Well Knowns Topics of Security

Cyber hijacking:

Cyber hijacking, or computer hijacking, is a type of network security attack in which the attacker takes control of computer systems, software programs, and/or network communications.

A wide range of cyber-attacks rely on hijacking in one form or another, and -- similar to other hijackings, such as an airplane hijacker or criminals seizing control of an armored transport vehicle.

There are several different kinds of cyber hijacking, among them:

I. browser hijacking

II. session hijacking

III. domain hijacking

IV. clipboard hijacking

V. domain name system (DNS) hijacking

VI. Internet Protocol (IP) hijacking

VII. page hijacking

Browser Hijacking: is a tactic used by hackers and unscrupulous online advertisers to take control of a web browser. In practice, browser hijacking is most often used to redirect web traffic, alter default browser settings or force a victim to click advertisements. However, there are also instances where hackers use hijacked browsers to intercept sensitive information and even make unwitting victims download additional malware.

Session Hijacking: is a type of computer hijacking where hackers gain unauthorized access to a victim's online account or profile by intercepting or cracking session tokens. Session tokens are cookies sent from a web server to users to verify their identity and website settings. If a hacker successfully cracks a user's session token, the results can range from eavesdropping to the insertion of malicious JavaScript programs.

Domain Hijacking: Domain hijacking or domain theft is the act of changing the registration of a domain name without the permission of its original registrant, or by abuse of privileges on domain hosting and registrar software systems.

DNS Hijacking: DNS hijacking and domain hijacking are similar in that both are attempts to hijack control of a web domain. DNS hijacking describes the takeover in a technical sense, however, whereas domain hijacking is a takeover by way of legal coercion or social engineering.

Clipboard Hijacking: When you use your device to copy and paste images, text and other information, the act of copying temporarily stores that data in random access memory (RAM). This section of RAM is known as the *clipboard*.

Clipboard Hijacking happens when hackers replace the contents of a victim's clipboard with their own -- often malicious -- content. Depending on the technical ability of the attacker, clipboard hijacking can be hard to detect and may be spread inadvertently by victims when they paste information into web forms.

Page Hijacking: Also known as *302 redirect hijacking* or *Uniform Resource Locator (URL) hijacking*, a page hijacking attack tricks web crawlers used by search engines to redirect traffic the hacker's way. The web community introduced 302 HTTP responses to provide website owners a way to temporarily redirect users -- and search engine crawlers -- to a different URL in cases where a website is undergoing maintenance or testing.

Internet Protocol Hijacking: this happens when an attacker hacks or masquerades as an internet provider claiming to own an IP address it doesn't. When this happens, traffic destined for one network is redirected to the hacker's network. The hacker then becomes a man in the middle and can carry out a range of attacks from eavesdropping to packet injection -- covertly inserting forged packets into a communication stream.

General Terms in Cyber Security:

Vulnerability: A weakness that can be exploited.

Threat: One who exploits a vulnerability.

Risk: Damage caused by exploiting the vulnerability.

Asset: This needs to be accessed after exploitation.

Bug: Error, fault, or flaw in a computer program that may cause unexpected behavior.

Hacker: Gain access with or without malicious intent.

Pivoting:

Pivoting is a hacking tactic that is used to move from a compromised system to another system/network/VLAN using information/credentials from the original compromised system to “pivot” to a different system.

Pivoting refers to a method used by penetration testers that use the compromised system to **attack** other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines.

Sniffing & Snoofing:

In **sniffing**, the attacker listens to a network’s data traffic and captures data packets using packet sniffers.

There are two types of sniffing attacks, active sniffing, and passive sniffing.

- **Active sniffing** – this is sniffing that is conducted on a switched 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.
- **Passive sniffing** – passive sniffing uses hubs instead of switches. Hubs perform the same way as switches only that they do use MAC addresses to read the destination ports of data. All an attacker needs to do is simply connect to LAN and they are able to sniff data traffic in that network.

How to Prevent Sniffing Attacks:

Untrusted networks: users should avoid connecting to unsecured networks, which include free public Wi-Fi.

Encryption: Encryption is the process of converting plaintext into gibberish in order to protect the message from attackers.

Network scanning and monitoring: Network administrators should scan and monitor their networks to detect any suspicious traffic. This can be achieved by bandwidth monitoring or device auditing.

Snoofing:

In **spoofing**, the attacker steals the credentials of a user and uses them in a system as a legitimate user. Spoofing attacks are also referred to as **man–in–the–middle** attacks since the attacker gets in the middle of a user and a system.

An **E-mail spoofing** targets the user while an IP spoofing is predominantly targeted at a network.

In an **IP spoofing attack**, the attacker attempts to obtain illicit and illegal access to a network through messages with a bogus or spoofed IP address to deceive and show it off as a message from a trusted source. This is achieved by using a genuine host's IP address and varying the packet headers led from their personal system to mimic it as an original and a trusted computer's IP address.

DATA EXFILTRATION

Data exfiltration is sometimes referred to as data extrusion, data exportation, or data theft. All of these terms are used to describe the unauthorized transfer of data from a computer or other device.

Data exfiltration can be conducted manually, by an individual with physical access to a computer, but it can also be an automated process conducted through malicious programming over a network.

Basically, data exfiltration is a form of security breach that occurs when an individual's or company's data is copied, transferred, or retrieved from a computer or server without authorization.

POWERSHELL & COMMAND PROMPT:

PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language.

It can operate with both batch commands and PowerShell cmdlets.

It has access to programming libraries as it is built on the .NET framework.

Command prompt or cmd is a default application of Windows that is used to interact with any Windows objects in the windows os. It enables users to directly interact with the system. It is most widely used for executing batch files or running simple utilities.

