C|EH Certified Ethical Hacker

Ethical Hacking and Countermeasures
Unicornscan Cheat Sheet

EC-Council
Building A Culture Of Security

Unicornscan
Source: https://sourceforge.

Unicornsca n is an information-gathering tool used for scanning a single or multiple host for open ports and other information, it is an asynchronous TCP and UDP port scanner, it is also used for OS detection.
1.Unicornscan Options
2.Unicornscan Scanning Options
3.Unicornscan Commands

Syntax

```
unicornscan [options
`b:B:cd:De:EFG:hHi:Ij:l:L:m:M:o:p:P:q:Qr:R:s:St:T:u:Uw:W:vVz
Z:' ] X.X.X.X/YY:S-E
```

Unicornscan Options

Options	
`-b, --broken-crc`	Set broken crc sums on Transport layer, [Network layer, or both]
`-B, --source-port`	Set source port or whatever the scan module expects as a number
`-c, --proc-duplicates`	Process duplicate replies
`-d, --delay-type`	Set delay type
`-D, --no-defpayload`	No default Payload, only probe known protocols
`-e, --enable-module`	Enable modules listed as arguments
`-E, --proc-errors`	For processing `non-open' responses (ICMP errors, tcp rsts...)
`-F, --try-frags`	--
`-G, --payload-group`	Payload group (numeric) for tcp/udp type payload selection (default all)
`-h, --help`	Help
`-H, --do-dns`	Resolve hostnames during the reporting phase
`-i, --interface`	String representation of the interface to use
`-I, --immediate`	Immediate mode, display things as we find them
`-j, --ignore-seq`	A string representing the intended sequence ignorance level
`-l, --logfile`	Path to a file where flat text will be dumped that normally would go to the users terminal
`-L, --packet-timeout`	Numeric value representing the number of seconds to wait before declaring the scan over
`-m, --mode`	String representation of the desired scanning mode
`-M, --module-dir`	Path to a directory containing shared object 'modules' for unicornscan to search
`-o, --format`	Format of what to display for replies
`-p, --ports`	Global list of ports to scan
`-P, --pcap-filter`	Extra pcap filter string for receiver

Options	
`-q, --covertness`	Covertness value from 0 to 255
`-Q, --quiet`	This option is intended to make unicornscan play the 'quiet game'
`-r, --pps`	it is a numeric option containing the desired packets per second for the sender to use
`-R, --repeats`	Repeat packet scan N times
`-s, --source-addr`	The address to use to override the listeners default interfaces address
`-S, --no-shuffle`	Do not shuffle ports
`-t, --ip-ttl`	Set TTL on sent packets as in 62 or 6-16 or r64-128
`-T, --ip-tos`	Set TOS on sent packets
`-u, --debug`	Debug mask
`-U, --no-openclosed`	Don't say open or closed
`-w, --safefile`	Write pcap file of received packets
`-W, --fingerprint`	OS fingerprint 0=cisco(def) 1=openbsd 2=WindowsXP 3=p0fsendsyn 4=FreeBSD 5=nmap 6=linux 7:strangetcp
`-v, --verbose`	Verbose
`-V, --version`	Display version
`-z, --sniff`	Sniff alike
`-Z, --drone-str`	drone String

Unicornscan Scanning Options

Options	
`-mT`	SYN scan
`-mTsA`	ACK scan
`-mTsF`	Fin scan
`-mTs`	Null scan
`-mTsFPU`	Xmas scan
`-msf -Iv`	Connect Scan
`-mTFSRPAU`	Full Xmas scan
`(-mT) host:1-5`	Scan ports 1 through 5
`-mTFSRPAUEC`	scan with all options
`Syn + osdetect`	-eosdetect -Iv (-mT)

Unicornscan Commands

Command	Description
`unicornscan <host>`	Basic Unicornscan scan
`unicornscan -r200 -mT <target website>:80,443`	TCP Scanning
`unicornscan -r300 -mU <Target website>`	UDP Scanning
`unicornscan -msf -v -I <target ip>/24`	Perform a TCP SYN Scan on a whole network
`unicornscan <target ip>–Iv`	Scan a host for services & OS(TTL)
`unicornscan –mU –v –I <target ip>/24`	Perform a UDP scan on the whole network
`unicornscan <host ip>:5505 -r500 -w huntfor5505.pcap -W1  -s <target ip>`	Saving to a PCAP file
`unicornscan -mTsA -v -I [IP ADDRESS]`	ACK scan
`unicornscan <target website>/24:161,53,123 -mU -r 400`	Scan the 256 hosts inside the network that target resides
`unicornscan <target ip>.233:q`	TCP syn scan target (/32 is implied) for "Quick" Ports
`unicornscan -B53 -mTEC -R2 -W2 -t5 <target website>/16:22`	TCP syn Scan
`unicornscan -B22 -sr -mTsR -r 5000 -R 10000 <target ip>:31425`	Send to the <Target>destination port 31425 TCP packets
`unicornscan -i eth0 -Ir 160 -E <target>/32:20-600.`	A basic connect scan to find all open ports in a range using UnicornScan

Ethical Hacking and Countermeasures

Unicornscan Cheat Sheet

EC-Council
Building A Culture Of Security

Unicornscan
Source: https://sourceforge.

Unicornsca n is an information-gathering tool used for scanning a single or multiple host for open ports and other information, it is an asynchronous TCP and UDP port scanner, it is also used for OS detection.
1.Unicornscan Options
2.Unicornscan Scanning Options
3.Unicornscan Commands

Syntax

```
unicornscan [options
`b:B:cd:De:EFG:hHi:Ij:l:L:m:M:o:p:P:q:Qr:R:s:St:T:u:Uw:W:vVz
Z:' ] X.X.X.X/YY:S-E
```

Unicornscan Commands

Command	Description
`unicornscan -msf -s 5.4.3.2 -r 340 -Iv -epgsqldb <target website>/21:80,8080,443,81`	Runs unicornscan in connect mode
`unicornscan -Iv -r 160 -mT IP:a`	unicornscan full tcp portscan
`unicornscan <target1> <target2>`	Scan multiple hosts
`unicornscan -r200 -Iv -eosdetect  -mT <target`	scanning for mysql with http and https ports