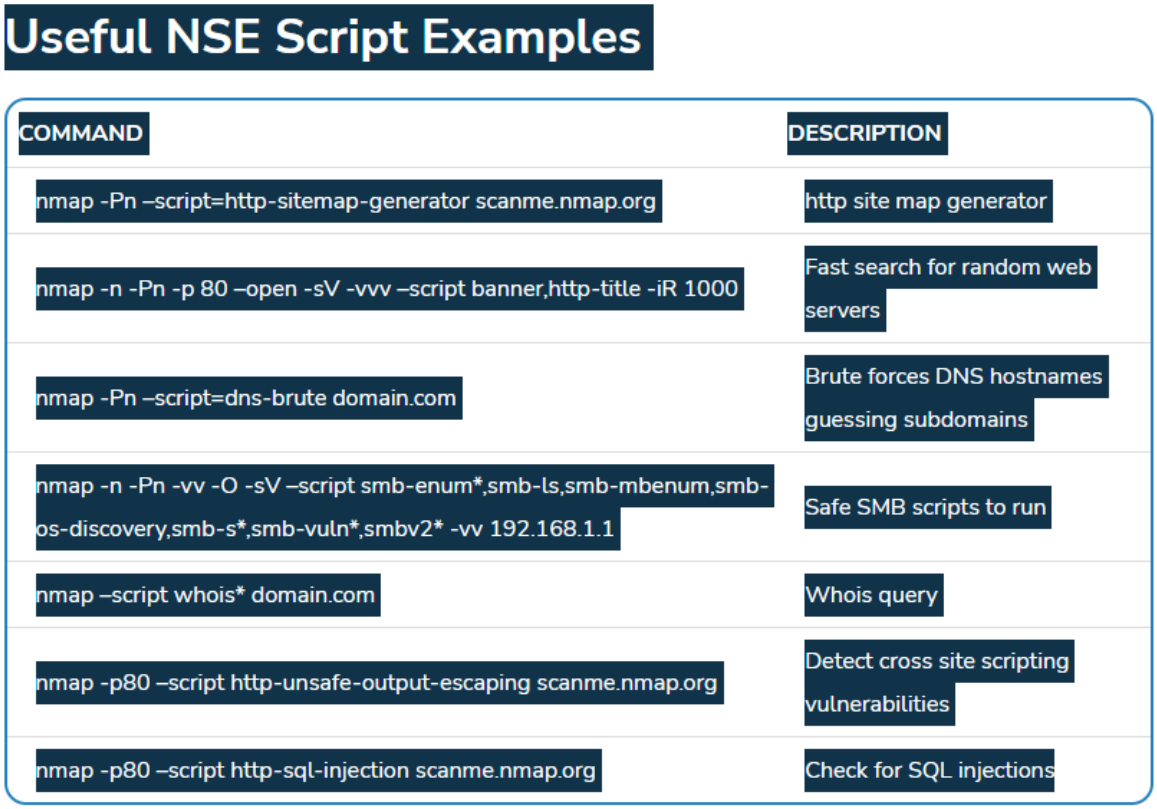
Nmap

Useful NSE Script Examples

```
nmap -Pn –script=http-sitemap-generator scanme.nmap.org
nmap -n -Pn -p 80 –open -sV -vvv –script banner,http-title -iR 1000
nmap -Pn –script=dns-brute domain.com
nmap –script whois* domain.com
nmap -p80 –script http-unsafe-output-escaping scanme.nmap.org
nmap -p80 –script http-sql-injection scanme.nmap.org
```



Useful NSE Script Examples

COMMAND	DESCRIPTION
nmap -Pn –script=http-sitemap-generator scanme.nmap.org	http site map generator
nmap -n -Pn -p 80 –open -sV -vvv –script banner,http-title -iR 1000	Fast search for random web servers
nmap -Pn –script=dns-brute domain.com	Brute forces DNS hostnames guessing subdomains
nmap -n -Pn -vv -O -sV –script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1	Safe SMB scripts to run
nmap –script whois* domain.com	Whois query
nmap -p80 –script http-unsafe-output-escaping scanme.nmap.org	Detect cross site scripting vulnerabilities
nmap -p80 –script http-sql-injection scanme.nmap.org	Check for SQL injections

OS Detection

```
nmap 192.168.1.1 -O
-O –osscan-limit
-O –osscan-guess
-O –max-os-tries 1
-A
```

OS Detection

SWITCH	EXAMPLE	DESCRIPTION
-O	nmap 192.168.1.1 -O	Remote OS detection using TCP/IP stack fingerprinting
-O –osscan-limit	nmap 192.168.1.1 -O –osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O –osscan-guess	nmap 192.168.1.1 -O –osscan-guess	Makes Nmap guess more aggressively
-O –max-os-tries	nmap 192.168.1.1 -O –max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

---

Nmap Scan Techniques

```
-sS     nmap 192.168.1.1 -sS    TCP SYN port scan (Default)
-sT     TCP connect port scan (Default without root privilege)
-sU     UDP port scan
-sA             TCP ACK port scan
-sW             TCP Window port scan
-sM             TCP Maimon port scan
```

Nmap Scan Techniques

SWITCH	EXAMPLE	DESCRIPTION
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Firewall / IDS Evasion and Spoofing

-f nmap 192.168.1.1 -f Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
–mtu nmap 192.168.1.1 –mtu 32 Set your own offset size
-D nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1 Send scans from spoofed IPs
-D nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip Above example explained
-S nmap -S www.microsoft.com www.facebook.com Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g nmap -g 53 192.168.1.1 Use given source port number
–proxies nmap –proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1 Relay connections through HTTP/SOCKS4 proxies
–data-length nmap –data-length 200 192.168.1.1 Appends random data to sent packets

Firewall / IDS Evasion and Spoofing

SWITCH	EXAMPLE	DESCRIPTION
-f	nmap 192.168.1.1 -f	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
–mtu	nmap 192.168.1.1 –mtu 32	Set your own offset size
-D	nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	Send scans from spoofed IPs
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Above example explained
-S	nmap -S www.microsoft.com www.facebook.com	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g	nmap -g 53 192.168.1.1	Use given source port number
–proxies	nmap –proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Relay connections through HTTP/SOCKS4 proxies
–data-length	nmap –data-length 200 192.168.1.1	Appends random data to sent packets

---

Output

Output

SWITCH	EXAMPLE	DESCRIPTION
-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file
-oA	nmap 192.168.1.1 -oA results	Output in the three major formats at once
-oG –	nmap 192.168.1.1 -oG –	Grepable output to screen. -oN -, -oX – also usable
–append-output	nmap 192.168.1.1 -oN file.file –append-output	Append a scan to a previous scan file
-v	nmap 192.168.1.1 -v	Increase the verbosity level (use -vv or more for greater effect)
-d	nmap 192.168.1.1 -d	Increase debugging level (use -dd or more for greater effect)
–reason	nmap 192.168.1.1 –reason	Display the reason a port is in a particular state, same output as -vv
–open	nmap 192.168.1.1 –open	Only show open (or possibly open) ports
–packet-trace	nmap 192.168.1.1 -T4 –packet-trace	Show all packets sent and received
–iflist	nmap –iflist	Shows the host interfaces and routes
–resume	nmap –resume results.file	Resume a scan