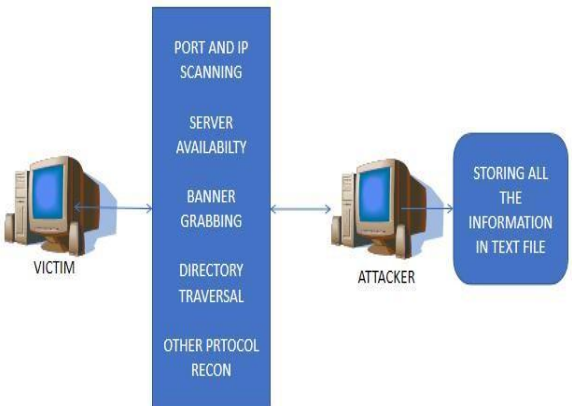

Fig. 1: Web Enumeration System Architecture

Gathered information is used to compromise the whole network or web application. Here this tool establishes the active connection with the system we are attacking. To enumerate web servers, we have so many tools available that are specific to certain tasks only. It may not contain multiple techniques of enumeration and also different tools means different usage and different commands to think about which is time-consuming. Time is the major issue when you are doing CTF(Capture the flag), bug bounty hunting and also in real-world pen-testing.

2. ARCHITECTURE

This tool, WebEnum, performs information gathering in an organized manner, and the outputs will be very simple so that beginners in this web application security field can analyze the output and can learn the way information gathering is done. This provides a final output which can be understandable by non-tech people also.

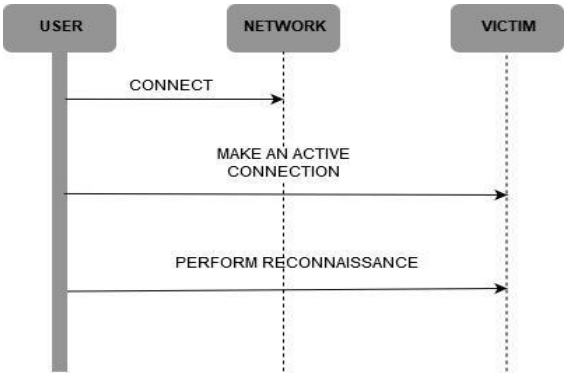

Fig. 2: Sequence Diagram

In this tool, first, we verify the port web server is running. After that, we perform directory Bruteforce technique to find the directories the web application contains along with that we check the existence of a sensitive pages or files, like, admin login page, which link is not presented in main web page, files having password and user-names, which could be happened due

to misconfiguration, information about private network the web servers may having. This tool also performs DNS enumeration to see if any DNS records are publicly available just to expand the attack surface.

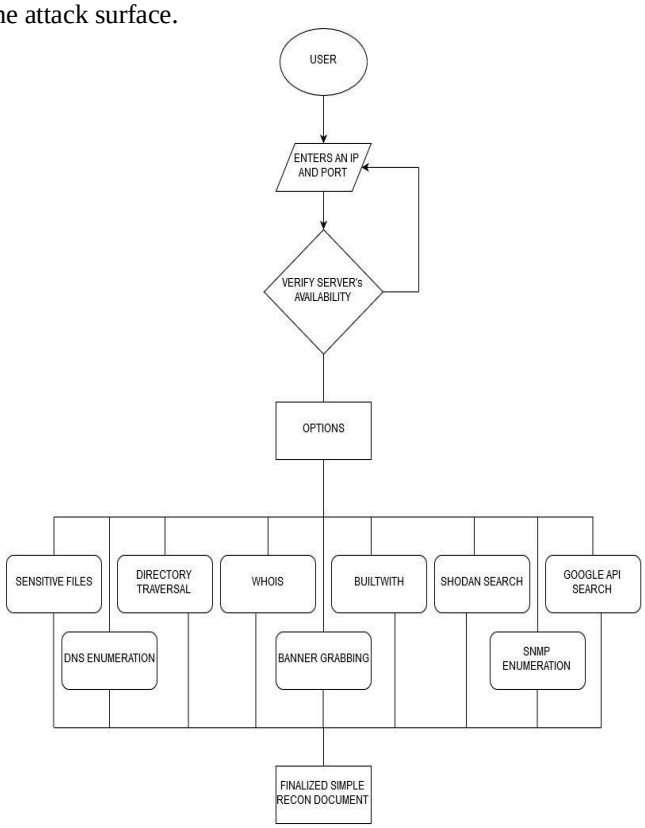

Fig. 3: Functional Diagram

3. USE OF WEBENUM

3.1 Web application and Security

Web applications are used worldwide and these have so many vulnerabilities [2]. OWASP (Open Web Application Security Project) is an organization that provides practical and genuine information about internet applications. In 2017 they have come up with the list of top 10 vulnerabilities of Web Applications.

Those are:

- Injection
- Broken authentication
- Sensitive Data exposure
- XML external entities
- Broken access control
- Security misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring

These are only the top 10 vulnerabilities in web applications. We have many more vulnerabilities in web applications not just limited to the above list.[1]

Some of these vulnerabilities are easy to find and also to exploit once you find the exact location of the vulnerable page or location. In some locations private data could be leaking so we have to find those data exposure and report it to the web admin.

3.2 Finding Sensitive Files using SHODAN

SHODAN search engine developed and designed by John Matherly. It is not like the other search engine. It lets the user get to know what all devices that are connected to the internet Nowadays as the internet grew, illegal activities also arose, an intruder or attacker can easily access and modify all the sensitive data remotely. Some of the common sensitive resources are password files, configuration files, log files these contain files, statistics data, databases, etc. These can be used by an attacker for getting the information or knowing more about his target. Using this attacker can compromise the website and create a new administration account.