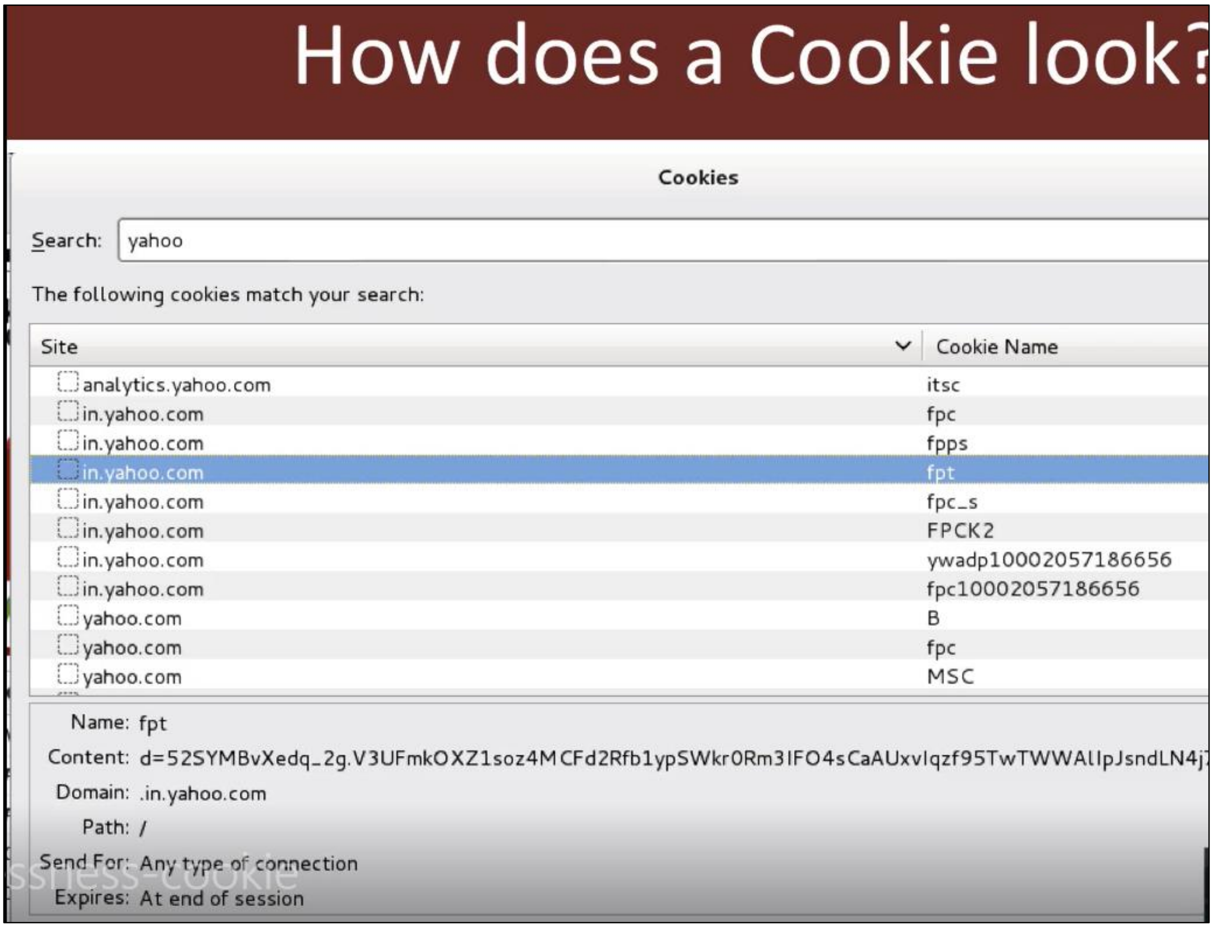
It can work only with batch commands.

No such access to libraries.

COOKIES:

Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience. Data stored in a cookie is created by the server upon your connection.

This data is labelled with an ID unique to you and your computer. When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you.



How does a Cookie look?

Cookies

Search: yahoo

The following cookies match your search:

Site	Cookie Name
analytics.yahoo.com	itsc
in.yahoo.com	fpc
in.yahoo.com	fpps
in.yahoo.com	fpt
in.yahoo.com	fpc_s
in.yahoo.com	FPCK2
in.yahoo.com	ywadp10002057186656
in.yahoo.com	fpc10002057186656
yahoo.com	B
yahoo.com	fpc
yahoo.com	MSC

Name: fpt
Content: d=52SYMBvXedq_2g.V3UFmkOXZ1soz4MCFd2Rfb1ypSWkr0Rm3IFO4sCaAUxvlqzf95TwTWWAlIpJsndLN4j
Domain: .in.yahoo.com
Path: /
Send For: Any type of connection
Expires: At end of session

Bug Bounty:

A **bug bounty** program, also called a **vulnerability rewards program** (VRP), is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs. ... Bug reports must document enough information for the organization offering the **bounty** to be able to reproduce the vulnerability.

Payload:

Payload is a simple script that the **hackers** utilize to interact with a **hacked** system. Using **payloads**, they can transfer data to a victim system.

Lateral Movement:

Network Lateral Movement, or simply **"Lateral Movement"**, refers to the techniques that cyber attackers, or "threat actors", use to progressively move through a network as they search for the key data and assets that are ultimately the target of their attack campaigns.

Reverse and Bind shell:

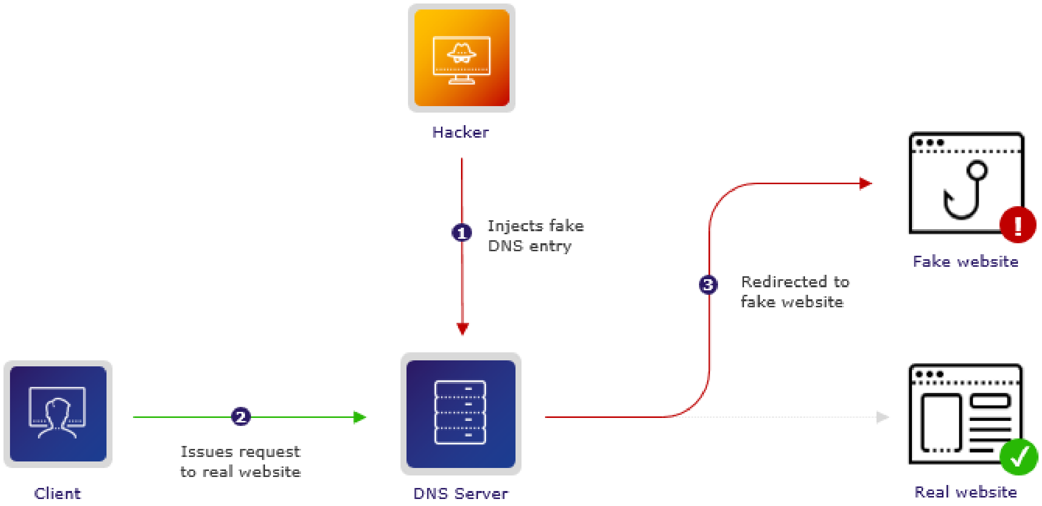
A **reverse shell** is a **shell** initiated from the target host back to the attack box which is in a listening state to pick up the **shell.**

