Python Hacking 101

Introduction

Who we are!

- Manindar Mohan, Beagle Security
- Febna V M, Beagle Security

Why security is of high importance

- World Wide Web has become a powerful platform for application delivery
- Sensitive data increasingly made available through web applications
- 98 % of the web applications are vulnerable.
- 78% of easily exploitable weakness occur in web applications.

Famous last words...

- “Nobody would bother to hack us.”
- “Our network firewall will keep us safe.”
- “We will add security to the system later.”
- “What's the worst that could actually happen?”

What is Penetration Testing?

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior.

Why is Pentesting Important?

Pen testing evaluates an organization’s ability to protect its networks, applications, endpoints and users from external or internal attempts to circumvent its security controls and gain unauthorized or privileged access to protected assets.

Types of penetration testing

Black box. In a black-box testing assignment, the penetration tester is placed in the role of the average hacker, with no internal knowledge of the target system. Testers are not provided with any architecture diagrams or source code that is not publicly available.

Gray box. The team has some knowledge of one or more sets of credentials. They also know about the target's internal data structures, code, and algorithms. Pen testers might construct test cases based on detailed design documents, such as architectural diagrams of the target system.

White box. For white box testing, pen testers have access to systems and system artifacts: source code, binaries, containers, and sometimes even the servers running the system. White box approaches provide the highest level of assurance in the least amount of time.

Basic Methodology of Security testing

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Post Exploitation
5. Reporting

Reconnaissance

- The reconnaissance phase is the most important phase of the hacking methodology.
- The importance of reconnaissance is to accumulate important information and facts about the selected target.

Two types of reconnaissance:

1. Passive reconnaissance
2. Active reconnaissance

Passive reconnaissance

Passive reconnaissance is what happens when you don't communicate with the target. This is accomplished by inspecting the webpage, exploring Google, studying social media accounts for information and much more. In short, you're watching for any data that can be applied to hold against the target.

Search for common usernames for the website.

If its an indian website there will be some

- Rahul
- Anita

Passive Reconnaissance Techniques

Google Dorks

- Site:
- Inurl:
- Intext:
- Cache:
- Filetype:
- Link:

https://www.exploit-db.com/google-hacking-database

Passive Reconnaissance Techniques

Guess Hostname

Use nslookup command followed by whois to get information related to the hostname.

Passive Reconnaissance Techniques

- www.netcraft.com
- www.archive.org
- www.shodan.io
- https://osint.link
- https://osintframework.com
- www.builtwith.com
- wappalyzer

Active reconnaissance

- Active reconnaissance is the phase you apply when you are investigating your target.
- It involves communicating directly with the target. It is necessary to perceive that during this method, the target may log your IP address and log your movement.

Scanning

After reconnaissance, scanning is the next stage of information gathering that hackers apply. Scanning is where hackers enter into the system to scan for relevant data and settings in a particular IP address series.

Nmap

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

Nikto

Nikto is a web server scanner .It identifies several vulnerabilities in web servers. Unlike the active reconnaissance tools that threat actors use, Nikto is highly detectable by an IDS, so it is ideal for ethical hacking purposes.

Gaining Access/exploitation

In the simplest words, exploitation is the method of gaining authority over a system. However, it is necessary to know that not every exploit points to complete system compromise. More precisely described, an exploit is a method to to successfully gain access to the systems by taking advantage of their vulnerabilities identified by scanning and information gathering.

Post Exploitation

Post exploitation essentially means the stages of the ethical hacking job once the target system has been jeopardized by the hacker. The condition of the endangered system is defined by the utility of the real data stored in it and how a hacker may gain the advantage of it for wicked ideas.

Reporting

Like every other phase we have mentioned, drafting a sound ethical hacking report is crucial.

The tester gathers the results of the penetration attempts into a report, which is then examined for weaknesses.

Why Python?

Python is a general-purpose scripting language that has gained immense popularity amongst professionals and beginners for its simplicity and powerful libraries. Python is insanely versatile and can be used for almost any kind of programming. From building small scale scripts that are meant to do banal tasks, to large scale system applications – Python can be used anywhere and everywhere. In fact, NASA actually uses Python for programming their equipment and space machinery.

Python Libraries Every Pentester Should Be Using

- Scapy

This is a Powerful python-based packet manipulation tool and library. It forges/decodes packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more

- Requests/BeautifulSoup

Requests allows programmers to easily send HTTP/1.1 requests, without the need for manual labor or encoding.

Beautiful Soup is a Python package for parsing HTML and XML documents. It creates a parse tree for parsed pages that can be used to extract data from HTML, which is useful for web scraping.

Python Libraries Every Pentester Should Be Using

- Socket

Low-level network interfacing library that allows systems to speak over a network.
More or less anything that communicates over a network interface, which is to say, tens of thousands of tools rely on the simple socket.

