TASK-5

AI FOR CYBER SECURITY

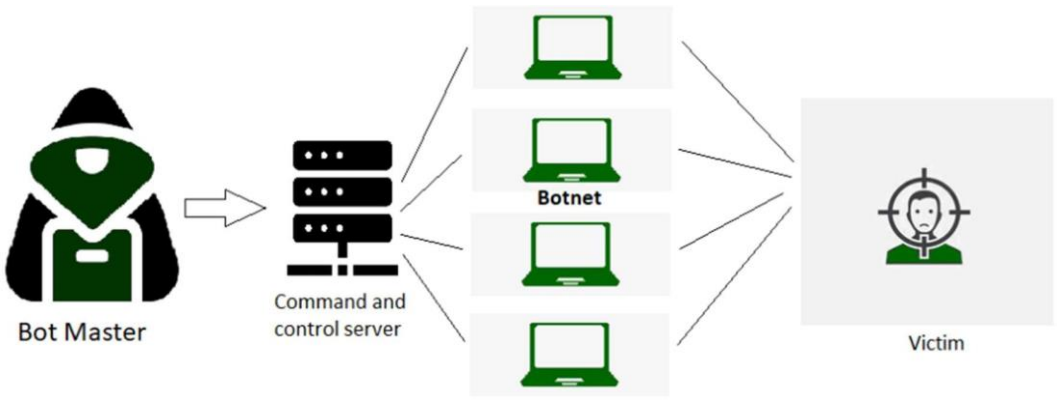
P. MONISH

21BCE9517

29-08-2023

Ten web server attacks

1. DENIAL-OF-SERVICE (DOS) / DISTRIBUTED DENIAL-OFSERVICE



Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are trojan infected, target a particular system which causes a DoS attack.

A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic. Thus, crashing the website or computer due to overloading.

2. WEB DEFACEMENT ATTACK:

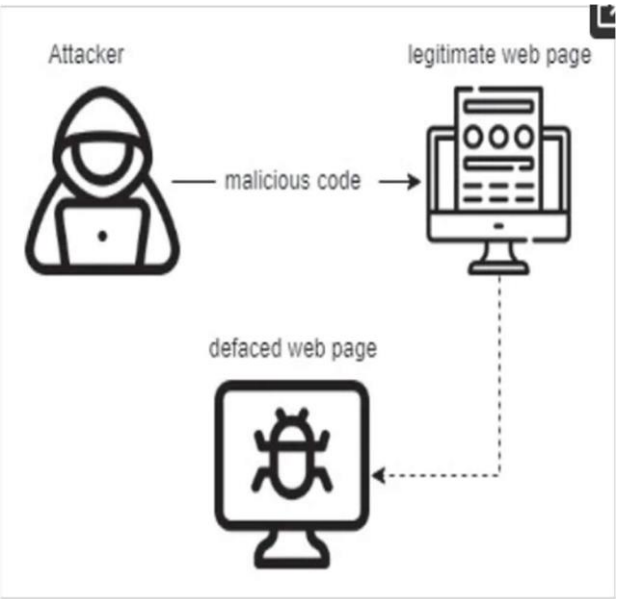


Figure 1. Overview of website defacement.

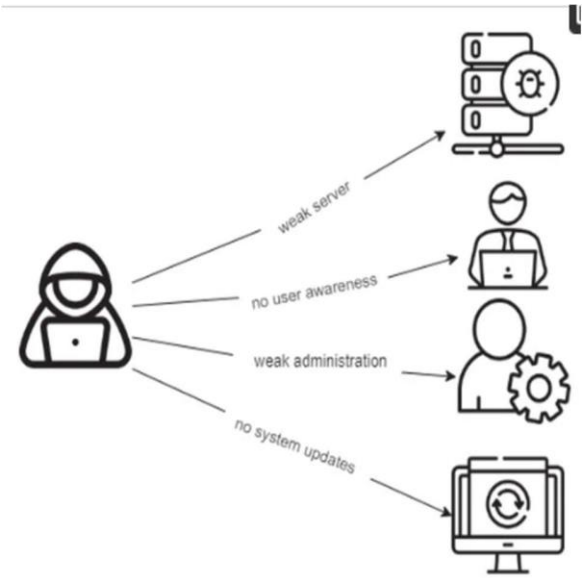


Figure 2. Defacement causes.

