Nmap

Nmap is awesome. There are many commands and options, but below are some commonly used ones which work well in both lab and penetration testing scenarios.

Nmap is a command-line tool but has a user-friendly GUI version called Zenmap, available for all major OS platforms. Zenmap also has preconfigured commands for common scans.

Host discovery (ping scan):

nmap -sn 192.168.1.1/24

Host discovery (specific range):

nmap -sn 192.168.1.1-100

Nmap also has the -Pn option which will disable the host discovery stage altogether on a scan. This option can be useful when the target is reported as down when it's actually up but not responding to host discovery probes (e.g. due to host-based firewall that drops ICMP packets). Using this option with the intense scans below can be helpful.

sudo nmap host >>>> SYN,SYN ACK,RST

TCP connect scan:

nmap -sT [host] >>>> SYN,SYN ACK,ACK,RST

OS fingerprinting and service detection:

nmap -sV -O [host]

Intense scan, all TCP ports:

nmap -p 1-65535 -T4 -A -v [host]

Intense scan, all TCP ports, no ping:

nmap -p 1-65535 -T4 -A -v -Pn [host]

Intense scan, plus UDP

nmap -sS -sU -T4 -A -v [host]

Warning: Big, nasty scans are great for labs, but sometimes get rate-limited. In real life settings, it's even worse. Start with light scans and do targeted scans when you discover something interesting.

Nmap scripting engine (NSE)

NSE is awesome too, its scripts can be used to detect a variety of vulnerabilities.

Running NSE scripts

General usage:

nmap --script=[scriptname] [host]

Example:

nmap --script=http-robots.txt [host]

Arguments can be passed to Nmap scripts using the --script-args option or from a file using the --script-args-file option.

Finding NSE scripts

Nmap scripts are located in the following directory:

/usr/share/nmap/scripts

FTP:

ls -l /usr/share/nmap/scripts/ftp\*

HTTP:

ls -l /usr/share/nmap/scripts/http\*

SMTP:

ls -l /usr/share/nmap/scripts/smtp\*

SMB:

ls -l /usr/share/nmap/scripts/smb\*

MySQL:

ls -l /usr/share/nmap/scripts/mysql\*

WordPress:

ls -l /usr/share/nmap/scripts/http-wordpress\*

Drupal:

ls -l /usr/share/nmap/scripts/http-drupal\*

Citrix:

ls -l /usr/share/nmap/scripts/citrix\*

Nmap script help

Most scripts have a help function that displays instructions when you type --script-help :

nmap --script-help ftp-anon

Updating Nmap scripts

If a script isn't available on your system, download it with the following command:

wget https://svn.nmap.org/nmap/scripts/smb-vuln-ms17-010.nse -O /usr/share/nmap/scripts/smb-vuln-ms17-010.nse

Once the script has downloaded, use the following command to update the Nmap script database so that the script will become available to Nmap:

nmap --script-updatedb

Detecting WAF

Web application firewalls (WAF) may drop malicious requests, such as those with SQL injections, or otherwise interfere with enumeration or testing:

Detect WAF using NMAP:

nmap -p80 --script http-waf-detect [host]

Fingerprint WAF using NMAP:

nmap -p80 --script http-waf-fingerprint [host]

Fingerprint WAF using WAFw00f:

wafw00f.py [url]