A **bind shell** is set up on the target host and binds to a specific port to listens for an incoming connection from the attack box.

DNS Cache Poisioning/DNS Spoofing:

DNS cache poisoning is the act of entering false information into a **DNS cache**, so that **DNS** queries return an incorrect response and users are directed to the wrong websites. **DNS cache poisoning** is also known as '**DNS spoofing**.

DNS poisoning takes advantage of weaknesses in this process to redirect traffic to an illegitimate IP address. Specifically, hackers gain access to a DNS server so that they can adjust its directory to point the domain name users enter to a different, incorrect IP address.



Once someone gains access to a DNS server and begins redirecting traffic, they are engaging in DNS spoofing.

DNS cache poisoning takes this one step further. When DNS cache poisoning happens, a user's device places the illegitimate IP address in its cache (aka memory). This means that the device will automatically direct the user to the illegitimate IP address -- even after the issue is resolved.

The current process is built on what's called the User Datagram Protocol (UDP), a process that does not require senders or recipients to verify they are ready to communicate or verify who they are. This vulnerability allows hackers to fake identity information (which requires no additional verification) and step into the process to start redirecting DNS servers.

While this is absolutely an enormous vulnerability, it is not as simple as it sounds.

A hacker must respond to a request within a few milliseconds before the authoritative server.

The attacker should know request ID.

Attacker should know in which authoritative server request is send by DNS server.

Some of the best ways to protect your organization from DNS Cache Poisoning/DNS Spoofing:

1-Introduce DNS Security Extensions (DNSSEC).

2- Always encrypt data.

3- Enable secure DNS configurations.

4- Regularly run system updates

VA and PT:

Vulnerability Assessment is the process of finding flaws on the target. Here, the organization knows that their system/network has flaws or weaknesses and want to find these flaws and prioritize the flaws for fixing.

Penetration Testing is the process of finding vulnerabilities on the target. In this case, the organization would have set up all the security measures they could think of and would want to test if there is any other way that their system/network can be hacked.

HIDS and NIDS

HIDS (Host IDS) and **NIDS (Network IDS)** are both Intrusion Detection System and work for the same purpose i.e., to detect the intrusions. The only difference is that the **HIDS** is set up on a particular host/device. It monitors the traffic of a particular device and suspicious system activities. On the other hand, **NIDS** is set up on a network. It monitors traffic of all device of the network.

Data Leakage

Data Leakage is an intentional or unintentional transmission of data from within the organization to an external unauthorized destination. It is the disclosure of confidential information to an unauthorized entity. Data Leakage can be divided into 3 categories based on how it happens:

1. **Accidental Breach**: An entity unintentionally send data to an unauthorized person due to a fault or a blunder
2. **Intentional Breach**: The authorized entity sends data to an unauthorized entity on purpose
3. **System Hack**: Hacking techniques are used to cause data leakage.

Data Leakage can be prevented by using tools, software and strategies known as DLP tools.

Brute Force Attack. How can you prevent it?

Brute Force is a way of finding out the right credentials by repetitively trying all the permutations and combinations of possible credentials. In most cases, brute force attacks are automated where the tool/software automatically tries to login with a list of credentials. There are various ways to prevent Brute Force attacks. Some of them are:

- **Password Length**: You can set a minimum length for password. The lengthier the password, the harder it is to find.
- **Password Complexity**: Including different formats of characters in the password makes brute force attacks harder. Using alpha-numeric passwords along with special characters, and upper and lower case characters increase the password complexity making it difficult to be cracked.
- **Limiting Login Attempts**: Set a limit on login failures. For example, you can set the limit on login failures as 3. So, when there are 3 consecutive login failures, restrict the user from logging in for some time, or send an Email or OTP to use to log in the next time. Because brute force is an automated process, limiting login attempts will break the brute force process.

ARP:

Address Resolution Protocol (ARP)is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

Msfvenom:

It is a command line instance of Metasploit that is **used** to generate and output all of the various types of shell code that are available in Metasploit.

Impersonation Attack:

An impersonation attack is a form of **fraud in which attackers pose as a known or trusted person to dupe an employee into transferring money to a fraudulent account, sharing sensitive information** (such as intellectual property, financial data or payroll information), or revealing login credentials that attackers can used to hack into a company's computer network.

Wevtutil Tool:

Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.

Custom command and control protocol:

are used by the adversaries to communicate with malware/trojan and exfiltrate the data. These channels mimic well-known protocols (i.e., HTTP, DNS) or follow custom protocols.

Sessions Vs Cookies:

The main **difference between** a **session** and a **cookie is** that **session** data **is** stored on the server, whereas **cookies** store data **in the** visitor's browser. **Sessions** are more secure than **cookies** as it **is** stored in server.
Data stored in cookie can be stored for months or years, depending on the life span of the cookie. But the data in the session is lost when the web browser is closed.

Cookies are stored in the browser as a text file format. It stores a limited amount of data, up to **4kb[4096bytes]**. A single Cookie cannot hold multiple values but yes we can have more than one cookie.

There is no such storage limit on session. Sessions can hold multiple variables. Since they are not easily accessible hence are more secure than cookies.