In a Web Defacement Attack, the hacker gains access to the site and defaces it for a variety of reasons, including humiliation and discrediting the victim. The attackers hack into a web server and replace a website hosted with one of their own.

3.SSH BRUTE FORCE ATTACK:

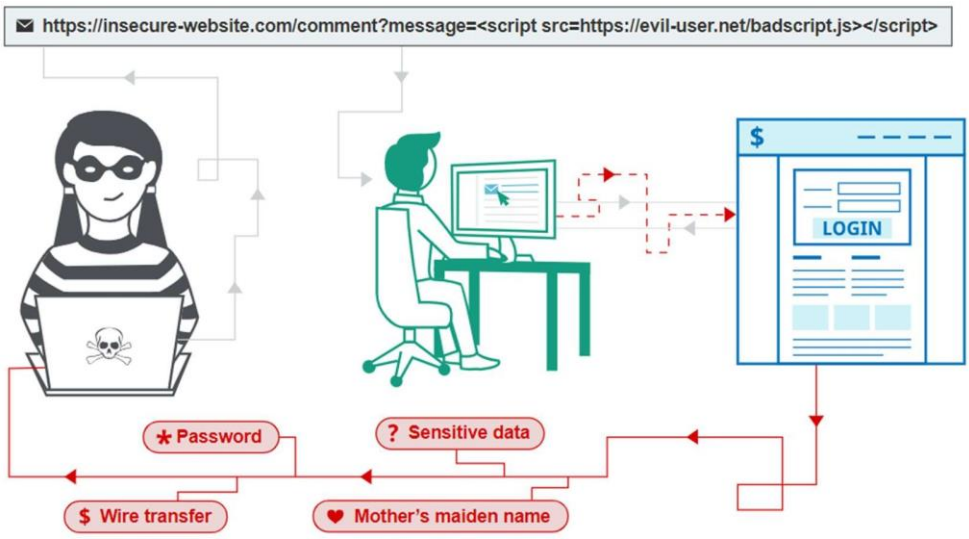
By brute-forcing SSH login credentials, an SSH Brute Force Attack is performed to attain access. This exploit can be used to send malicious files without being noticed. Unlike a lot of other tactics

used by hackers, brute force attacks aren't reliant on existing vulnerabilities

This blog post introduces our newest addition to our pentestion arsenal, the ssh-putty-brute.ps1. This tool can turn the well-known PuTTY SSH client (putty.exe or plink.exe) into a reliable SSH login brute force tool which in addition also evades any Antivirus or endpoint protection solution.

4 CROSS SITE SCRIPTING (XSS):

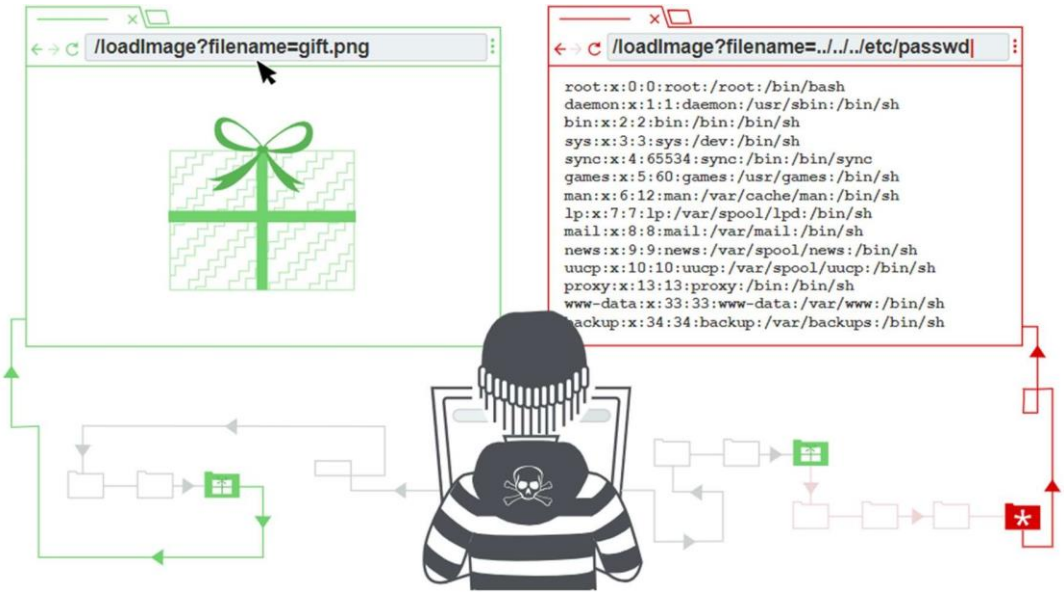
This type of attack is more likely to target websites with scripting flaws. The injection of malicious code into web applications is known as Cross-Site Scripting. The script will give the hacker access to web app data such as sessions, cookies, and so on.



Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

5 DIRECTORY TRAVERSAL:

Directory Traversal Attack is usually effective on older servers with vulnerabilities and misconfiguration. The root directory is where web pages are stored, however, in this attack, the hacker is after directories outside of the root directory.



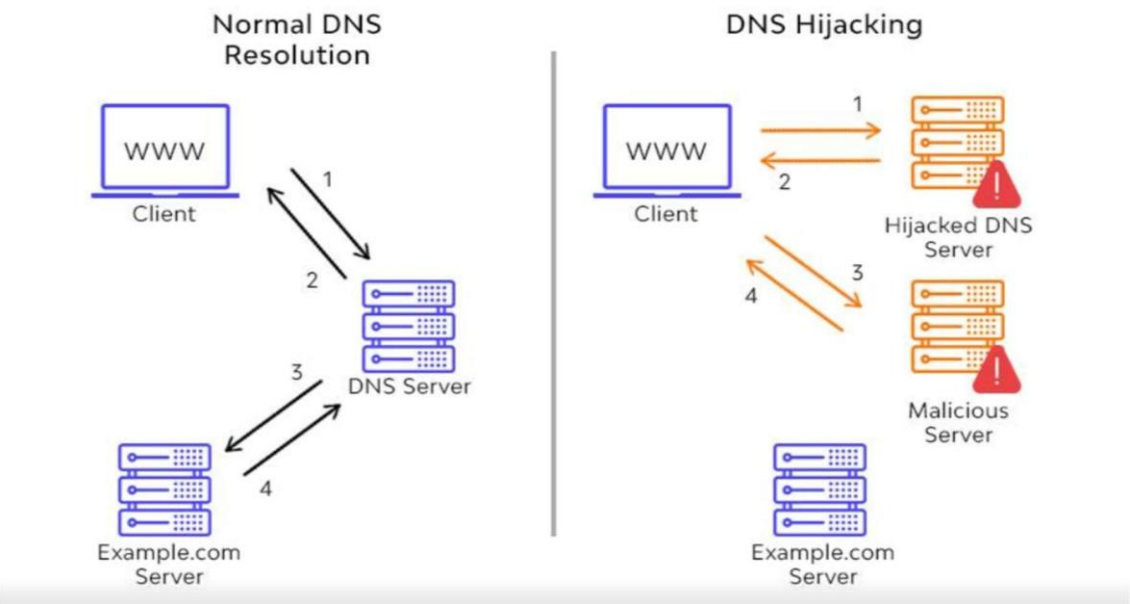
Path traversal is also known as directory traversal. These vulnerabilities enable an attacker to read arbitrary files on the server that is running an application. This might include:

- Application code and data.
- Credentials for back-end systems.
- Sensitive operating system files.

In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server.

6 DNS SERVER HIJACKING:

DNS Hijacking refers to any attack that tricks the end-user into thinking he or she is communicating with a legitimate domain name when in reality they are communicating with a domain name or IP address that the attacker has set up. DNS Redirection is another name for this.

