MALNAD COLLEGE OF ENGINEERING

Under the auspices of M.T.E.S ®
(An Autonomous Institution Affiliated to VTU, Belgaum)
P.B No. 21, Hassan-573202, Karnataka

Computer Networks(21CS603)

Activity-1

Report on Banner Grabbing

Submitted by:

Monisha B R	4MC21CS095
Monisha Ganapati Moger	4MC21CS096
Nandini C N	4MC21CS103

Under the guidance of

Mr. Keerthi K S

Assistant Professor

Department of Computer Science & Engineering

Malnad College of Engineering, Hassan – 573202

Problem Statement :

Perform an experiment to grab a banner with telnet and perform the task using Netcat utility.

Banner Grabbing

Banner grabbing is a method used by attackers and security teams to obtain information about network computer systems and services running on open ports. A banner is a text displayed by a host that provides details such as the type and version of software running on the system or server. The screen displays the software version number on the network server and other system information, giving cybercriminals an advantage in cyber attacks.
Banner grabbing considers collecting software banner information such as name and version. Hackers can use the OSINT tool to get the banners manually or automatically. Banner capture is one of the essential steps in both offensive and defensive penetration testing environments.

Types of Banner Grabbing:

- **Active Banner Grabbing**: In this method, Hackers send packets to a remote server and analyse the response data. The attack involves opening a TCP or similar connection between the origin and the remote server. An Intrusion Detection System (IDS) can easily detect an active banner.

- **Passive Banner Capture**: This method allows hackers and security analysts to get the same information while avoiding disclosing the original connection. In passive banner grabbing, the attackers deploy software and malware as a gateway to prevent direct connection when collecting data from the target. This technique uses third-party network tools and services to capture and analyse packets to identify the software and version being used. run on the server.

TELNET

TELNET is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO. The computer which starts the connection is known as the local computer. The computer which is being connected to i.e. which accepts the connection known as the remote computer. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle.

History of TELNET:

The Telnet protocol originated in the late 1960s, it was created to provide remote terminal access and control over mainframes and minicomputers. Initially, it was designed to be a simple and secure method of connecting to a remote system. This protocol allowed users to access remote computers using a terminal or command-line interface. Over time, Telnet's use has diminished due to security concerns, and alternatives like SSH are now preferred for secure remote management.

Logging in TELNET

The logging process can be further categorized into two parts:

- Local Login
- Remote Login

Syntax:

The basic telnet syntax is: telnet [target ip] [port no.]

Key Features of Telnet:

- **Remote Access**: Telnet allows users to remotely access and manage devices and servers.
- **Text-Based Interface**: It provides a text-based interface for interacting with remote systems, which can be used for various administrative tasks.
- **Port Number**: Telnet typically uses port 23 for establishing connections.

- **Session Control**: It allows for control over remote sessions, enabling users to execute commands as if they were physically present at the remote system.
- **Terminal Emulation**: Telnet clients can emulate different types of terminals, making it compatible with a wide range of systems.
- **Authentication**: Basic authentication is required to start a Telnet session, usually in the form of a username and password.

NETCAT

Netcat or NC is a utility tool. It is one of the most commonly used hacking tool.
It's simple but powerful tool that helps us communicate computers over a network. that uses TCP and UDP connections to read and write in a network. It can be used for both attacking and security. In the case of attacking, it helps us to debug the network along with investigating it. It runs on all operating systems.
It can be used to create and manage network connections, transfer files, and even perform port scanning and network discovery.

Syntax :

The basic telnet syntax is: ncat v [target ip] [port no.]

Key features:

- **Port Scanning**: Netcat can scan for open ports on a network, helping to identify services that are running.
- **Port Listening**: It can listen on a specified port, acting as a simple server.
- **Data Transfer**: Netcat can transfer files between computers over a network.
- **Network Debugging**: It can help troubleshoot network issues by allowing raw data transfer and testing.
- **Banner Grabbing**: Netcat can connect to services and grab banners, useful for identifying service versions.
- **Scripting and Automation**: It can be used in scripts to automate network tasks.