Weaponizing Python

MAC Spoofing

MAC Address

MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: IP address and MAC address. It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.

MAC Spoofing

MAC spoofing refers to altering the MAC address on a NIC (network interface controller) card.

MAC Spoofing

MAC Spoofing in Penetration Testing

An important feature of MAC spoofing in penetration testing is that it allows absolutely untraceable scans, because both source IP and MAC addresses are spoofed.

MAC spoofing can be used to test redirection of network traffic, and for testing access points. By allowing the impersonation of different MAC addresses within a network, MAC spoofing provides the facility for penetration tests to test firewalls, and to acquire information from a remote host.

MAC changer

Hands_on

Changing physical address of the host system.

For this we make use of subprocess python module to execute system commands and achieve the goal.

Port Scanning

Network scanning refers to a set of procedures that investigate a live host, the type of host, open ports, and the type of services running on the host.

Network scanning is a part of intelligence gathering by virtue of which an attack can create a profile of the target organization.

Port Scanner

Hands_on

Identify the open ports and services running on them.

Open ports can be dangerous when the service listening on the port is misconfigured, unpatched, vulnerable to exploits, or has poor network security rules.

“ it is the context that matters not the state of port.”

Packet Sniffing

When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called data packets and reassembled at receiver's node in original format. It is the smallest unit of communication over a computer network. It is also called a block, a segment, a datagram or a cell. The act of capturing data packet across the computer network is called packet sniffing.

Types of Sniffing

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. allows listening only. It works with the Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts can see the traffic. Therefore, an attacker can easily capture traffic going through.

Types of Sniffing

Active Sniffing

In active sniffing, the traffic is not only captured and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network.

A switch is a device that connects two network devices together. Switches use the media access control (MAC) address to forward information to their intended destination ports.

Attackers take advantage of this by injecting traffic into the LAN to enable sniffing.

Network Sniffer

Hands_on

Capturing TCP, UDP, and ping packets to and fro of a system

Here we will make use of scapy python module to capture and manipulate packets

Footprinting of a Web Server

For web server pentesting, we must know about web server, its hosting software & operating systems along with the applications, which are running on them.

Footprinting is basically a process of finding all the possible ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target

Types of Footprinting

1. Active Footprinting:

Active Footprinting is a process of collecting information by directly communicating with the concerned personal or the machine.

2. Passive Footprinting:

Passive Footprinting is a process of gathering information about any victim without any direct communication. This can be done using various google search or public reports.

Methods for footprinting of a web server

Testing availability of HTTP methods

A very good practice for a penetration tester is to start by listing the various available HTTP methods.

HTTP Methods

- GET
- POST
- PUT
- HEAD
- DELETE
- PATCH
- OPTIONS

Footprinting - HTTP Methods

Hands_on

Connect to the target web server and enumerate the available HTTP methods using requests library in Python.

We will make use of some standard methods like 'GET', 'POST', 'PUT', 'DELETE', 'OPTIONS' and a non-standard method ‘TEST’ to check how a web server can handle the unexpected input.

Footprinting - HTTP Header

Foot printing by checking HTTP headers

HTTP headers are found in both requests and responses from the web server. They also carry very important information about servers. HTTP headers let the client and the server pass additional information with an HTTP request or response.

Headers can be grouped according to their contexts:

1. General headers apply to both requests and responses, but with no relation to the data transmitted in the body.
2. Request headers contain more information about the resource to be fetched, or about the client requesting the resource.
3. Response headers hold additional information about the response, like its location or about the server providing it.
4. Entity headers contain information about the body of the resource, like its content length or MIME type.

Footprinting - HTTP Header

Hands_on

Gather information about headers of the web server.

```
Server: Apache-Coyote/1.1,
Set-Cookie: JSESSIONID=7BE519A9794277555FABD701F41B9A4C; Path=/;
HttpOnly,
Content-Type: text/html;charset=ISO-8859-1;
Transfer-Encoding: chunked,
Date: Sat, 08 May 2021 07:46:08 GMT
```

HTTP header informations can be used to test insecure web server configurations.

Local File Inclusion

Local file inclusion (LFI) and path traversal vulnerabilities occur when user-supplied data is able to probe the underlying file system of the server. In other words, an attacker can read files from the server.