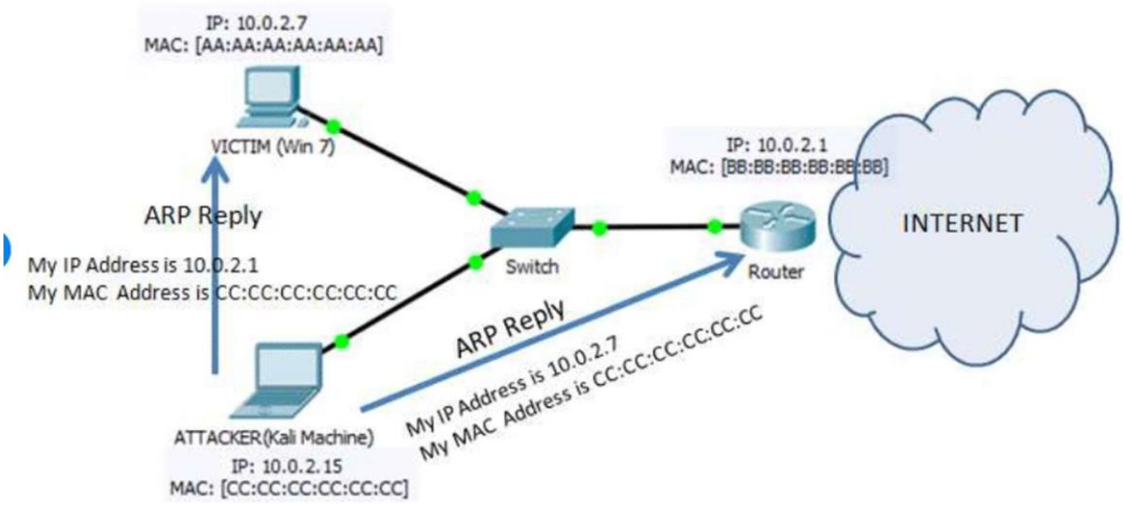


DNS hijacking is an attack on a domain name system (DNS). In some cases, it could be an attack on the DNS to make it unavailable for use, while in others, it could be a stealth mode of redirecting the website's users to go to an alternative website. Either way, DNS hijacking attacks use the DNS as a significant part of the attack process. Usually, during a DNS hijacking, attackers incorrectly resolve DNS queries sent by users and redirect them to bogus sites without the users' notice. Afterward, the website user inadvertently proceeds to the linked harmful website or continues using the internet on a server that cyber attackers have compromised.

7 MITM ATTACK:

Man-in-the-Middle (MITM) attack allows the attacker to access sensitive information by blocking and modifying the connection between the end-user and web servers. In MITM attacks or smells, the hacker captures or corrects modified messages between the user and the web server by listening or intervening in the connection. This allows the attacker to steal sensitive user information such as online banking details, usernames, passwords, etc., which are transmitted

