Name : Abhishek Srivastava.
Reg. No : 19BLE10071
Subject : Ethical Hacking
Slot : B11 + B12 + B13
Date : 9th may 2022

Term End Examination.

1] a) Ethics in Ethical Hacking.

Ethics in the broadest sence refers to the concern that human have always had for figuring out how best to live.

Cybersecurity professionals need to know that the same trick is used by their black hat counterpart. This means that programmer should know how to. and therefore, be able to copy credit card data, voilate intellectual property agreement, etc. The safety of your customers data is in their hands.

Cybersecurity also has a potential to interrupt your regular business procedures. So called Ethical hacking and protective measures can ~~cost~~ cause inconvinience of your customer and other Employees. Most professional focus on technical aspect of their job, but providing Ethical service to your customers is the most important part of this Job.

The Five major Steps involved in ethical hacking:-

STEP 1

Reconnaissance - In this step we gather data of the target computer. It is of two types.

Active Reconnaissance
- Involves direct communication with target.

Passive Reconnaissance
- Involves indirect methods to collect information.

STEP 2

Scanning - Hacker scans the collected data and deploys the appropriate tools to hack the aimed system.

STEP-3

Gaining Access - In this step, the hacker gain access to the target System, network or application using specific tools.

STEP-4

Maintaining Access - In this step the hackers try to maintain access for future attacks without the user knowing about it. Malicious files are available online to do this job.

STEP-5

Covering tracks- In this step the hacker tries to cover all the tracks so that he doesn't get caught by the security personnel.

2]
(b) (4)

(1) Various Attacks

Types of Cybersecurity Attack:-

Malware
Malwar is a term that describes malicious software, including spyware, randomsome, viruses and worms. Malware breaches the network through a vulnesability, typically when a user clicks on a vulnerable link or email attachment that include risky software.

Phishing
It is a method of sending fraudulent communication that seen to come from a reputable source, usually through email. The goal is to steal and get some sensitive data or to install malware on victim's machine.

Man-in-the-middle attack
MitM attacks, also called as eavesdropping attack, occur when attacker insert themselves into a two-party transaction. Once the attacker interrupt the trafic, it can steal or filter data.

Denial of Service

It is an attack on file system, servers or network with traffic that exhaust resources and bandwidth. It makes system incompatible to fulfill request.

SQL Injection

A SQL Injection happens when the attacker inserts malicious code into the server that uses SQL and forces it to reveal information that it would normally don't.

Zero-day Exploit

It hits after network vulnerability is announced but before the patch or solution is implemented. It requires constant awareness.

DNS Tunnelling

It requires DNS protocol to communicate over non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS.

Examples of Cybersecurity Attacks:

- Instant messaging abuse.
- Identity fraud, thread or extortion.
- Malware, phishing, spamming, spoofing.
- Password sniffing.
- System Infiltration.
- Breach of access.
- Website defacement.

2]. b)

ii) Vulnerabilities

Vulnerability is defined as an issue in the software code that the hacker can exploit to harm the system. It can be a gap in the implementation of the cyber security procedures or the weakness in the control over the system.

Types of Vulnerability.

i. Faulty defences.
ii. Resource manggement not adequate.
iii. Insecure connections.
iv. End user error and misuse.

Examples of Vulnerability:

i. Injection.
ii. Broken Authentication.
iii. XML External Entities.
iv. Sensitive data Exposure.
v. Cross-Site scripting.
vi. Security Misconfiguration.

PTO

4]

Buffer Overflow.

It is a software coding error or vulnerability that can be exploited by hackers to gain unauthorised access to corporate systems. It is fairly common vulnerability.

The software error focuses on buffer, which is sequential section in the computing memory that hold data temporarily as it is transferred between locations. It occurs when the amount of data overflows or exceed the buffer capacity. The extra data overflows into adjacent memory location and corrupts or overwrite the data in those locations.

Example

Attacker taking advantage of Buffer overflow by writing shell code.

In the code mentioned below, program will grant access if password is correct:

```
char pass[64];
gets(pass);
if (gets(pass)) {
   printf("Correct password");
   c = 1;
}
if (c) {
   printf("Access granted");
}
```

In the above code there is a possibility of buffer overflow as the gets() function didn't checked for length.

Here's the example what attacker could do.

```
$./bufferprog.
Enter a password:
hhhhhhhhhhhhhhhhhhhhhhhhhhhhhhhh
Wrong password
root priviledges given.
```

In the program, the root priviledges are given even if the password is wrong.

