[Top 5 Intrusive Nmap Scripts Hackers & Pentesters Should Know](https://null-byte.wonderhowto.com/how-to/advanced-nmap-top-5-intrusive-nmap-scripts-hackers-pentesters-should-know-0187287/)

* BY [**DISTORTION**](https://creator.wonderhowto.com/distortion/)
* 09/14/2018 6:42 AM

Nmap is more powerful than you know. With a few scripts, we can extend its functionality beyond a simple port scanner and start to identify details about target servers sysadmins don't want us to know.

Possibly the most popular and well-known reconnaissance tool currently available in the hacking world, Nmap has been [covered several times](https://null-byte.wonderhowto.com/collection/nmap/) on Null Byte before. For example, we've shown how to [detect CVEs](https://null-byte.wonderhowto.com/how-to/easily-detect-cves-with-nmap-scripts-0181925/), [automate brute-force attacks](https://null-byte.wonderhowto.com/how-to/automate-brute-force-attacks-for-nmap-scans-0184132/), and [perform advanced reconnaissance](https://null-byte.wonderhowto.com/how-to/hack-like-pro-advanced-nmap-for-reconnaissance-0151619/), to name just a few Nmap tutorials.

This article assumes readers have some experience with [the Nmap basics](https://www.amazon.com.au/Nmap-Simple-Guide-Network-Scanning/dp/1976410231/?tag=wnbau-22). I'll be targetting ports 80 and 443 (**-p80,443**) with most of the commands, as these are common web server ports. I'll also be engaging [Nmap's NSE functions](https://null-byte.wonderhowto.com/how-to/hack-like-pro-using-nmap-scripting-engine-nse-for-reconnaissance-0158681/) with the **--script** argument.

* **Don't Miss:**[**Using the Nmap Scripting Engine (NSE) for Reconnaissance**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-using-nmap-scripting-engine-nse-for-reconnaissance-0158681/)

Most-known for its ability to accurately fingerprint ports on web servers, Nmap's NSE functionalities make it an extremely powerful, multipurpose tool, scaling it far beyond an ordinary port scanner. In this multi-part Nmap series, I'll be showing off some of its more advanced capabilities for aggressively discovering web server error pages, web application firewall fingerprints, subdomains, and extracting metadata from photos.

*Disclaimer: The*[*intrusive Nmap scripts*](https://nmap.org/nsedoc/categories/intrusive.html)*exhaust significate resources (CPU and bandwidth) on the target web server and may cause it to crash, break, or unintentionally inflict denial of service attacks. Based on the scope of your penetration testing engagement, this may not be allowed by a given employer. Pentester's should use the below scripts with caution.*

Update Nmap on Your Kali System

Before we dive into Nmap scripts, let's first make sure we have the latest available version of Nmap installed on our Kali Linux system. At the time of this writing, Kali is offering v7.70.

Nmap can be installed using the below [**apt-get**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-5-installing-new-software-0147591/) commands.

apt-get update && apt-get install nmap

When that's done, we can verify it was installed with the **--version** argument.

nmap --version

Nmap version 7.70 ( https://nmap.org )

Platform: x86\_64-pc-linux-gnu

Compiled with: liblua-5.3.3 openssl-1.1.0h libssh2-1.8.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6

And as always, we can use the **--help** argument to view its available options. These options can be coupled with Nmap scripts to further enhance the commands featured in this article.

nmap --help

Nmap 7.70 ( https://nmap.org )

Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude\_file>: Exclude list from file

HOST DISCOVERY:

-sL: List Scan - simply list targets to scan

-sn: Ping Scan - disable port scan

-Pn: Treat all hosts as online -- skip host discovery

-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-PO[protocol list]: IP Protocol Ping

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

--system-dns: Use OS's DNS resolver

--traceroute: Trace hop path to each host

SCAN TECHNIQUES:

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans

-sU: UDP Scan

-sN/sF/sX: TCP Null, FIN, and Xmas scans

--scanflags <flags>: Customize TCP scan flags

-sI <zombie host[:probeport]>: Idle scan

-sY/sZ: SCTP INIT/COOKIE-ECHO scans

-sO: IP protocol scan

-b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:

-p <port ranges>: Only scan specified ports

Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9

--exclude-ports <port ranges>: Exclude the specified ports from scanning

-F: Fast mode - Scan fewer ports than the default scan

-r: Scan ports consecutively - don't randomize

--top-ports <number>: Scan <number> most common ports

--port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/version info

--version-intensity <level>: Set from 0 (light) to 9 (try all probes)

--version-light: Limit to most likely probes (intensity 2)

--version-all: Try every single probe (intensity 9)

--version-trace: Show detailed version scan activity (for debugging)

SCRIPT SCAN:

-sC: equivalent to --script=default

--script=<Lua scripts>: <Lua scripts> is a comma separated list of

directories, script-files or script-categories

--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts

--script-args-file=filename: provide NSE script args in a file

--script-trace: Show all data sent and received

--script-updatedb: Update the script database.

--script-help=<Lua scripts>: Show help about scripts.

<Lua scripts> is a comma-separated list of script-files or

script-categories.

OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:

Options which take <time> are in seconds, or append 'ms' (milliseconds),

's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

-T<0-5>: Set timing template (higher is faster)

--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes

--min-parallelism/max-parallelism <numprobes>: Probe parallelization

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies

probe round trip time.

--max-retries <tries>: Caps number of port scan probe retransmissions.

--host-timeout <time>: Give up on target after this long

--scan-delay/--max-scan-delay <time>: Adjust delay between probes

--min-rate <number>: Send packets no slower than <number> per second

--max-rate <number>: Send packets no faster than <number> per second

FIREWALL/IDS EVASION AND SPOOFING:

-f; --mtu <val>: fragment packets (optionally w/given MTU)

-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys

-S <IP\_Address>: Spoof source address

-e <iface>: Use specified interface

-g/--source-port <portnum>: Use given port number

--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies

--data <hex string>: Append a custom payload to sent packets

--data-string <string>: Append a custom ASCII string to sent packets

--data-length <num>: Append random data to sent packets

--ip-options <options>: Send packets with specified ip options

--ttl <val>: Set IP time-to-live field

--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address

--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

OUTPUT:

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,

and Grepable format, respectively, to the given filename.

-oA <basename>: Output in the three major formats at once

-v: Increase verbosity level (use -vv or more for greater effect)

-d: Increase debugging level (use -dd or more for greater effect)

--reason: Display the reason a port is in a particular state

--open: Only show open (or possibly open) ports

--packet-trace: Show all packets sent and received

--iflist: Print host interfaces and routes (for debugging)

--append-output: Append to rather than clobber specified output files

--resume <filename>: Resume an aborted scan

--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

--webxml: Reference stylesheet from Nmap.Org for more portable XML

--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:

-6: Enable IPv6 scanning

-A: Enable OS detection, version detection, script scanning, and traceroute

--datadir <dirname>: Specify custom Nmap data file location

--send-eth/--send-ip: Send using raw ethernet frames or IP packets

--privileged: Assume that the user is fully privileged

--unprivileged: Assume the user lacks raw socket privileges

-V: Print version number

-h: Print this help summary page.

EXAMPLES:

nmap -v -A scanme.nmap.org

nmap -v -sn 192.168.0.0/16 10.0.0.0/8

nmap -v -iR 10000 -Pn -p 80

SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

Related Book: "[Network Scanning Cookbook: Practical Network Security using Nmap and Nessus 7](https://www.amazon.com.au/Network-Scanning-Cookbook-Practical-Security-ebook/dp/B07G1B5TGV/?tag=wnbau-22)" by Sairam Jetty

1Web Application Firewall Detection

A [web application firewall](https://www.owasp.org/index.php/Web_Application_Firewall), shortened to WAF, detects and blocks malicious traffic transmitting to and from the web server its protecting. WAFs are most commonly used to help protect websites against SQL injection, file inclusion, and cross-site scripting (XSS) attacks.