Implementation of Banner grabbing

1. **Using Telnet :**

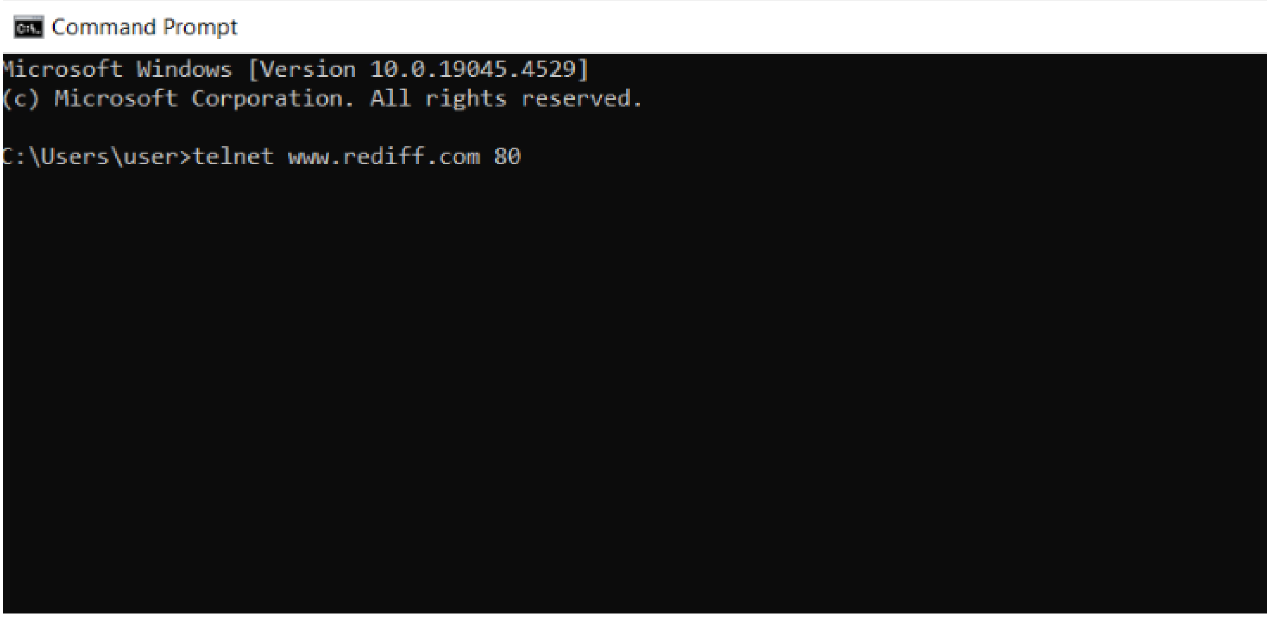
   Steps:

   1. Go to Command Prompt.

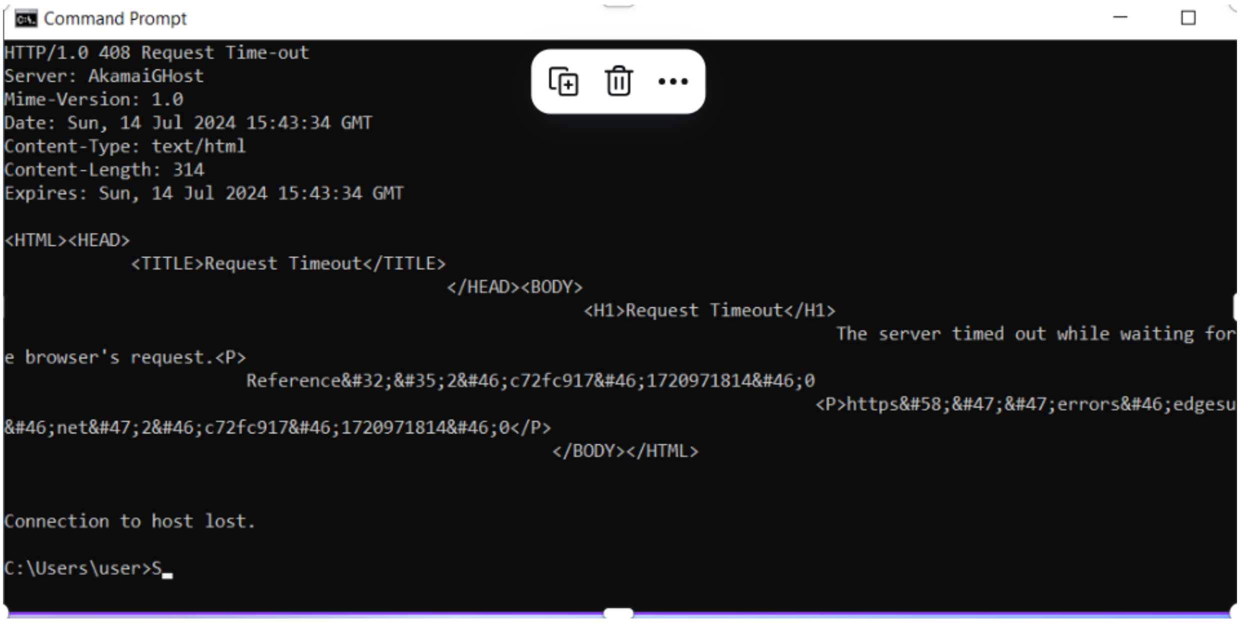
   2. Type telnet followed by IP Address and Port number