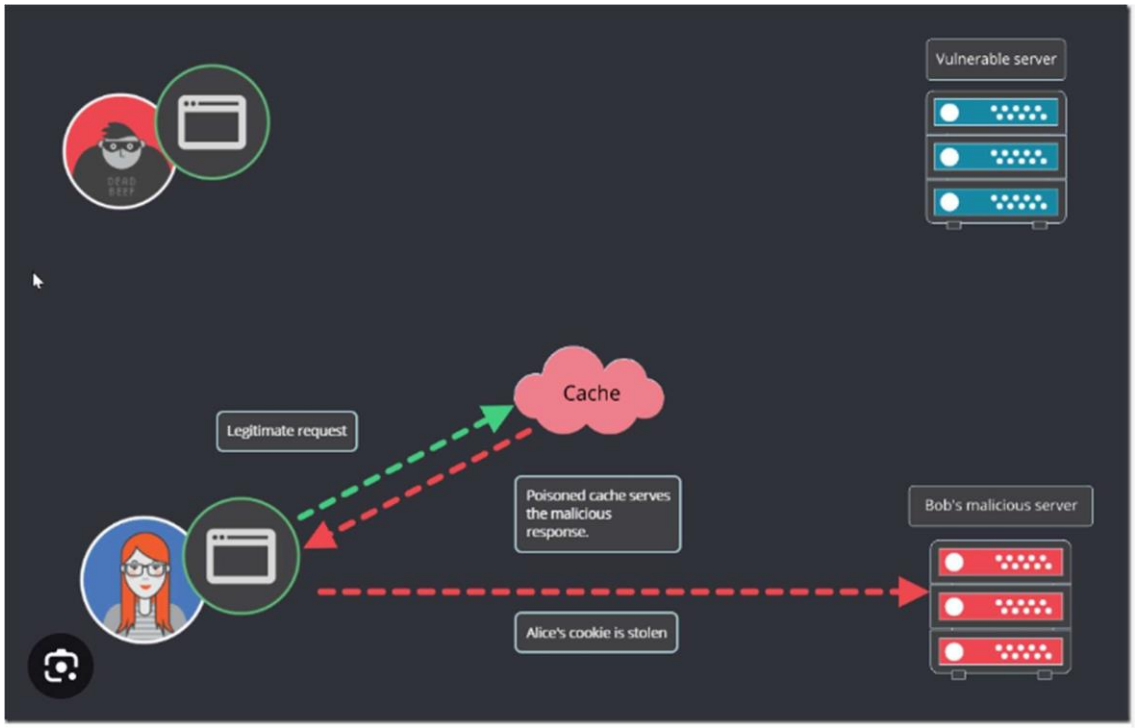
online to the webserver. The attacker entices the victim to attach to an Internet server by pretending to be an agent



Sample MITM Attack by Deceiving Gateway.

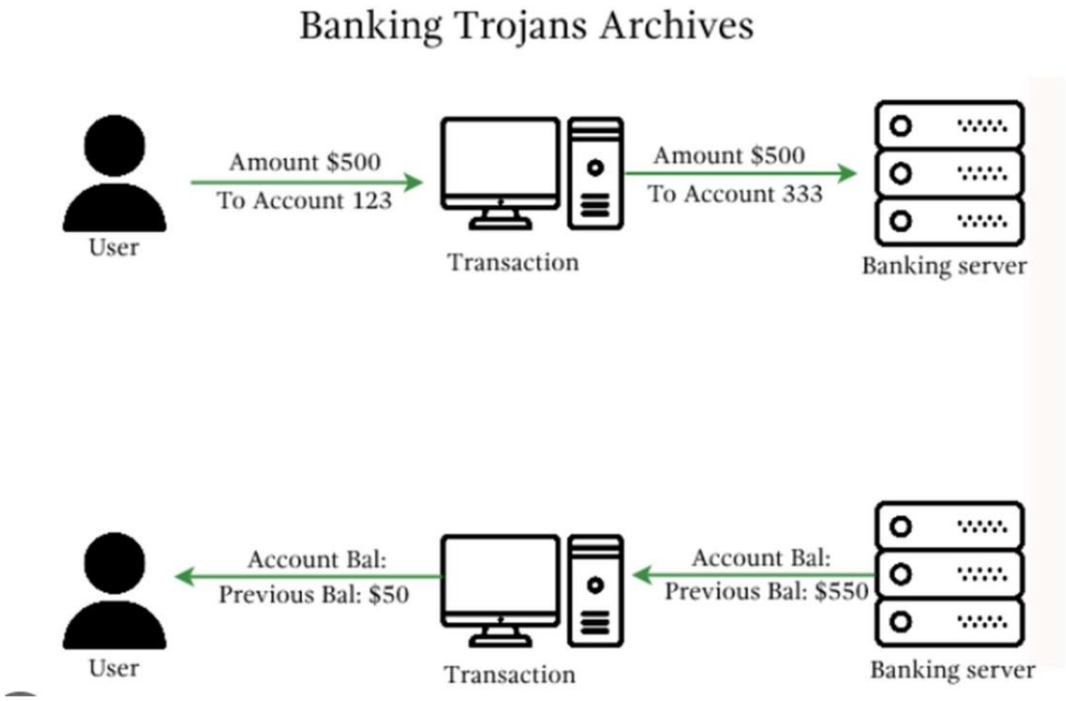
8 HTTP RESPONSE SPLITTING ATTACK:

HTTP Response Splitting is a protocol manipulation attack, similar to Parameter Tampering. Only programs that use HTTP to exchange data are vulnerable to this attack. Because the entry point is in the user viewable data, it works just as well with HTTPS. The attack can be carried out in a variety of ways.