A server well-protected by a WAF could mean all potential web-based vulnerabilities are thwarted. Adversely, a server unprotected by any kind of WAF could be disastrous for system's administrators trying to defend against hackers. Our ability to detect web application firewalls on target web servers is crucial as pentesters.

The [**http-waf-detect**](https://nmap.org/nsedoc/scripts/http-waf-detect.html) script is designed to help us learn the presence of a web application firewall. It will probe the target web server with several requests. First, it'll send a normal web request and record the response from the server. Then, it'll send another request with a payload (malformed URL) and compare the responses. This method of detecting WAFs is far from perfect and may vary based on the type of web server and WAF product.

To enable the **http-waf-detect** script, use the below **nmap** command.

nmap -p80,443 --script http-waf-detect --script-args="http-waf-detect.aggro,http-waf-detect.detectBodyChanges" targetWebsite.com

Here, I'm using the **http-waf-detect.aggro** argument, which instructs Nmap to try all of its built-in attack vectors to trigger the servers WAF. Also enabled is the **http-waf-detect.detectBodyChanges** argument, which looks for changes in the body of the HTTP requests and further increases the likeliness of detection.

Starting Nmap 7.70 ( https://nmap.org )

Nmap scan report for targetWebsite.com

Host is up (0.65s latency).

PORT STATE SERVICE

80/tcp open http

| http-waf-detect: IDS/IPS/WAF detected:

|\_targetWebsite.com:80/?p4yl04d=hostname%00

443/tcp open https

| http-waf-detect: IDS/IPS/WAF detected:

|\_targetWebsite.com:443/?p4yl04d=hostname%00

As we can see in the above output, Nmap has detected some kind of web application firewall present on the target web server. There are many commercial WAF products available to administrators. To learn which WAF is in production, we'll need to employ a different Nmap script.

2Web Application Firewall Fingerprint Detection

Learning which WAF is in use can be important as every WAF has its own predefined rate-limiting and detection methods. Identifying the type of WAF can aid pentester's in evading detection (or staying *under the radar*) if we can preemptively learn the WAFs limitations and detection triggers.

The [**http-waf-fingerprint**](https://nmap.org/nsedoc/scripts/http-waf-fingerprint.html) Nmap script is designed to help us learn the exact web application firewall in use on a target web server. It will also attempt to identify its type and exact version number.

In its simplest form, we don't need to include any **--script-args** to get this Nmap script working.

nmap -p80,443 --script http-waf-fingerprint targetWebsite.com

Starting Nmap 7.70 ( https://nmap.org )

Nmap scan report for targetWebsite.com

Host is up (0.71s latency).

PORT STATE SERVICE

80/tcp open http

| http-waf-fingerprint:

| Detected WAF

|\_ Cloudflare

443/tcp open https

As you can see above, this particular website is using the popular Cloudflare service as a front-end to protect their website from attackers.

We can further improve Nmap's ability to detect WAF types and versions using the **http-waf-fingerprint.intensive** argument. This will prolong the scan time and also increase the amount of *noise* (web traffic) generated by the script.

nmap -p80,443 --script http-waf-fingerprint --script-args http-waf-fingerprint.intensive=1 targetWebsite

Starting Nmap 7.70 ( https://nmap.org )

Nmap scan report for targetWebsite

Host is up (0.84s latency).

PORT STATE SERVICE

80/tcp open http

| http-waf-fingerprint:

| Detected WAF

|\_ BinarySec version 3.4.0

443/tcp open https

We've just learned the BinarySec WAF (version 3.4) is in use. An attack could study the WAF manual to better learn the triggers to avoid detection while penetration testing.

3Find HTTP Errors

Hypertext Transfer Protocol (HTTP) [status codes](https://en.wikipedia.org/wiki/Http_status_codes), also known as "response codes," are issued by web servers to our web browsers when we make requests. These codes are a way for web servers to communicate errors to server administrators, web developers, and end-users alike.