SAM File:

The **Security Account Manager** (**SAM**) is a database file[1] in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users.

Peinjector:

The executable file format on the Windows platform is PE COFF. The peinjector provides different ways to infect these files with custom payloads without changing the original functionality. It creates patches, which are then applied **seamlessly during file transfer**. It is very performant, lightweight, modular and can be **operated on embedded hardware**

Session ID:

Session ID is unique identifier or token to identify user and session.

May be provided to both authenticated and anonymous users.

It can be stored in url, form field, cookies etc.

Ideal session ID:

1-Should be long and random.

2-Name should not suggest functionality.

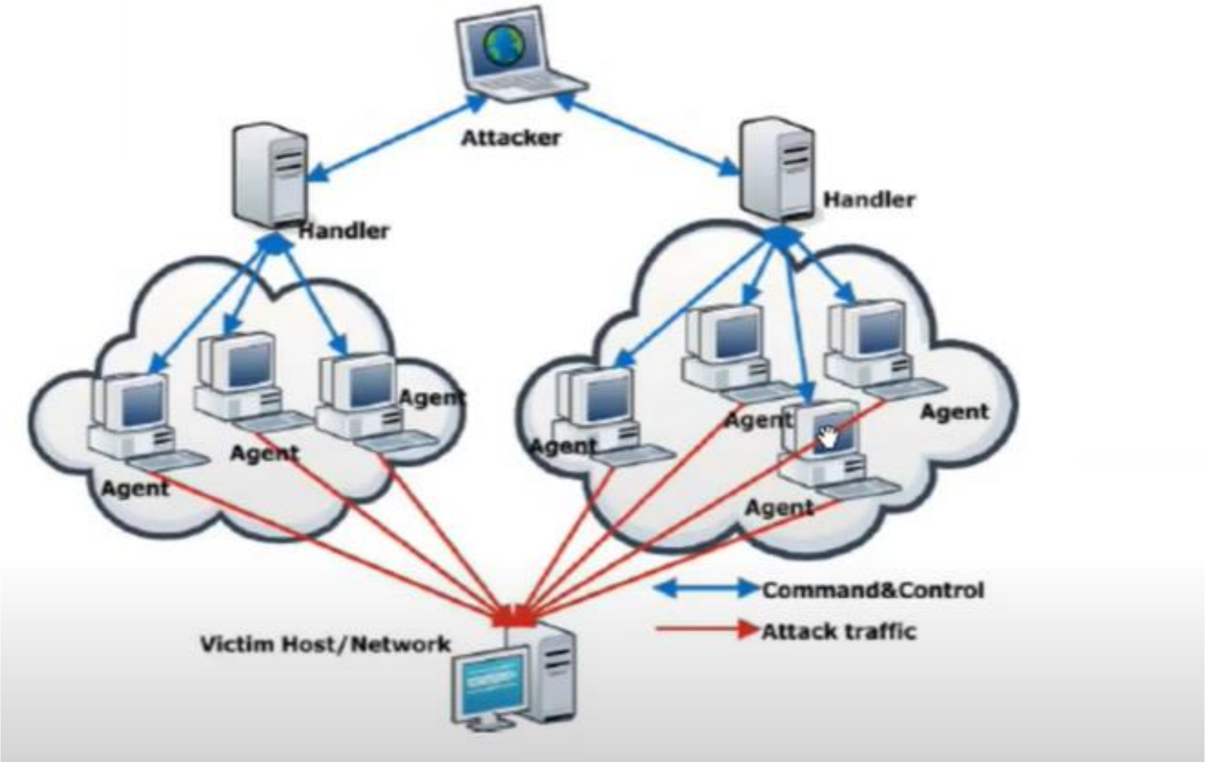
3-Should automatically timeout and should never be recycled.

4-Should not be derived using shared secret **eg**: password and username.

5-Sent through secure channel.

BOTNET:

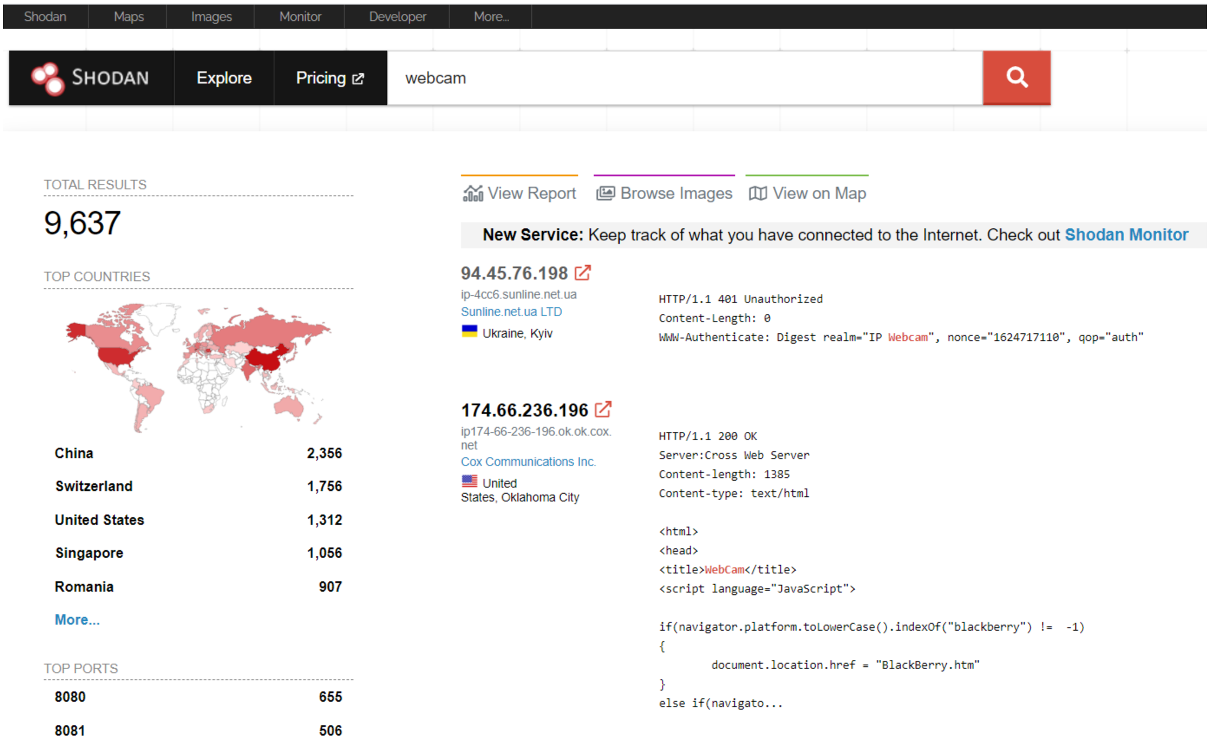
A botnet is an internet connected devices which may include PCs, servers, mobile devices that are infected from a common type of malware. Users are often unaware of a botnet infecting their systems.