There are many search queries would locate all web pages which have that particular text or a file contained within them. It is normal for applications to include their current running version on every page they serve. One can even retrieve the username and password list from Microsoft Front-Page servers by inputting the given micro script in the Google search field[2].

3.3 Brute Force attack

A Brute Force attack is a method used in the form of guessing by an attacker to decode such as passwords or Data Encryption Standard which are encrypted data

Brute force directory guessing attacks by trial and error and are very common attacks used against websites and web servers. A path traversal attack which is also known as directory traversal aims to access files and directories that are stored outside the web root folder Brute force attacks are difficult, if not impossible, to carry out manually. Instead, hackers write simple scripts, called bots, that carry out thousands of these break-in attempts against websites on auto-pilot. Typically, these bots are custom-written by the attackers and designed to be easily distributed across many hacked machines. These groups of bots, or bot nets, work in conjunction with other commonly accessible tools that either generate thousands of passwords or use a word-list. The latter is often referred to as a dictionary attack, because of they rely on “dictionaries” or long lists of words to try as a list of passwords and/or user-names on your website. These lists can be reused by many hackers over and over.

Once attackers have gained access to your website, they can use its files and the web host server to cause a wide variety of damage through malicious behavior, including:

- Defacement: your site can display unwanted and sometimes malicious content, your content may be deleted, and website of yours can be taken down altogether;
- Malware distribution: The site pages of yours may infect your visitors with malware, ransom-ware, and viruses;
- Spamvertising: Your website may display spam content and/or links to spam websites;
- Redirection: Accessing your domain name may cause your visitors to be redirected to malicious websites, or to pages that contain affiliate links and make money for the hackers;
- Stealing system resources: by using your web server’s resources, attackers are carrying out tasks such as email campaigns and content delivery on your dime;
- Fun: It may be hard for some people to imagine, but some attackers, particularly younger ones, are simply bored and find the act of hacking into strangers’ websites entertaining, particularly in the case of brute force attacks, which are relatively simple to learn and carry out.[3]

3.4 ONSIT (Open Source Intelligence)

Open-source intelligence is data collected from sources which are publicly available to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources. As per DoD, OSINT is “produced from publicly available information that is collected, exploited,

and disseminated promptly to an appropriate audience for addressing a specific intelligence requirement." The expanding explosive growth of internet users now pays for goods and services online sharing their thoughts which are personal blogs and expose sharing their day to day lives to other people.

This generates extensive data or intelligence in various forms like audio, video, images, and text which is free and accessible to everyone unless restricted by an organization or law.

OSINT sources can be divided into different categories of information flow:

- Media: print newspapers, magazines, radio, and television from across and between countries.
- Internet, online publications, blogs, discussion groups, citizen media, YouTube, and other social media websites. This source also outpaces a variety of other sources due to its timeliness and ease of access.
- Public – government data, public government reports, budgets, hearings, telephone directories, press conferences, websites, and speeches. Although this source comes from an official source they are publicly accessible and may be used openly and freely.
- Professional – academic publications, information acquired from journals, conferences, symposia, academic papers, dissertations, and theses.
- Commercial Data, commercial imagery, financial and industrial assessments, and databases. Grey literature, technical reports, preprints, patents, working papers, business documents, unpublished works, and newsletters.[4]

Some of the tools are

- MALTEGO: Maltego is a product of Paterva and is a part of the Kali Linux operating system. Maltego tools help to play out a critical observation against targets with the assistance of different built-in transforms and it is open source so it gives the capability to write custom transform or modules.
- HARVESTER: The Harvester is an outstanding tool for collecting intelligence like email and domain for the specified target. This tool is a part of the Kali Linux operating system and very popular for harvesting intelligence used in the early stages of a penetration test or phishing.
- RECON-NG: Recon-ng is another powerful tool for target intelligence collection which also comes with the Kali Linux operating system. Recon-ng builds with a modular approach in mind just like Metaspoilt.
- TINEYE: TinEye is a reverse image search engine. You'll submit a picture to TinEye to seek out wherever it came from and how it's getting used. TinEye uses neural networks, pattern recognition, machine learning, and image recognition technology instead of keywords or metadata.[5]

4. APPLICATIONS

It is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software and other problems.

- CAPTURE THE FLAG: A cybersecurity CTF is a competition between security professionals and/or students learning about cybersecurity. This competition is used as a learning tool for everyone interested in cybersecurity and it can help sharpen the tools they have learned during their training
- BUG BOUNTY HUNTING: They are known as bug bounty hunters. Bug bounty hunters are ethical hackers who make a hobby (or, even a business) of finding security issues or bugs in an online business. Bug bounty programs in major firms like Facebook, Google and Apple have regularized the process.

5. RESULT

The result is to check whether the port is open or closed, the presence of critical files in web server. Possible web directories available, Information gathered about web server through ONSIT DNS, SMTP, FTP, SSH, HTTP, Banner Grabber, DNS enumeration

6. CONCLUSION

Webenum performs information gathering in an organized manner, and the outputs will be very simple so that beginners in this web application security field can analyze the output and can learn the way information gathering is done. This provides a final output which can be understandable by non-tech people.

7. REFERENCES

[1] www.oswap.org
[2] www.shodon.io
[3] www.wordtrence.com
[4] www.breachlock.com
[5] Python Web Penetration Testing Cookbook by Cameron Buchanan, Benjamin May, Terry Ip, Andrew Mabbit, Dave Mound.

