SYSTEMOD SECURITY

SYSTEMOD SECURITY

SYSTEMOD SECURITY

PENETRATION TESTING COURSE (01)

Understanding How Its Done

JOY GHOSH

WHOAMI

JOY GHOSH

- I am a Full time Pen-tester
- I do Bug Hunting sometimes
- I love to break things thats why i am a Pen-tester

COMMON KEYWORD IN HACKING

Payload?

In cybersecurity, a payload is malware that the threat actor intends to deliver to the victim.

Exploit?

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in an application or a system to cause unintended or unanticipated behavior to occur.

Revershell?

To gain control over a compromised system, an attacker usually aims to gain interactive shell access for arbitrary command execution. With such access, they can try to elevate their privileges to obtain full control of the operating system. However, most systems are behind firewalls and direct remote shell connections are impossible. One of the methods used to circumvent this limitation is a reverse shell.

Webshell?

A web shell is a malicious script used by an attacker with the intent to escalate and maintain persistent access on an already compromised web application. A web shell itself cannot attack or exploit a remote vulnerability.

Botnet?

A botnet is a network of compromised systems that an attacker would control, either to use themselves or to lease to other criminals.

PENETRATION TESTING METHODOLOGY

METHODOLOGY OF PENETRATION TESTING

- RECON
- MAPPING
- DISCOVERY
- EXPLOITATION

Penetration Testing Methodology

RECON

The recon phase consists in searching for open-source information on the target of the security audit. All information potentially useful for an attacker is collected, for example: IP addresses, domain and sub-domain names, types and versions of technologies used, technical information shared on forums or social networks, data leaks…

Mapping

The mapping phase allows listing all functionalities of the audit target. This step enables pentesters to have a better visibility on the most critical and exposed elements. This step is particularly essential when the objective of the security audit is to conduct tests on all the functionalities of a target.

Discovery

The discovery phase is an attack phase: pentesters look for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

Exploitation

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, in order to discover new vulnerabilities. The exploitation of security vulnerabilities allows evaluating their real impact and thus their criticality level.

SYSTEMOD SECURITY

SYSTEMOD SECURITY

SYSTEMOD SECURITY

LETS START LEARNING

PEN-TESTING (V1.0)