HTTP status codes are split into several categories or "classes." The first digit defines the categories and the following digits are sub-categories, specific to different types of error messages. For example, the 4xx categories is a class of errors specific to HTTP requests that cannot be fulfilled by the web server. Like trying to view a webpage that doesn't exist. That's defined as a status "404 Not Found," probably one of the most well-known status codes on the internet.

Status codes are especially useful to pentester's because it helps us identify broken, malformed, and misconfigured parts of a server which might be leaking sensitive information, or they can allow for some exploitable way of controlling aspects of the server.

[As per Wikipedia](https://en.wikipedia.org/wiki/Http_status_codes#4xx_Client_errors), below is a list of the five HTTP status code categories. Web application penetration testers should familiarize themselves with all of the status codes and their definitions.

* **1xx** (Informational): The request was received, continuing process
* **2xx** (Successful): The request was successfully received, understood, and accepted
* **3xx** (Redirection): Further action needs to be taken in order to complete the request
* **4xx** (Client Error): The request contains bad syntax or cannot be fulfilled
* **5xx** (Server Error): The server failed to fulfill an apparently valid request

The [**http-errors**](https://nmap.org/nsedoc/scripts/http-errors.html) Nmap script can be used to identify interesting status codes for further investigation.

nmap -p80,443 --script http-errors targetWebsite.com

Simply calling the **http-errors** script is enough to get started. Ports 80 and 443 are command web server ports but can be changed to meet your needs.

Nmap scan report for targetWebsite.com

Host is up (0.67s latency).

PORT STATE SERVICE

80/tcp open http

| http-errors:

| Spidering limited to: maxpagecount=40; withinhost=targetWebsite.com

| Found the following error pages:

|

| Error Code: 403

|\_ http://targetWebsite.com:80/

443/tcp open https

| http-errors:

| Spidering limited to: maxpagecount=40; withinhost=targetWebsite.com

| Found the following error pages:

|

| Error Code: 400

|\_ http://targetWebsite.com:443/

In the above output, Nmap detected a status 403, which suggests the servers file permissions are misconfigured and visitors don't have access to the requested resource. Below is a more refined command that includes several script arguments.

nmap -vv -p80,443 --script http-errors --script-args "httpspider.url=/docs/,httpspider.maxpagecount=3,httpspider.maxdepth=1" targetwebsite.com

This particular Nmap script utilizes the **[httpspider](https://nmap.org/nsedoc/lib/httpspider.html" \l "script-args" \t "_blank)** library, so we can use arguments like **httpspider.url**, **httpspider.maxpagecount**, and **httpspider.maxdepth** to refine our scan to specific URLs and define how many pages we want Nmap to crawl before stopping.

4Find Shared & New Servers

Subdomains are often used to host additional websites for a specific subset of users. For example, Null Byte (null-byte.wonderhowto.com) is one of many subdomains in the WonderHowTo network of websites. Popular subdomains include **m**.facebook.com, **mobile**.twitter.com, and **developer**.github.com.

These subdomains are useful to hackers because the subdomain and main domain may actually be hosted on completely different virtual private servers, in different parts of the world, and may not exercise the same degree of security.

The **[dns-brute](https://nmap.org/nsedoc/scripts/dns-brute.html" \t "_blank)** script built into Nmap is designed to enumerate subdomains and their corresponding server IP addresses.

nmap -p80,443 --script dns-brute targetWebsite.com

Starting Nmap 7.70 ( https://nmap.org )

Nmap scan report for targetWebsite.com

Host is up (0.16s latency).