3](b)

Malwares

Malware is a malicious software, and is a blanket term for worms, viruses, trojans and other harmful computer programs used by hackers to ~~wreck~~ wreck system and gain access. It can cause harm to the victim in unimaginable ways. The victim can be individuals, organisation, businesses or government.

Types of Malware.

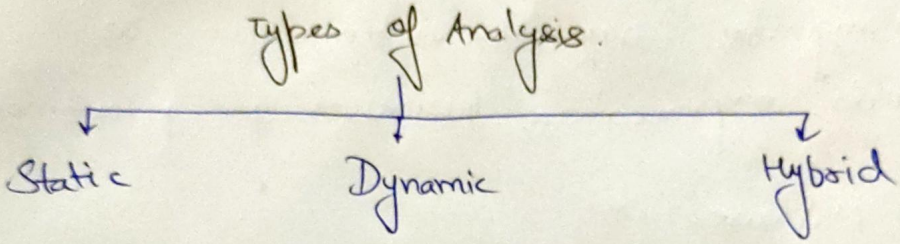
~~There are many~~

1) Adware
2) Fileless Malware.
3) Viruses
4) Worms.
5) Trojans.
6) Bots
7) Ransomware
8) Spyware.

Although, there are other types of Malwares, but the above mentioned are the most common ones

Malware Analysis.

Malware analysis is the process of understanding the behaviour and purpose of a suspicious file or URL. The output of the process aids in detecting and mitigating any potential threat.



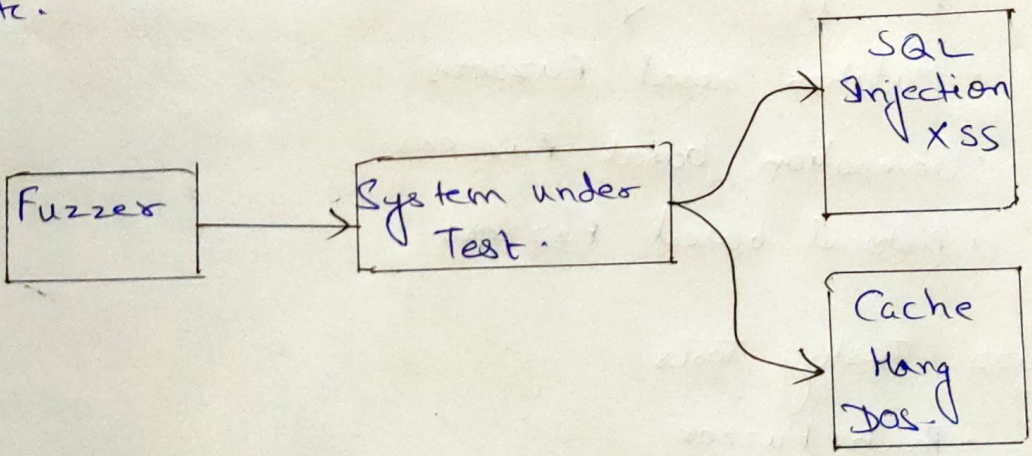
Malware Analysis in Commercial Applications.

- To apply sophisticated techniques and provide deep behavioural analysis and identifying code, functionality threat can easily be detected.
- Helps in Improve alerts early.
- It provides root cause analysis and determing the impact
- It exposes facts like access to a port etc.

5]

Fuzzing or Fuzz Testing is a Software testing technique of putting an invalid or random data called Fuzz into the System Software to discover coding errors and security Loopholes.

The purpose of Fuzzing is inserting data using automated or semi-automated techniques and testing the System on various Exceptions. like System cache failure, built-in code failure, etc.



Role of Fuzz Testing.

- Usually, fuzz testing finds out most serious security faults or a defect in the System.
- Fuzzing is used to test the Vulnerability of Software. It is a cost effective testing technique.

- Fuzzing is one of the black box testing techniques.
- Fuzzing is one of the most common method used by hackers to find vulnerability of a System.
- Fuzzing gives more effective results when used with Black box testing, Beta testing and other debugging methods.

Examples of Fuzzing

- Mutation based fuzzers.
- Generation based fuzzers.
- Protocol based fuzzers.

Fuzz Testing Tools

- Peach Fuzzer
- Spike Proxy
- Webscarab
- OWASP WSFuzzer

Types of bugs detected using fuzzing.

- Correctness bug.
- Invalid input.
- Assertion failure
- Memory leaks.