

# 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:

1. **Active Banner Grabbing:** In this method, Hackers send packets to a remote server and analyze 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.
2. **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 analyze packets to identify the software and version being used. run on the server.

## Usage:

Hackers can perform a banner-grabbing attack against various protocols to discover insecure and vulnerable applications and exploits. There are many services, protocols, and types of banner information that you can collect using banner grabbing. You can develop various methods and tools for the discovery process. In general, banner grab allows an attacker to discover network servers and services running along with their instances on open ports, as well as the operating system. Given the type and version of an application, a hacker, or pen tester, can quickly scan for known and exploitable vulnerabilities in that version.

## Service Ports:

- Port 80 is running on [Hypertext Transfer Protocol \(HTTP\)](#) service.
- Port 21 is running on the [File Transfer Protocol \(FTP\)](#) service.
- Port 25 runs on the [Simple Mail Transfer Protocol \(SMTP\)](#) service.

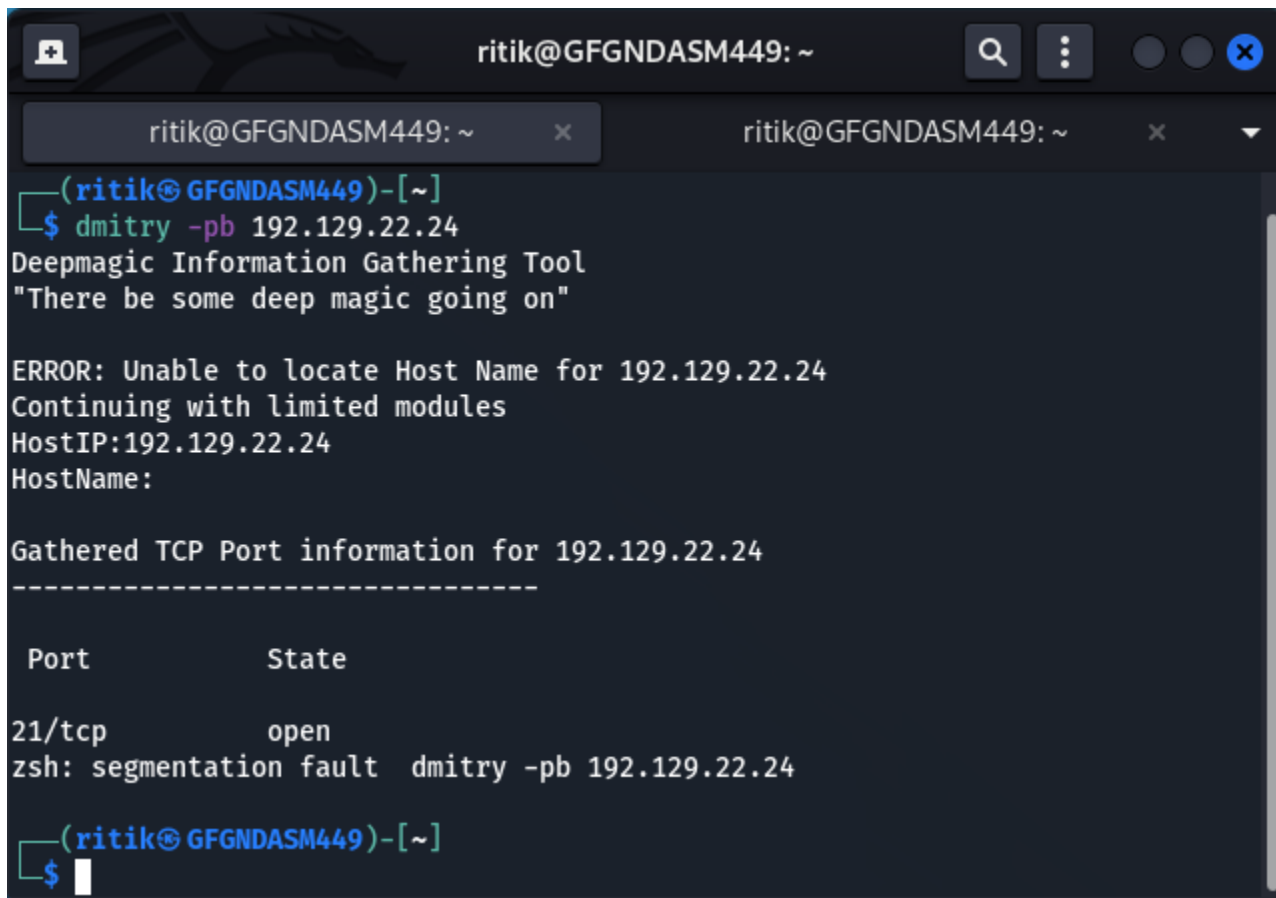
## Important Points:

- Banner Grabbing is used in Ethical Hacking to gather information about a target system before launching an attack.
- In order to gather this information, the Hacker must choose a website that displays banners from affiliate sites and navigate from the banner to the site served by the affiliate website.
- Banner Grabbing can be done through manual means or through the use of automated tools such as web crawlers, which search websites and download everything on them, including banners and files.

## Banner Grabbing Using Dmitry:

We can simply grab banners of any particular network using Dmitry tool of Kali Linux. here is an example. Type the following command to grab a banner of any host.

*dmitry -p -b [IPv4 Address of any host]*



```
ritik@GFGNDASM449: ~  
ritik@GFGNDASM449: ~ x ritik@GFGNDASM449: ~ x  
(ritik@GFGNDASM449)-[~]  
$ dmitry -pb 192.129.22.24  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
ERROR: Unable to locate Host Name for 192.129.22.24  
Continuing with limited modules  
HostIP:192.129.22.24  
HostName:  
  
Gathered TCP Port information for 192.129.22.24  
-----  
  
Port          State  
21/tcp        open  
zsh: segmentation fault  dmitry -pb 192.129.22.24  
  
(ritik@GFGNDASM449)-[~]  
$
```

**Countermeasures:**

- To avoid banner-grabbing attacks, companies can disable their banners on shady affiliate websites that are associated with known hacker forums where malicious tools are sold.
- Companies can also pay a fee to legitimate websites for their affiliate program to ensure that reputable and established sites will display the banners of the company in an attempt to target legitimate customers who would be interested in purchasing their product or service.
- Companies should always patch any software that they use, including antivirus programs and operating systems.

**Conclusion:**

Banner-grabbing is one of the first steps in an attack. It allows hackers to determine which exploit will be used and what action will be taken on the target system. While banner-grabbing is important, it is not something a hacker will do by themselves. It requires time, but when it's done correctly, you can gather valuable information that would otherwise cost you thousands of dollars to find out.