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Host script results:

| dns-brute:

| DNS Brute-force hostnames:

| http.targetWebsite.com - 198.105.244.228

| http.targetWebsite.com - 198.105.254.228

| mysql.targetWebsite.com - 198.105.244.228

| mysql.targetWebsite.com - 198.105.254.228

| news.targetWebsite.com - 104.17.202.106

| news.targetWebsite.com - 104.17.203.106

| news.targetWebsite.com - 104.17.204.106

| news.targetWebsite.com - 104.17.205.106

| news.targetWebsite.com - 104.17.206.106

| app.targetWebsite.com - 104.97.95.87

| apps.targetWebsite.com - 12.18.141.21

| web.targetWebsite.com - 198.105.244.228

| web.targetWebsite.com - 198.105.254.228

| auth.targetWebsite.com - 204.238.150.111

| web2test.targetWebsite.com - 198.105.244.228

| web2test.targetWebsite.com - 198.105.254.228

| beta.targetWebsite.com - 98.99.252.42

| id.targetWebsite.com - 98.99.254.9

| blog.targetWebsite.com - 216.87.148.114

| www.targetWebsite.com - 104.97.95.87

| www2.targetWebsite.com - 207.76.137.99

| cms.targetWebsite.com - 98.99.252.57

| ldap.targetWebsite.com - 98.99.254.57

| owa.targetWebsite.com - 98.99.252.118

| sip.targetWebsite.com - 199.233.179.46

| mail.targetWebsite.com - 98.99.254.8

| mobile.targetWebsite.com - 216.87.148.114

| help.targetWebsite.com - 98.99.252.46

| home.targetWebsite.com - 198.105.244.228

|\_ home.targetWebsite.com - 198.105.254.228

Nmap done: 1 IP address (1 host up) scanned in 32.62 seconds

This particular website has many subdomains configured and not all share the same IP address. At this point, a penetration tester can further expand their reconnaissance to the newly discovered servers under this websites control.

Below is a **dns-brute** command that features several **--script-args**.

nmap -p80,443 --script dns-brute --script-args dns-brute.threads=25,dns-brute.hostlist=/root/Desktop/custom-subdomain-wordlist.txt targetWebsite.com

Starting Nmap 7.70 ( https://nmap.org )

Nmap scan report for targetWebsite.com

Host is up (0.17s latency).

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Host script results:

| dns-brute:

| DNS Brute-force hostnames:

| www7.targetWebsite.com - 198.105.244.228

| www7.targetWebsite.com - 198.105.254.228

| www.targetWebsite.com - 104.97.95.87

| webdisk.test.targetWebsite.com - 198.105.244.228

| webdisk.test.targetWebsite.com - 198.105.254.228

| www4.targetWebsite.com - 198.105.244.228

| www4.targetWebsite.com - 198.105.254.228

| www1.targetWebsite.com - 198.105.244.228

| www1.targetWebsite.com - 198.105.254.228

| app.targetWebsite.com - 104.97.95.87

| mail.targetWebsite.com - 98.99.254.8

| www.m.targetWebsite.com - 198.105.244.228

| www.m.targetWebsite.com - 198.105.254.228

| meet.targetWebsite.com - 199.233.179.60

| members.targetWebsite.com - 52.85.88.11

| members.targetWebsite.com - 52.85.88.178

| members.targetWebsite.com - 52.85.88.184

| members.targetWebsite.com - 52.85.88.186

| webmail2.targetWebsite.com - 198.105.244.228

| webmail2.targetWebsite.com - 198.105.254.228

| ww2.targetWebsite.com - 198.105.244.228

| ww2.targetWebsite.com - 198.105.254.228

| sip.targetWebsite.com - 199.233.179.46

| www.beta.targetWebsite.com - 198.105.244.228

| www.beta.targetWebsite.com - 198.105.254.228

| news.targetWebsite.com - 104.17.202.106

| news.targetWebsite.com - 104.17.203.106

| news.targetWebsite.com - 104.17.204.106

| news.targetWebsite.com - 104.17.205.106

| news.targetWebsite.com - 104.17.206.106

| www.news.targetWebsite.com - 198.105.244.228

| www.news.targetWebsite.com - 198.105.254.228

| www.shop.targetWebsite.com - 198.105.244.228

| www.shop.targetWebsite.com - 198.105.254.228

| portal.targetWebsite.com - 192.237.142.31

| preview.targetWebsite.com - 104.97.95.87

| search.targetWebsite.com - 98.99.252.118

| www.support.targetWebsite.com - 198.105.244.228

| www.support.targetWebsite.com - 198.105.254.228

| api.targetWebsite.com - 98.99.252.56

| share.targetWebsite.com - 69.28.231.168

| mobile.targetWebsite.com - 216.87.148.114

| lyncdiscover.targetWebsite.com - 199.233.179.60

| mysql.targetWebsite.com - 198.105.244.228

| mysql.targetWebsite.com - 198.105.254.228

| owa.targetWebsite.com - 98.99.252.118

| webdisk.forum.targetWebsite.com - 198.105.244.228

| webdisk.forum.targetWebsite.com - 198.105.254.228

| www.blog.targetWebsite.com - 198.105.244.228

| www.blog.targetWebsite.com - 198.105.254.228

| beta.targetWebsite.com - 98.99.252.42

| partner.targetWebsite.com - 98.99.252.118

| a.targetWebsite.com - 63.149.195.18

| a.targetWebsite.com - 67.134.222.254

| a.targetWebsite.com - 8.33.184.254

| blogs.targetWebsite.com - 98.99.252.176

| webdisk.m.targetWebsite.com - 198.105.244.228

| webdisk.m.targetWebsite.com - 198.105.254.228

| webdisk.demo.targetWebsite.com - 198.105.244.228

| webdisk.demo.targetWebsite.com - 198.105.254.228

| ldap.targetWebsite.com - 98.99.254.57

| www.webmail.targetWebsite.com - 198.105.244.228

| www.webmail.targetWebsite.com - 198.105.254.228

| webmail.targetWebsite.com - 98.99.254.8

| web3.targetWebsite.com - 198.105.244.228

| web3.targetWebsite.com - 198.105.254.228

| community.targetWebsite.com - 216.87.148.114

| webmail.cp.targetWebsite.com - 198.105.244.228

| webmail.cp.targetWebsite.com - 198.105.254.228

| www.demo.targetWebsite.com - 198.105.244.228

| www.demo.targetWebsite.com - 198.105.254.228

| remote.targetWebsite.com - 216.87.148.114

| my.targetWebsite.com - 198.105.244.228

| my.targetWebsite.com - 198.105.254.228

| webdisk.dev.targetWebsite.com - 198.105.244.228

| webdisk.dev.targetWebsite.com - 198.105.254.228

| www.forum.targetWebsite.com - 198.105.244.228

| www.forum.targetWebsite.com - 198.105.254.228

| webdisk.targetWebsite.com - 198.105.244.228

| webdisk.targetWebsite.com - 198.105.254.228

| www.test.targetWebsite.com - 198.105.244.228

| www.test.targetWebsite.com - 198.105.254.228

| www.mobile.targetWebsite.com - 198.105.244.228

| www.mobile.targetWebsite.com - 198.105.254.228

| web1.targetWebsite.com - 198.105.244.228

| web1.targetWebsite.com - 198.105.254.228