Shodan Search Engine:

It is a type of search engine which is used to collect data of **IOT (Internet of things)** means devices which are connected with internet.

It also provides exploits of different services. For using these options, you know about the version of that particular service whose exploit are you searching.



TOTAL RESULTS

9,637

TOP COUNTRIES

China	2,356
Switzerland	1,756
United States	1,312
Singapore	1,056
Romania	907

More...

TOP PORTS

8080	655
8081	506

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

94.45.76.198
ip-4cc6.sunline.net.ua
Sunline.net.ua LTD
Ukraine, Kyiv

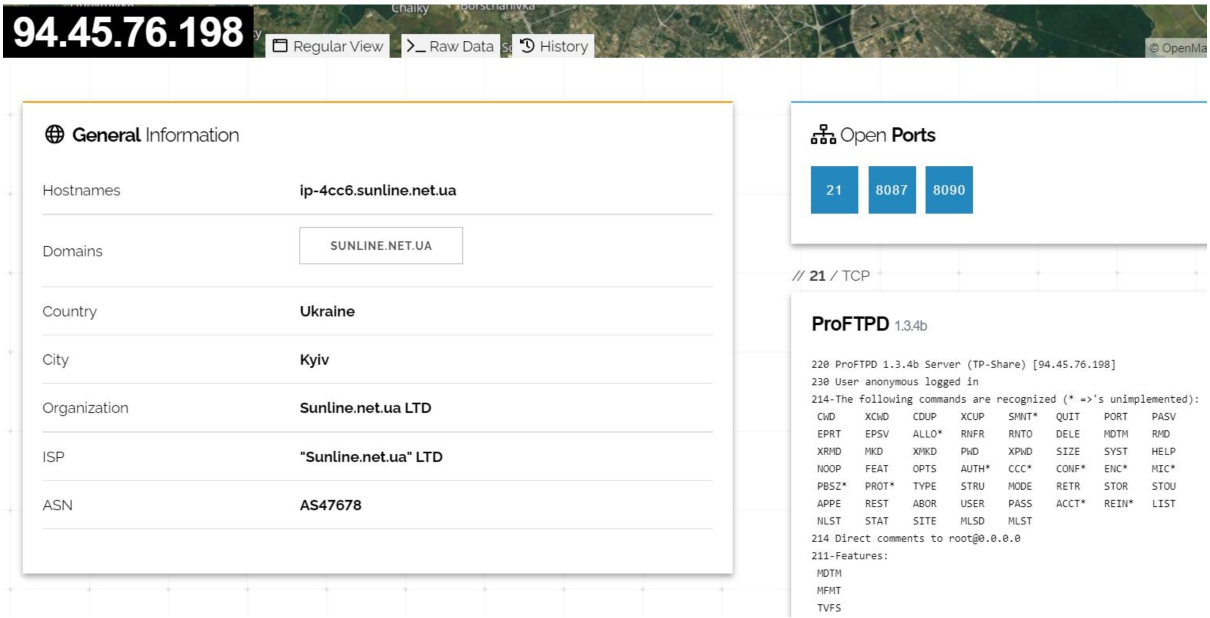
```
HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1624717110", qop="auth"
```

174.66.236.196
ip174-66-236-196.ok.ok.cox.net
Cox Communications Inc.
United States, Oklahoma City

```
HTTP/1.1 200 OK
Server:Cross Web Server
Content-length: 1385
Content-type: text/html

<html>
<head>
<title>WebCam</title>
<script language="JavaScript">

if(navigator.platform.toLowerCase().indexOf("blackberry") !=  -1)
{
        document.location.href = "BlackBerry.htm"
}
else if(navigato...
```

In the left-hand side, you will see all the required details like total results, countries which are using webcam, top ports, top services running on it, operating system details and many more.

Now I am going to open IP : 94.45.76.198 and will show the details related to this IP.



General Information

Hostnames	ip-4cc6.sunline.net.ua
Domains	SUNLINE.NET.UA
Country	Ukraine
City	Kyiv
Organization	Sunline.net.ua LTD
ISP	"Sunline.net.ua" LTD
ASN	AS47678

Open Ports

21 8087 8090

// 21 / TCP

ProFTPD 1.3.4b

```
220 ProFTPD 1.3.4b Server (TP-Share) [94.45.76.198]
230 User anonymous logged in
214-The following commands are recognized (* =>'s unimplemented):
 CWD     XCWD    CDUP    XCUP    SMNT*   QUIT    PORT    PASV
 EPRT    EPSV    ALLO*   RNFR    RNTO    DELE    MDTM    RMD
 XRMD    MKD     XMKD    PWD     XPWD    SIZE    SYST    HELP
 NOOP    FEAT    OPTS    AUTH*   CCC*    CONF*   ENC*    MIC*
 PBSZ*   PROT*   TYPE    STRU    MODE    RETR    STOR    STOU
 APPE    REST    ABOR    USER    PASS    ACCT*   REIN*   LIST
 NLST    STAT    SITE    MLSD    MLST
214 Direct comments to root@0.0.0.0
211-Features:
 MDTM
 MFMT
 TVFS
```

As you see 3 ports are open on this public IP and also give the details of services running on this public IP.

