### Dmitry

dmitry –h

dmitry –winse example.com

### NMap

Nmap Target Selection

Scan a single IP

nmap 192.168.1.1

Scan a host

nmap http://scanme.nmap.org/

Scan a range of IPs

nmap 192.168.1.1-20

Scan a subnet

nmap 192.168.1.0/24

Nmap Port Selection

Scan a single Port

nmap -p 22 192.168.1.1

Scan a range of ports

nmap -p 1-100 192.168.1.1

Scan 100 most common ports (Fast)

nmap -F 192.168.1.1

Scan all 65535 ports

nmap -p- 192.168.1.1

Nmap Port Scan types

Scan using TCP connect

nmap -sT 192.168.1.1

Scan using TCP SYN scan (default)

nmap -sS 192.168.1.1

Scan UDP ports

nmap -sU -p 123,161,162 192.168.1.1

Service and OS Detection

Detect OS and Services

nmap -A 192.168.1.1

Standard service detection

nmap -sV 192.168.1.1

Nmap Output Formats

Save default output to file nmap -oN outputfile.txt 192.168.1.1

Save results as XML nmap -oX outputfile.xml 192.168.1.1

Save results in a format for grep nmap -oG outputfile.txt 192.168.1.1

Save in all formats nmap -oA outputfile 192.168.1.1

https://nmap.org/nsedoc/

Digging deeper with NSE Scripts

Scan using default safe scripts nmap -sV -sC 192.168.1.1

Get help for a script nmap --script-help=ssl-heartbleed

Scan using a specific NSE script nmap -sV -p 443 –script=ssl-heartbleed.nse 192.168.1.1

Scan with a set of scripts nmap -sV --script=smb\* 192.168.1.1

HTTP Service Information

Gather page titles from HTTP services nmap --script=http-title 192.168.1.0/24

Get HTTP headers of web services nmap --script=http-headers 192.168.1.0/24

Find web apps from known paths nmap --script=http-enum 192.168.1.0/24

Detect Heartbleed SSL Vulnerability

Heartbleed Testing

nmap -sV -p 443 --script=ssl-heartbleed 192.168.1.0/24

IP Address information

Find Information about IP address

nmap --script=asn-query,whois,ip-geolocation-maxmind 192.168.1.0/24

### Recon NG

sudo apt-get update

sudo apt-get install git

sudo apt-get install python-pip python-dev build-essential

git clone https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git

cd recon-ng

pip install -r REQUIREMENTS

./recon-ng

use recon/domains-hosts/hackertarget

show options

set SOURCE teslamotors.com

### Netcat

Netcat is a great network utility for reading and writing to network connections using the TCP and UPD protocol. Netcat is often referred to as the Swiss army knife in networking tools and we will be using it a lot throughout the different tutorials on Hacking Tutorials

Banner grabing

nc [ip address][port]

nc 192.168.253.131 21