| relay.targetWebsite.com - 98.99.254.28

| web2.targetWebsite.com - 198.105.244.228

| web2.targetWebsite.com - 198.105.254.228

| web.targetWebsite.com - 198.105.244.228

| web.targetWebsite.com - 198.105.254.228

| dialin.targetWebsite.com - 199.233.179.60

| jobs.targetWebsite.com - 216.87.148.114

| webdisk.blog.targetWebsite.com - 198.105.244.228

| webdisk.blog.targetWebsite.com - 198.105.254.228

| home.targetWebsite.com - 198.105.244.228

| home.targetWebsite.com - 198.105.254.228

| www3.targetWebsite.com - 198.105.244.228

| www3.targetWebsite.com - 198.105.254.228

| www.store.targetWebsite.com - 104.16.53.60

| www.store.targetWebsite.com - 104.16.54.60

| www6.targetWebsite.com - 198.105.244.228

| www6.targetWebsite.com - 198.105.254.228

| www.my.targetWebsite.com - 198.105.244.228

| www.my.targetWebsite.com - 198.105.254.228

| www5.targetWebsite.com - 198.105.244.228

| www5.targetWebsite.com - 198.105.254.228

| autodiscover.targetWebsite.com - 98.99.254.176

| www.admin.targetWebsite.com - 198.105.244.228

| www.admin.targetWebsite.com - 198.105.254.228

| store.targetWebsite.com - 104.16.206.251

| store.targetWebsite.com - 104.16.207.251

| web01.targetWebsite.com - 198.105.244.228

| web01.targetWebsite.com - 198.105.254.228

| cms.targetWebsite.com - 98.99.252.57

| www.old.targetWebsite.com - 198.105.244.228

| www.old.targetWebsite.com - 198.105.254.228

| blog.targetWebsite.com - 216.87.148.114

| www2.targetWebsite.com - 207.76.137.99

| webservices.targetWebsite.com - 198.105.244.228

| webservices.targetWebsite.com - 198.105.254.228

| www.video.targetWebsite.com - 198.105.244.228

| www.video.targetWebsite.com - 198.105.254.228

| web4.targetWebsite.com - 198.105.244.228

| web4.targetWebsite.com - 198.105.254.228

| e.targetWebsite.com - 63.149.195.18

| e.targetWebsite.com - 67.134.222.254

| e.targetWebsite.com - 8.33.184.254

| auth.targetWebsite.com - 204.238.150.111

| wwww.targetWebsite.com - 198.105.244.228

| wwww.targetWebsite.com - 198.105.254.228

| help.targetWebsite.com - 98.99.252.46

| jira.targetWebsite.com - 98.99.254.68

| outlook.targetWebsite.com - 98.99.254.66

| www.mail.targetWebsite.com - 198.105.244.228

| www.mail.targetWebsite.com - 198.105.254.228

| MAIL.targetWebsite.com - 98.99.254.8

| www.new.targetWebsite.com - 198.105.244.228

| www.new.targetWebsite.com - 198.105.254.228

| mdm.targetWebsite.com - 192.30.68.141

| origin-www.targetWebsite.com - 104.97.95.87

| sslvpn.targetWebsite.com - 204.238.150.49

| assets.targetWebsite.com - 107.14.46.27

| assets.targetWebsite.com - 107.14.46.35

| www.en.targetWebsite.com - 198.105.244.228

| www.en.targetWebsite.com - 198.105.254.228

| docs.targetWebsite.com - 98.99.254.67

| www.dev.targetWebsite.com - 198.105.244.228

| www.dev.targetWebsite.com - 198.105.254.228

| www.forums.targetWebsite.com - 198.105.244.228

| www.forums.targetWebsite.com - 198.105.254.228

| www.ads.targetWebsite.com - 198.105.244.228

| www.ads.targetWebsite.com - 198.105.254.228

| apps.targetWebsite.com - 12.18.141.21

| www.wiki.targetWebsite.com - 198.105.244.228

| www.wiki.targetWebsite.com - 198.105.254.228

| webconf.targetWebsite.com - 198.105.244.228

| webconf.targetWebsite.com - 198.105.254.228

| ww.targetWebsite.com - 198.105.244.228

| ww.targetWebsite.com - 198.105.254.228

| webcam.targetWebsite.com - 198.105.244.228

| webcam.targetWebsite.com - 198.105.254.228

| www.chat.targetWebsite.com - 198.105.244.228

|\_ www.chat.targetWebsite.com - 198.105.254.228

Nmap done: 1 IP address (1 host up) scanned in 62.15 seconds

By default, dns-brute will scan using five concurrent threads. We can increase or decrease this value with the **dns-brute.threads**. Depending on the type of web server, many threads will crash a server or act as a denial of service, making the website slow or unresponsive for other users. Adjust this value with caution.