   example: telnet www.rediff.com 80 and press enter

   key.



```
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>telnet www.rediff.com 80
```

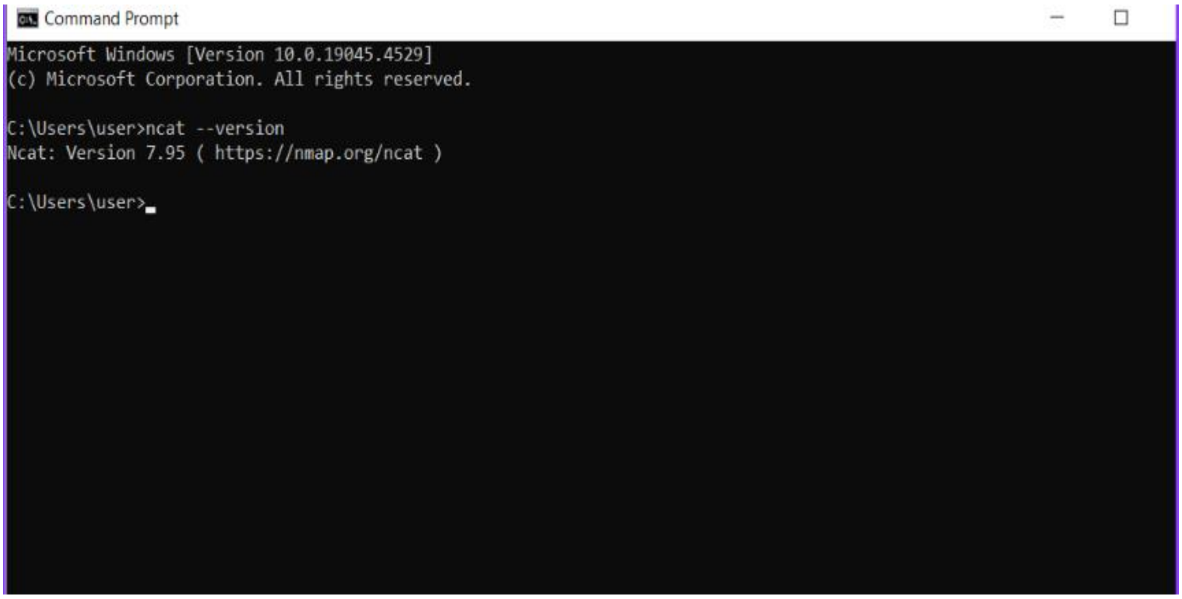


```
HTTP/1.0 408 Request Time-out
Server: AkamaiGHost
Mime-Version: 1.0
Date: Sun, 14 Jul 2024 15:43:34 GMT
Content-Type: text/html
Content-Length: 314
Expires: Sun, 14 Jul 2024 15:43:34 GMT

<HTML><HEAD>
            <TITLE>Request Timeout</TITLE>
                                          </HEAD><BODY>
                                                       <H1>Request Timeout</H1>
                                                                               The server timed out while waiting for
e browser's request.<P>
                       Reference&#32;&#35;2&#46;c72fc917&#46;1720971814&#46;0
                                                                             <P>https&#58;&#47;&#47;errors&#46;edgesu
&#46;net&#47;2&#46;c72fc917&#46;1720971814&#46;0</P>
                                                    </BODY></HTML>


Connection to host lost.

C:\Users\user>S
```

