

COURSE: Top 5 Tools & Tricks for Ethical Hacking & Bug Bounties 2021

Unveiling the Ultimate Toolkit: Mastering Ethical Hacking & Bug Bounties with Top 5 Tools & Tricks 2021



Introduction:

In the dynamic landscape of cybersecurity, staying one step ahead of potential threats is paramount. Ethical hackers, penetration testers, and bug bounty hunters are the guardians of this digital realm, armed with knowledge, skills, and cutting-edge tools. Welcome to the transformative Udemy course "Top 5 Tools & Tricks for Ethical Hacking & Bug Bounties 2021." In this article, we'll provide you with a glimpse into the exciting world of this course, which unveils the quintessential tools and techniques that can empower you to become a skilled cybersecurity professional.

Navigating the Path of Mastery:

MassDNS

MassDNS is a high-performance DNS stub resolver that is designed for bulk DNS queries, allowing users to efficiently perform large-scale DNS reconnaissance and data collection tasks. It's commonly used in cybersecurity and network analysis to gather information about numerous domain names quickly.



Installation Process:-

Step 1 :- git clone <https://github.com/blechschmidt/massdns.git>

```
(root@kali)-[/home/kali]
# git clone https://github.com/blechschmidt/massdns.git
Cloning into 'massdns'...
remote: Enumerating objects: 1170, done.
remote: Counting objects: 100% (465/465), done.
remote: Compressing objects: 100% (206/206), done.
remote: Total 1170 (delta 281), reused 278 (delta 258), pack-reused 705
Receiving objects: 100% (1170/1170), 907.23 KiB | 6.77 MiB/s, done.
Resolving deltas: 100% (753/753), done.
```

Figure:-

The above figure shows that the command is used to clone the "massdns" repository from GitHub.

Step 2:- cd massdns

```
(root@kali)-[/home/kali]
# cd massdns
```

Figure:-

The above figure shows that the command "cd massdns" changes the current directory to the "massdns" directory.

Step 3:- make

```
(root@kali)-[/home/kali/massdns]
# make
mkdir -p bin
cc -DMASSDNS_REVISION="\v1.0.0-89-g20594ba\" -O3 -std=c11 -DHAVE_EPOLL -DHAVE_SYSINFO -Wall -fstack-protector-strong src/main.c -o bin/massdns
```

Figure:-

The above figure shows that the command make is used to compile source code and create an executable

Step 4:- make install

```
(root@kali)-[/home/kali/massdns] "the quieter you become, t
# make install
mkdir -p /usr/local/bin
mkdir -p /usr/local/man/man1
install -m 0755 bin/massdns /usr/local/bin
install -m 0644 doc/massdns.1 /usr/local/man/man1
```

Figure:-

The above figure shows that the make install command is used to compile and install software from the source code.

Step 5:- to Check massdns -h

```
(root@kali)-[/home/kali/massdns]
# massdns -h
Usage: massdns [options] [domainlist]
-b --bindto          Bind to IP address and port. (Default: 0.0.0.0:0)
--busy-poll          Use busy-wait polling instead of epoll.
-c --resolve-count   Number of resolves for a name before giving up. (Default: 50)
--drop-group         Group to drop privileges to when running as root. (Default: nogroup)
--drop-user          User to drop privileges to when running as root. (Default: nobody)
--extended-input     Input names are followed by a space-separated list of resolvers.
                    These are used before falling back to the resolvers file.
--filter            Only output packets with the specified response code.
--flush             Flush the output file whenever a response was received.
-h --help           Show this help.
--ignore            Do not output packets with the specified response code.
-i --interval       Interval in milliseconds to wait between multiple resolves of the same
                    domain. (Default: 500)
-l --error-log       Error log file path. (Default: /dev/stderr)
--norecurse         Use non-recursive queries. Useful for DNS cache snooping.
-o --output          Flags for output formatting.
--predictable       Use resolvers incrementally. Useful for resolver tests.
--processes         Number of processes to be used for resolving. (Default: 1)
-q --quiet          Quiet mode.
--rand-src-ipv6     Use a random IPv6 address from the specified subnet for each query.
--rcvbuf            Size of the receive buffer in bytes.
--retry            Unacceptable DNS response codes.
                    (Default: All codes but NOERROR or NXDOMAIN)
-r --resolvers       Text file containing DNS resolvers.
```

Figure:-

The above figure shows that the -h flag is used to display the help menu or usage.