With the help of Shodan you can search for all devices like web servers, routers, anything which is connected through internet.

HTTRACK:

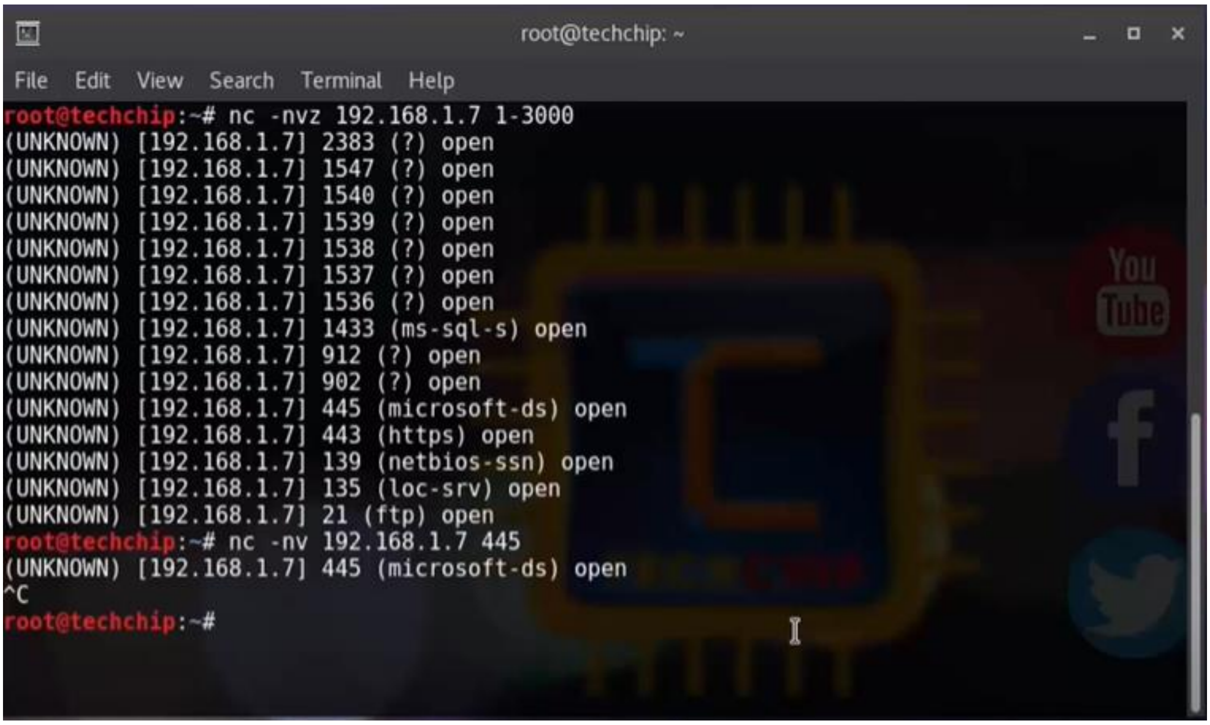
HTTrack is a free (GPL, libre/free software) and easy-to-**use** offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

This tool is available in kali Linux.

Netcat:

Netcat aka nc is a network utility for reading from and writing to network connections using TCP and UDP.
Netcat is very useful to both attacks and the network security auditors.
For an attacking purpose it is a multi-functional tool which accurate and useful. Security auditors uses Netcat to debug and investigate the network.

It's often referred to as the **Swiss Army knife of hacking tools** because it can do several things as both a client and a server during hacking adventures.



```
root@techchip:~# nc -nvz 192.168.1.7 1-3000
(UNKNOWN) [192.168.1.7] 2383 (?) open
(UNKNOWN) [192.168.1.7] 1547 (?) open
(UNKNOWN) [192.168.1.7] 1540 (?) open
(UNKNOWN) [192.168.1.7] 1539 (?) open
(UNKNOWN) [192.168.1.7] 1538 (?) open
(UNKNOWN) [192.168.1.7] 1537 (?) open
(UNKNOWN) [192.168.1.7] 1536 (?) open
(UNKNOWN) [192.168.1.7] 1433 (ms-sql-s) open
(UNKNOWN) [192.168.1.7] 912 (?) open
(UNKNOWN) [192.168.1.7] 902 (?) open
(UNKNOWN) [192.168.1.7] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.7] 443 (https) open
(UNKNOWN) [192.168.1.7] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.7] 135 (loc-srv) open
(UNKNOWN) [192.168.1.7] 21 (ftp) open
root@techchip:~# nc -nv 192.168.1.7 445
(UNKNOWN) [192.168.1.7] 445 (microsoft-ds) open
^C
root@techchip:~#
```

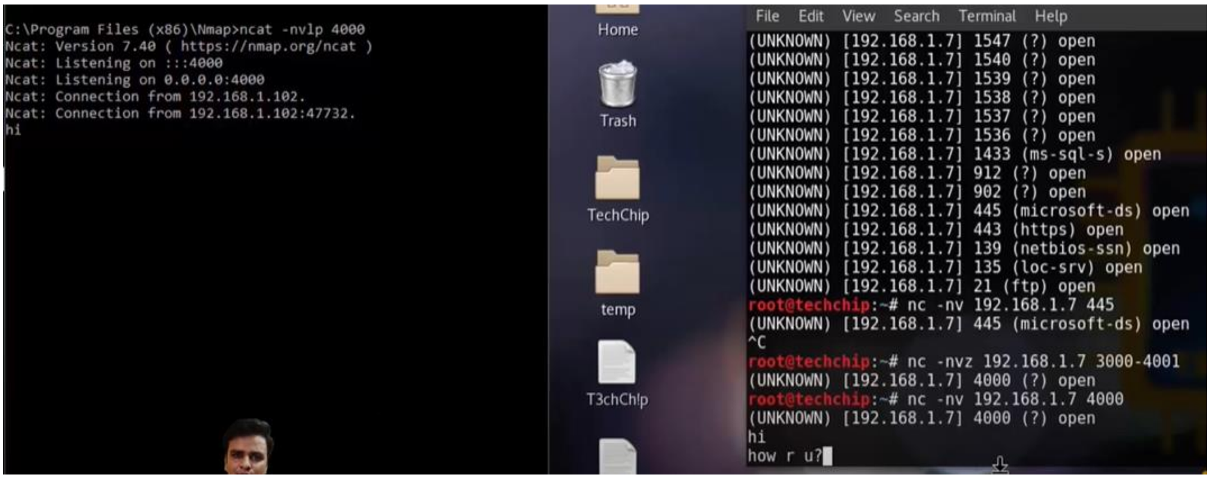
In the above screen shot I have shown you how we use netcat for scanning of ports as well as I have also successfully connected to port 445.