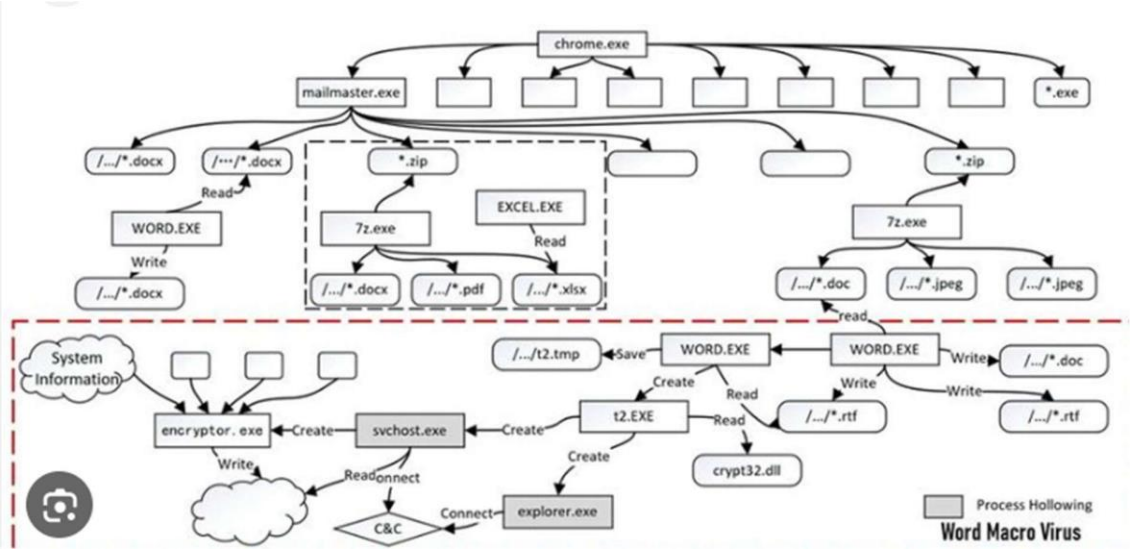
9. Trojans

A Trojan is not a virus, though it is part of the "malware" family. Unlike a computer virus, a Trojan Horse doesn't replicate itself by infecting other files or computers. A trojan is a decoy that may well end up downloading viruses onto your machine, but it is not itself a virus. A Trojan is basically a small piece of malicious software hidden inside a useful program. Once installed, a Trojan can:



10. Macro viruses

Macro viruses infect applications like Microsoft Word or Excel. They're called macro viruses because they're written in the macro language used by the apps they infect. A macro language is a simple programming language that enables users to write and execute automated tasks in sequence. That "shortcut" is called a macro. If macros are enabled in the app, legitimate macros and macro viruses will run during an application's initialization sequence. Thankfully, Microsoft has now disabled them by default, but many users enable them to work more productively. Hence, despite Microsoft's mitigation, macro viruses remain a serious infection vector.


chrome.exe
mailmaster.exe
*.exe
/.../*.docx
/···/*.docx
*.zip
*.zip
Read
WORD.EXE
Write
/.../*.docx
7z.exe
EXCEL.EXE
Read
/.../*.docx
/.../*.pdf
/.../*.xlsx
7z.exe
/.../*.doc
/.../*.jpeg
/.../*.jpeg
read
System Information
/.../t2.tmp
Save
WORD.EXE
WORD.EXE
Write
/.../*.doc
Create
Read
Write
Write
encryptor.exe
Create
svchost.exe
Create
t2.EXE
Read
/.../*.rtf
/.../*.rtf
Write
Read
onnect
Create
crypt32.dll
C&C
Connect
explorer.exe
Process Hollowing
Word Macro Virus