Output will be seen like this

```
root@musab: ~/Downloads/tools/massdns/bin  x  root@musab: ~/Desktop/massdns  x  root@musab: ~/Downloads/tools/massdns  x
root@musab:~/Downloads/tools/massdns/bin# assetfinder att.com --subs-only | ./massdns -r ../lists/resolvers.txt -o S -w resolved.txt

Processed queries: 19560
Received packets: 15627
Progress: 100.00% (00 h 01 min 59 sec / 00 h 01 min 59 sec)
Current incoming rate: 12 pps, average: 131 pps
Current success rate: 4 pps, average: 81 pps
Finished total: 19560, success: 9686 (49.52%)
Mismatched domains: 2418 (15.54%), IDs: 0 (0.00%)
Failures: 0: 0.00%, 1: 1.66%, 2: 1.45%, 3: 0.86%, 4: 0.85%, 5: 1.44%, 6: 1.51%, 7: 0.95%, 8: 1.98%, 9: 2.95%, 10: 1.54%, 11: 2.96%, 12: 4.12%, 13: 5.19%, 14: 7.29%, 15:
5.63%, 16: 3.53%, 17: 2.10%, 18: 1.25%, 19: 0.65%, 20: 0.38%, 21: 0.19%, 22: 0.16%, 23: 0.09%, 24: 0.10%, 25: 0.04%, 26: 0.00%, 27: 0.01%, 28: 0.01%, 29: 0.01%, 30: 0.01
%, 31: 0.01%, 32: 0.02%, 33: 0.00%, 34: 0.01%, 35: 0.01%, 36: 0.02%, 37: 0.01%, 38: 0.01%, 39: 0.02%, 40: 0.03%, 41: 0.02%, 42: 0.05%, 43: 0.06%, 44: 0.04%, 45: 0.04%, 4
6: 0.06%, 47: 0.06%, 48: 0.08%, 49: 0.12%, 50: 50.48%,
Response: Success: Total:
OK: 9412 ( 97.17%) 11228 ( 72.16%)
NXDOMAIN: 58 ( 0.60%) 67 ( 0.43%)
SERVFAIL: 216 ( 2.23%) 270 ( 1.74%)
REFUSED: 0 ( 0.00%) 3994 ( 25.67%)
FORMERR: 0 ( 0.00%) 0 ( 0.00%)
root@musab:~/Downloads/tools/massdns/bin# ls
massdns resolved.txt
```

Figure :-

The Above figure shows the command retrieves subdomains of att.com using assetfinder, then resolves them using massdns with specified resolvers and give output in resolved.txt

```
h-135-207-181-149.research.att.com. A 135.207.181.149
h-135-197-255-75.research.att.com. A 135.197.255.75
fastpass.att.com. A 144.160.230.60
h-135-207-180-88.research.att.com. A 135.207.180.88
eds-aldc-dw10.wireless.att.com. A 144.160.237.240
h-135-207-220-29.research.att.com. A 135.207.220.29
atlabipssms.wireless.labs.att.com. A 70.151.40.193
kcretail.dp.att.com. A 144.161.163.235
h-135-207-53-249.research.att.com. A 135.207.53.249
tchosted.business.att.com. CNAME tchosted.business.att.com.edgekey.net.
h-135-207-231-87.research.att.com. A 135.207.231.87
h-135-207-33-187.research.att.com. A 135.207.33.187
perfpreps.ipnetwork.att.com. A 130.8.204.64
bthscmintegration.att.com. A 135.209.156.248
h-135-207-98-107.research.att.com. A 135.207.98.107
h-135-207-182-189.research.att.com. A 135.207.182.189
h-135-207-181-107.research.att.com. A 135.207.181.107
h-135-197-209-59.research.att.com. A 135.197.209.59
dal04.c2bc.um.att.com. A 199.108.23.32
h-135-207-229-187.research.att.com. A 135.207.229.187
h-135-207-53-59.research.att.com. A 135.207.53.59
h-135-207-58-38.research.att.com. A 135.207.58.38
smi03.dp.att.com. A 144.161.109.30
slmdm03.dp.att.com. A 144.160.40.49
h-135-207-230-178.research.att.com. A 135.207.230.178
h-135-207-183-218.research.att.com. A 135.207.183.218
csi-ext-lmsgw-ist01.test.att.com. CNAME csi-lmsgw-ist01.att-idns.net.
origin-itwww.wireless.att.com. A 170.35.236.77
tamp2.vpn.att.com. A 144.160.96.147
h-135-207-183-96.research.att.com. A 135.207.183.96
h-135-207-19-68.research.att.com. A 135.207.19.68
h-135-207-54-138.research.att.com. A 135.207.54.138
h-135-207-216-97.research.att.com. A 135.207.216.97
h-135-207-30-26.research.att.com. A 135.207.30.26
h-135-207-55-59.research.att.com. A 135.207.55.59
root@musab:~/Downloads/tools/massdns/bin#
```

Figure:-

The above figure shows the output of resolved.txt.