Netcat also used for opening ports on machine with the help of below command:

ncat -nvlp 4000

v: verbose l: listening p: port

We can use netcat for chatting purpose as shown below:

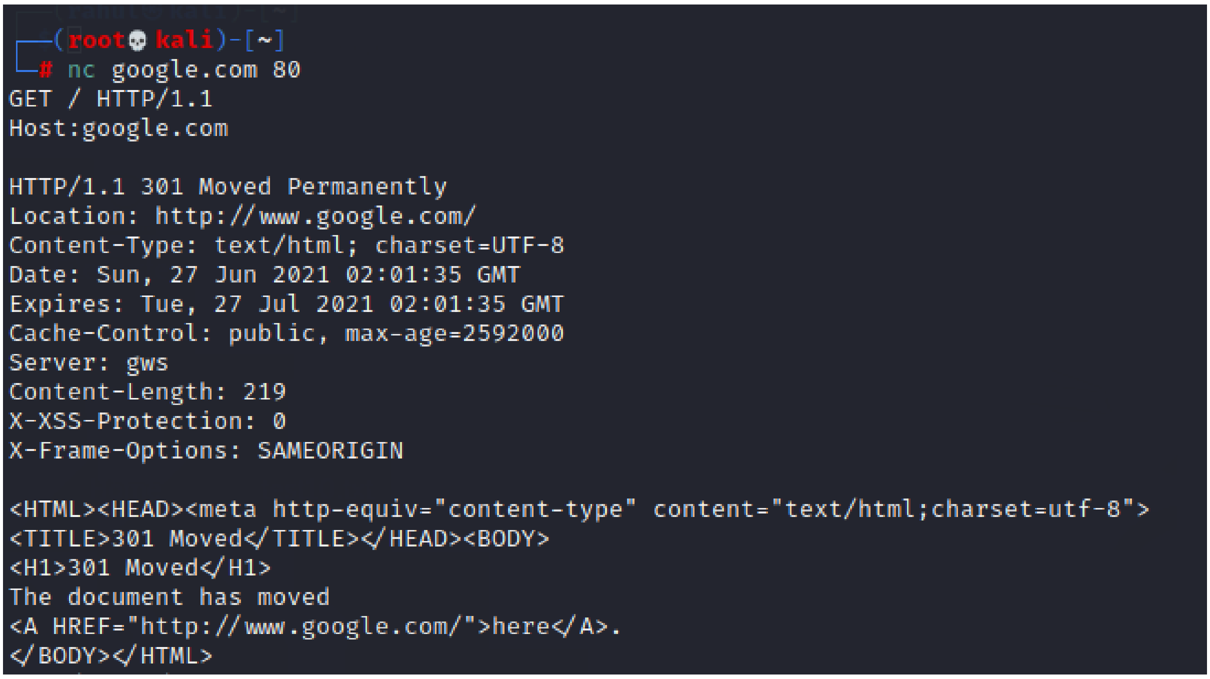


```
C:\Program Files (x86)\Nmap>ncat -nvlp 4000
Ncat: Version 7.40 ( https://nmap.org/ncat )
Ncat: Listening on :::4000
Ncat: Listening on 0.0.0.0:4000
Ncat: Connection from 192.168.1.102.
Ncat: Connection from 192.168.1.102:47732.
hi
```

```
(UNKNOWN) [192.168.1.7] 1547 (?) open
(UNKNOWN) [192.168.1.7] 1540 (?) open
(UNKNOWN) [192.168.1.7] 1539 (?) open
(UNKNOWN) [192.168.1.7] 1538 (?) open
(UNKNOWN) [192.168.1.7] 1537 (?) open
(UNKNOWN) [192.168.1.7] 1536 (?) open
(UNKNOWN) [192.168.1.7] 1433 (ms-sql-s) open
(UNKNOWN) [192.168.1.7] 912 (?) open
(UNKNOWN) [192.168.1.7] 902 (?) open
(UNKNOWN) [192.168.1.7] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.7] 443 (https) open
(UNKNOWN) [192.168.1.7] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.7] 135 (loc-srv) open
(UNKNOWN) [192.168.1.7] 21 (ftp) open
root@techchip:~# nc -nv 192.168.1.7 445
(UNKNOWN) [192.168.1.7] 445 (microsoft-ds) open
^C
root@techchip:~# nc -nvz 192.168.1.7 3000-4001
(UNKNOWN) [192.168.1.7] 4000 (?) open
root@techchip:~# nc -nv 192.168.1.7 4000
(UNKNOWN) [192.168.1.7] 4000 (?) open
hi
how r u?
```

Netcat also used to send and receive data from one system to other.

With the help of netcat you can do http request also.

