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`

The default format could also be saved to a file using a simple file redirect `command > file` . Using the `-oN` option allows the results to be saved but also can be monitored in the terminal as the scan is under way.

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`

According to my Nmap install there are currently **581 NSE scripts**. The scripts are able to perform a wide range of security related testing and discovery functions. If you are serious about your network scanning you really should take the time to get familiar with some of them.

The option `--script-help=$scriptname` will display help for the individual scripts. To get an easy list of the installed scripts try `locate nse | grep script` .

You will notice I have used the `-sV` service detection parameter. Generally most NSE scripts will be more effective and you will get better coverage by including service detection.

A scan to search for DDOS reflection UDP services

Scan for UDP DDOS reflectors	`nmap –sU –A –PN –n –pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr 192.168.1.0/24`

UDP based DDOS reflection attacks are a common problem that network defenders come up against. This is a handy Nmap command that will scan a target list for systems with open UDP services that allow these attacks to take place. Full details of the command and the background can be found on the Sans Institute Blog where it was first posted.

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

There are many HTTP information gathering scripts, here are a few that are simple but helpful when examining larger networks. Helps in quickly identifying what the HTTP service that is running on the open port. Note the `http-enum` script is particularly noisy. It is similar to Nikto in that it will attempt to enumerate known paths of web applications and scripts. This will inevitably generated hundreds of `404 HTTP responses` in the web server error and access logs.

Detect Heartbleed SSL Vulnerability

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

Heartbleed detection is one of the available SSL scripts. It will detect the presence of the well known Heartbleed vulnerability in SSL services. Specify alternative ports to test SSL on mail and other protocols *(Requires Nmap 6.46)*.

IP Address information

Find Information about IP address	`nmap --script=asn-query,whois,ip-geolocation-maxmind 192.168.1.0/24`

Gather information related to the IP address and netblock owner of the IP address. Uses ASN, whois and geoip location lookups. See the IP Tools for more information and similar IP address and DNS lookups.

understand exactly what is allowed into your network. This is the reason we offer a hosted or online version of the Nmap port scanner. To enable remote scanning easily and effectively because anyone who has played with `shodan.io` knows very well how badly people test their perimeter networks.

Additional Resources

The above commands are just a taste of the power of Nmap. Check out our Nmap Tutorial that has more information and tips.
You could also view the full set of features by running Nmap with no options. The creator of Nmap, Fyodor, has a book available that covers the tool in depth.

PREVIOUS
← Maltego – Open Source Intelligence Gathering

NEXT
Samurai, BackTrack and Kali – LiveCD's for Pentesting →

July 25, 2013

rkhunter & chkrootkit: wise crackers only

April 10, 2008

Wireshark Tutorial and Cheat Sheet

May 19, 2018

Metasploit Express Review

June 2, 2010

ABOUT

From attack surface discovery to vulnerability identification, we host tools to make the job of securing your systems easier.

Membership Learn More

CONNECT

MAILING LIST

SIGN UP