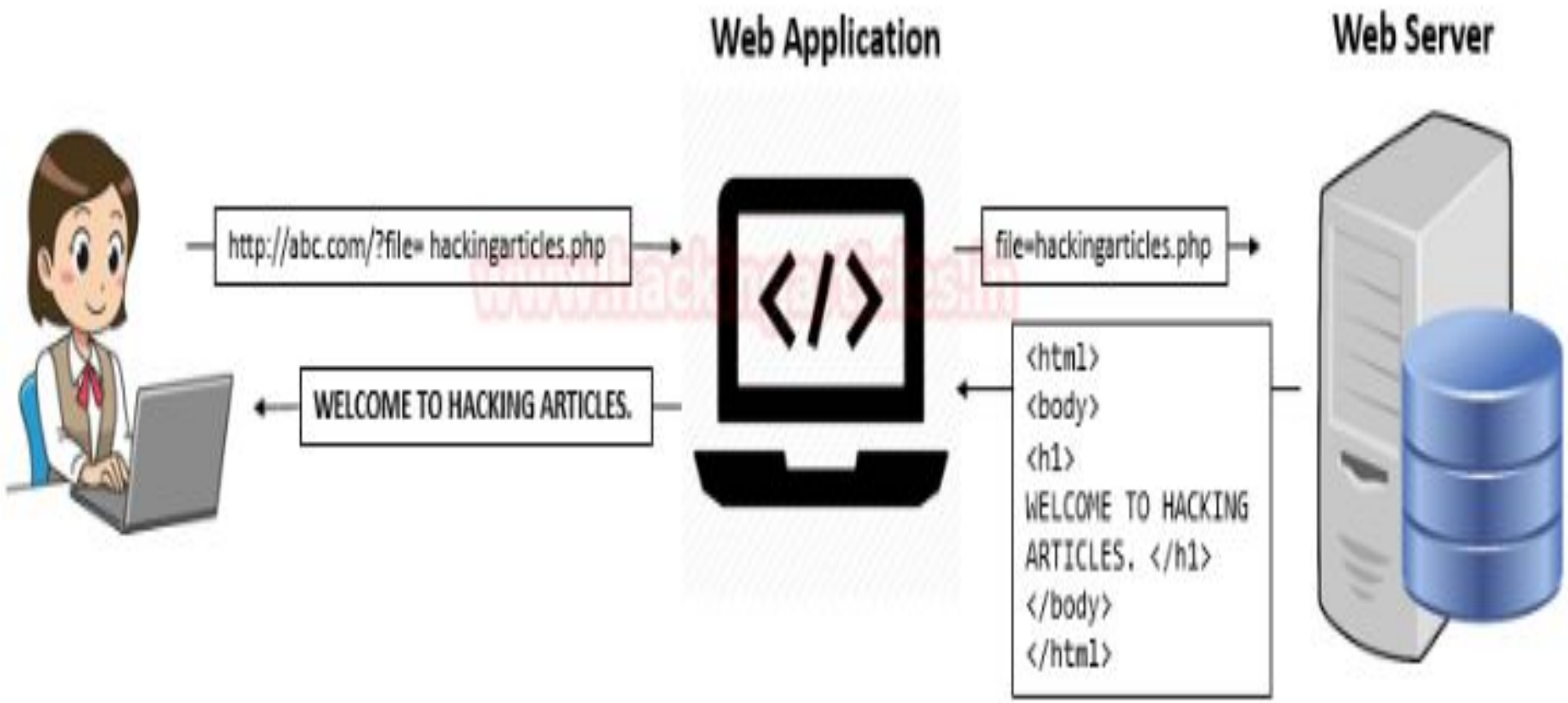
Scripts that take file names as parameters, without securing user input are good candidates for LFI. A very basic example would be the following php script:

```
// vuln.php
<?php
  include $_GET['file'];t
?>
```

http://test.com/vuln.php?file=image.jpg

Which takes image.jpg as a parameter. An attacker would exchange image.jpg for sensitive files such as:

http://test.com/vuln.php?file=../../../../../../../../etc/ passwd


Web Application
Web Server
http://abc.com/?file= hackingarticles.php
file=hackingarticles.php
WELCOME TO HACKING ARTICLES.
<html>
<body>
<h1>
WELCOME TO HACKING
ARTICLES. </h1>
</body>
</html>

LFI

Hands_on

Using the Directory Traversal or ../, we will traverse the directories to get the content of passwd file located at /etc/ directory.

Retrieve the source code of the file or configuration files using the php://filter wrapper.

Cross-Site scripting

Cross-site scripting (also known as XSS) is a code injection attack executed on the client side of a application.

Steals cookies, session token and other sensitive information

Types of XSS

- Reflected XSS, where the malicious script comes from the current HTTP request.
- Stored XSS, where the malicious script comes from the website's database.
- DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.

XSS

Hands_on

Sample payload

```
<script>alert("xss alert");</script>
```

```
<script>alert(document.cookie);</script>
```

To check the possibility of an XSS attack, we can check the response text for the attack vector we provided.

If the attack vector is present in the response without any escape or validation, there is a high possibility of XSS attack.

Contact

Manindar Mohan
manu.m@beaglesecurity.com
8075841659

Febna VM
febna.vm@appfabs.com
7510328242

THANK YOU