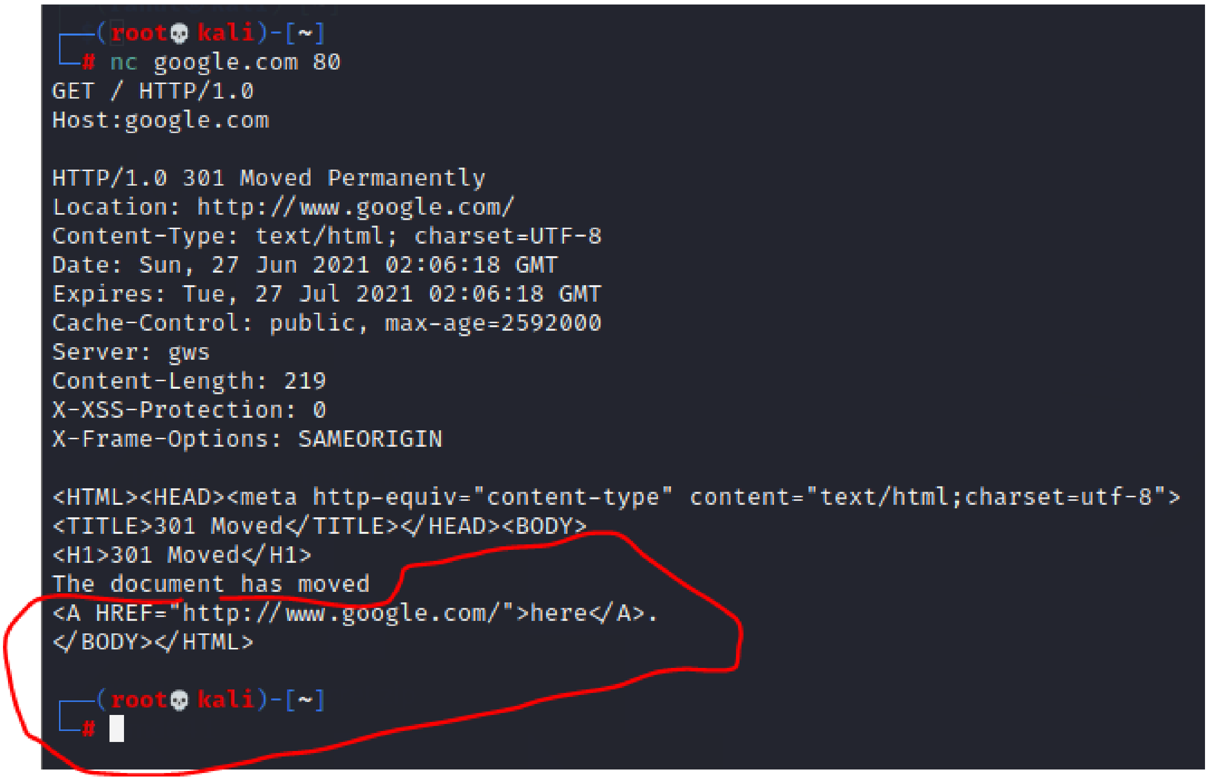


```
┌──(root💀kali)-[~]
└─# nc google.com 80
GET / HTTP/1.1
Host:google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Sun, 27 Jun 2021 02:01:35 GMT
Expires: Tue, 27 Jul 2021 02:01:35 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

Difference between HTTP 1.0 and HTTP 1.1

Http 1.0 is an older version while Http 1.1 is latest.

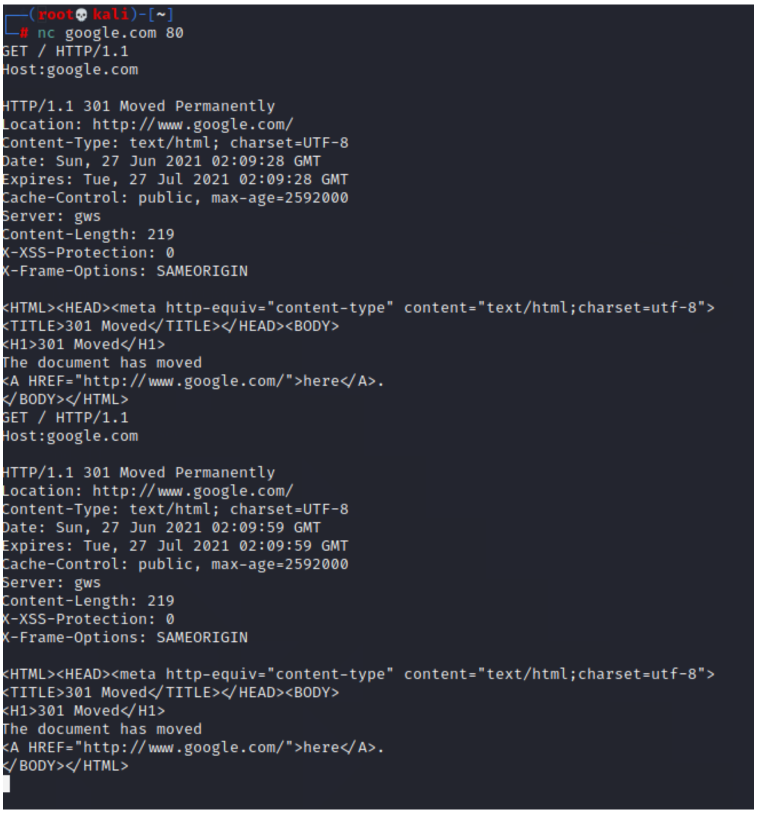
Http 1.0 uses single request to get resource from the server then close the connection as shown in below figure:



```
┌──(root💀kali)-[~]
└─# nc google.com 80
GET / HTTP/1.0
Host:google.com

HTTP/1.0 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Sun, 27 Jun 2021 02:06:18 GMT
Expires: Tue, 27 Jul 2021 02:06:18 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>

┌──(root💀kali)-[~]
└─# 
```

While in Http 1.1 single connection to get request resources from the server many times as shown in figure.

In below figure I have sent 2 GET request to google server but connection is still alive.



```
┌──(root💀kali)-[~]
└─# nc google.com 80
GET / HTTP/1.1
Host:google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Sun, 27 Jun 2021 02:09:28 GMT
Expires: Tue, 27 Jul 2021 02:09:28 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
GET / HTTP/1.1
Host:google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Sun, 27 Jun 2021 02:09:59 GMT
Expires: Tue, 27 Jul 2021 02:09:59 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
```

OWASP 10 :

OWASP Top 10 is an awareness document that outlines the most critical security risks to web applications. Pentesting is performed according to the OWASP TOP 10 standard to reduce/mitigate security risks.