Dns-brute will attempt about 125 popular subdomains. We can use [custom subdomain lists](https://github.com/felmoltor/DNSBruteForcer/tree/master/dictionaries) with the **dns-brute.hostlist** argument. As we can see in the above output, using a [comprehensive wordlist](https://null-byte.wonderhowto.com/how-to/use-leaked-password-databases-create-brute-force-wordlists-0184006/), we were able to detect more subdomains and IP addresses controlled by this website.

Related Book: "Nmap 6: Network Exploration and Security Auditing Cookbook" by Paulino Calderon (Available from [Amazon](https://www.amazon.com.au/Nmap-exploration-security-auditing-Cookbook/dp/1849517487/?tag=wnbau-22) | [Walmart](https://linksynergy.walmart.com/deeplink?id=Cty0dj6o3sg&mid=2149&u1=WHT-nb&murl=https%3A%2F%2Fwww.walmart.com%2Fip%2FNmap-6-Network-Exploration-and-Security-Auditing-Cookbook%2F53696904))

5Extract EXIF Data from Photos

Exchangeable image file, known more as EXIF, is information stored in JPEG, PNG, PDF, and many more file types. This embedded data can sometimes reveal interesting information, including timestamps, device information, and GPS coordinates. Most websites still do not properly sanitize EXIF data from images, leaving themselves or their users at risk.

As penetration testers, knowing what kind of device a target is using will aid us in determining what kind(s) of payloads to generate. A classic example of [EXIF data being used to catch a black hat](http://gizmodo.com/5901430/these-breasts-nailed-anonymous-hacker-in-fbi-case) is the arrest of Higinio Ochoa. FBI agents extrapolated his girlfriend's geographic location using the GPS data found in a photo Higinio uploaded to the internet.

Nmap's [**http-exif-spider**](https://nmap.org/nsedoc/scripts/http-exif-spider.html) script can be used to extract interesting EXIF data from photos found on websites. Such a script isn't useful against mainstream sites like Instagram, Twitter, and Facebook. Major websites scrub EXIF data when users upload new photos. However, personal blogs, small businesses, and corporate organizations may not practice strong security precautions or monitor what employees are posting online. It's not uncommon to find GPS data in photos.

nmap -p80,443 --script http-exif-spider targetWebsite.com

Starting Nmap 7.70 ( https://nmap.org )

Nmap scan report for targetWebsite.com

Host is up (0.12s latency).

PORT STATE SERVICE

80/tcp open http

| http-exif-spider:

| http://targetWebsite.com:80/image\_10012.jpg

| Make: NIKON CORPORATION

| Model: NIKON D4

| Date: 2017:04:26 21:22:49

| http://targetWebsite.com:80/ips.jpg

| Make: Samsung

| Model: Galaxy S6

|\_ Date: 2017:02:24 23:37:14

443/tcp open https

| http-exif-spider:

| https://targetWebsite.com:443/clifton.jpg

| Make: Canon

|\_ Model: Canon EOS 5D Mark III

Nmap done: 1 IP address (1 host up) scanned in 30.43 seconds

We can see the above target is using an Android phone and a variety of digital cameras. We can now (with some degree of certainty) generate an Android-specific payload and send it to the target to further compromise their devices, accounts, and networks.

When attempting to extract EXIF data from large photos, Nmap may produce an error message that states "Current http cache size exceeds max size." This is Nmap telling us that the photo is too large and is exceeding the default maximum file size value. Use the **http.max-cache-size** argument and increase the value as needed. Below I've set it to an arbitrarily high number.

nmap -p80,443 --script http-exif-spider --script-args="http.max-cache-size=99999999" targetWebsite.com

More Nmap Scripts to Come ...

Whether we're enumerating subdomains, detecting WAF version info, or reporting broken webpages for a small bug bounty, Nmap scripts have us covered. And we've barely scratched the surface with what Nmap scripts are capable of. In my next article, I'll be talking about scripts that don't trigger web application firewalls or alert system administrators to our attempts at reconnaissance.