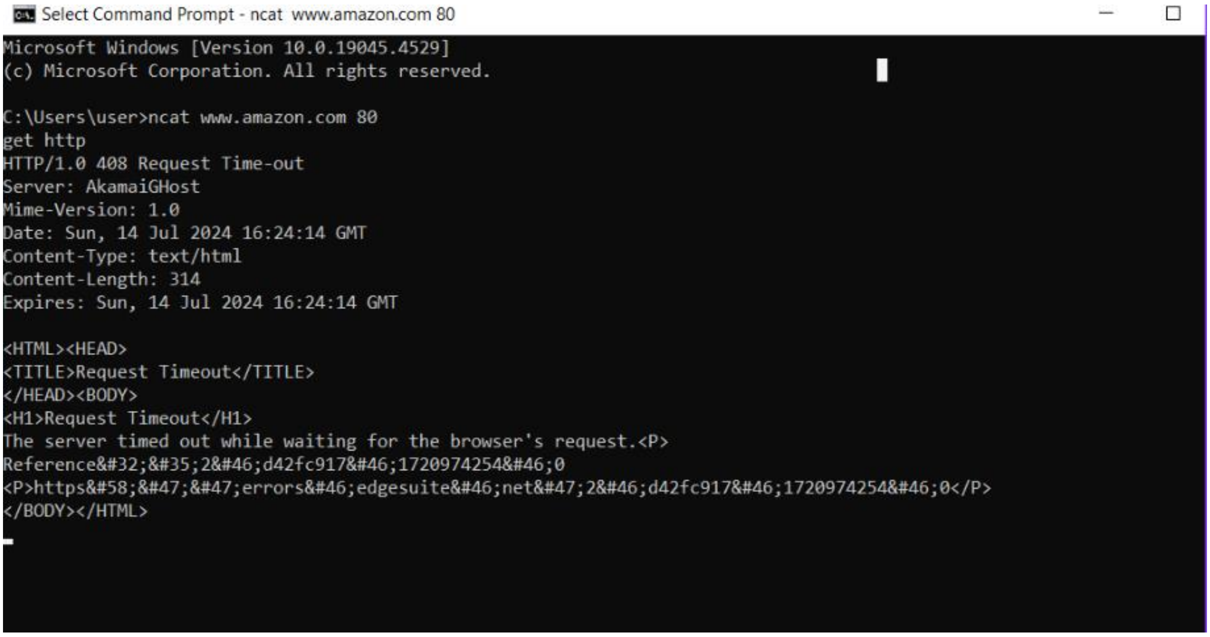
2. Using Netcat :

Steps :

1. Go to Command Prompt we need to check the version of ncat
2. Type ncat followed by IP Address/url port number example: ncat www.amazon.com 80
3. You will get a blinking cursor that you have successfully connected to that TCP port.
4. Then type GET HTTP.



```
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ncat --version
Ncat: Version 7.95 ( https://nmap.org/ncat )

C:\Users\user>
```



```
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>ncat www.amazon.com 80
get http
HTTP/1.0 408 Request Time-out
Server: AkamaiGHost
Mime-Version: 1.0
Date: Sun, 14 Jul 2024 16:24:14 GMT
Content-Type: text/html
Content-Length: 314
Expires: Sun, 14 Jul 2024 16:24:14 GMT

<HTML><HEAD>
<TITLE>Request Timeout</TITLE>
</HEAD><BODY>
<H1>Request Timeout</H1>
The server timed out while waiting for the browser's request.<P>
Reference&#32;&#35;2&#46;d42fc917&#46;1720974254&#46;0
<P>https&#58;&#47;&#47;errors&#46;edgesuite&#46;net&#47;2&#46;d42fc917&#46;1720974254&#46;0</P>
</BODY></HTML>
```

Conclusion

Banner grabbing with Telnet and Netcat both involves connecting to a remote server to retrieve initial service information. Using telnet and netcat for banner grabbing is a straightforward and effective method to retrieve service banners from remote servers. Telnet, a simple command-line tool, allows users to establish a plain text connection to a specified port, making it useful for banner grabbing on well-known services like HTTP, FTP, or SMTP by manually connecting to their respective ports.

However, its lack of encryption poses a security risk. On the other hand, netcat (often referred to as the "Swiss Army knife" of networking) offers greater versatility and more advanced features. It can handle both TCP and UDP protocols, perform port scanning, and transfer files. Netcat's flexibility and ease of use make it particularly suitable for scripting and automation in penetration testing and network diagnostics. Despite these tools being somewhat outdated, they remain valuable for quick and uncomplicated banner grabbing tasks, especially in scenarios where modern alternatives are not available. However, their use should be complemented with more secure and sophisticated tools for comprehensive network security assessments.