

Forum:[Hack Forums](#)

Thread: [Introduction to Web Hacking : Mapping Attack Surface](#)

Asdethprime - May 28, 2017, 2:23 am

Introduction to Web Hacking: Mapping The Attack Surface

When hacking a web server, one of the most important thing you need to do is map the appropriate surface.

Essentially what happens is that the web-server you are targeting is often a part of a much wider network. What you need to do is get a detail list of web-servers connected to a particular application that you can attack. Any one of the web server identified can be used to penetrate the network (and eventually rape it depending on how skilled you are and how vulnerable the system is).

Target and Operating System on the attacking machine

An awesome part in cyber security is that in most countries it's completely legal to map a network including identifying attack surface. Running a vulnerability scanner or attempting to fuzz applications running on the servers however is NOT legal.

However, since the part we are investigating is legal lets take a live web server.

For our example the web server we will be creating a skeleton to attack is : 123movesfree.com

As you can possibly guess by the name it's a website that streams free movies, and is distributed under Cloud Flare (that is bad for hackers because Cloud Flare has a rather effective web application firewall which makes hacking it more difficult).

Alright, enough of intro let's get into mapping the target.

Basic Security Before Proceeding

The first thing we want to do is set up proxychains and tor to prevent our anonymity. I am using Ubuntu though this should work for most linux terminals:

The command I would type is

```
$ sudo apt-get install tor  
$ sudo apt-get install proxychains
```

Once both of them are installed lets get to the actual work of mapping the target.

Mapping the Target

So the first thing I am going to use is ping to find the IP address of the target

```
$ ping 123moviesfree.com
```

I get the IP address to be : 213.247.47.190

Which is good, so the next thing we do is try running fierce.

Fierce is a DNS enumeration tool, free, open source (please feel free to google up on this because it's very useful) which is very useful for network enumeration. If anyone uses Kali Linux it should come pre-installed, if it doesn't finding and installing it should be a trival matter.

So the command I will run is :

```
$ proxychains perl fierce.pl -dns 123freemovies.com
```

Fierce does it's little things like bruteforcing the DNS and trying DNS zone transfer - which is a cool way to enumerate provided its working. As expected DNS zone transfer does not work.

The program however outputs a group of subnets worth probing futher:

Subnets found (may want to probe here using nmap or unicornscan):

```
173.239.2.0-255 : 1 hostnames found.  
173.239.5.0-255 : 1 hostnames found.  
174.137.132.0-255 : 1 hostnames found.  
213.247.47.0-255 : 1 hostnames found.  
54.225.100.0-255 : 1 hostnames found.  
64.95.64.0-255 : 1 hostnames found.
```

So that's not a bad start.

Now we are going to ping individual subnets to figure out what IP address are live on the network and which of them belong to 123freemovies.com (through a reverse DNS lookup)

This is a lengthy process which tool me a whole day.

Just for tips this is how you would go about pinging host to find if any one of them are alive.

```
$ sudo proxychains nmap -T5 -sP 173.239.2.0-255
```

This scan returned 134 live host when most of them were not a part of 123freemovies.com

Iterating the process we get the following results:

The mapped attack surface

So this is the result we get:

```
184.95.38.195:123moviesfree.ae
```

```
104.31.87.5:123moviesfree.be
```

```
69.64.147.242:123moviesfree.biz
```

```
52.0.217.44:123moviesfree.bz
```

52.0.217.44:123moviesfree.cc
179.43.173.118:123moviesfree.ch
69.64.147.242:123moviesfree.co
104.27.141.252:123moviesfree.com
103.224.182.250:123moviesfree.cz
103.224.182.239:123moviesfree.de
104.18.37.66:123moviesfree.es
103.224.182.211:123moviesfree.eu
184.168.221.13:123moviesfree.in
104.28.2.151:123moviesfree.info
185.53.178.6:123moviesfree.io
185.53.178.8:123moviesfree.is
141.8.224.169:123moviesfree.it
173.208.215.108:123moviesfree.ml
72.52.4.121:123moviesfree.net
69.64.147.242:123moviesfree.org
45.79.222.138:123moviesfree.ph
164.138.223.139:123moviesfree.pro
128.199.141.59:123moviesfree.pw
185.53.179.8:123moviesfree.re
184.95.38.195:123moviesfree.se
91.144.20.76:123moviesfree.sy
195.20.41.218:123moviesfree.tk
178.175.129.10:123moviesfree.to
192.64.119.2:123moviesfree.today
69.64.147.242:123moviesfree.tv

198.54.126.90:123moviesfree.us

103.224.182.252:123moviesfree.vc

88.198.29.97:123moviesfree.vg

69.64.147.242:123moviesfree.ws

38 publicly reach-able servers for us to probe. Not bad for starters right.

c0rephakt - May 28, 2017, 2:43 am

Thanks for this. Appreciate the time and effort.

Asdethprime - May 28, 2017, 2:43 am

Our next job is to probe even further on each node to enumerate the content.

A quick nmap scan with -A (sudo proxychains nmap -T5 -A <target IP>) will produce a list like the following:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	NcFTPd
22/tcp	open	ssh	SCS sshd 3.2.9.1 (protocol 2.0)
80/tcp	open	http	Apache httpd
110/tcp	open	pop3	qmail pop3d
143/tcp	open	imap	Courier Imapd (released 2008)
993/tcp	open	ssl/imap	Courier Imapd (released 2008)
1110/tcp	open	pop3	qmail pop3d
3306/tcp	open	mysql	MySQL 5.0.51

That makes for a good way to start.

As a rule of thumb: any FTP, SSH or Telnet port you get, your best bet in is a good old fasion bruteforce.

With even the version number of services running on the node as well as name of the services running can be very useful because we can then probe then with set of more specialized tools: I would probe an open port 80 with nikto.

So there you have it, this is how you would normally map an attack surface before hacking a target.

(May 28, 2017 02:43 AM)c0rephakt Wrote: [\[CITE\]](#) Thanks for this. Appreciate the time and effort. You are most welcome =)

Baud - June 14, 2017, 10:29 am

Very good and useful tutorial, thank you a lot! I like how you actually used proxychains to have a layer of security during the enumeration process unlike almost everyone else writing this sort of tutorials without saying a word about how important anonymity is, especially in intrusive operations such as enumeration. I'm positively surprised.

Asdethprime - June 15, 2017, 1:13 am

Thank you very much for the kind words

Obfuscatedcode - July 6, 2019, 2:29 am

(Jun 15, 2017 01:13 AM)Asdethprime Wrote: [\[CITE\]](#) Thank you very much for the kind words I liked your tutorial. The only problem I have is the fact you described having to use proxychains but you weren't very elaborate about how to keep yourself anonymous. Are you using the predefined configuration from when you install proxychains or are you setting up specific proxy lists?

Asdethprime - July 6, 2019, 3:14 am

(Jul 6, 2019 02:29 AM)Obfuscatedcode Wrote: [\[CITE\]](#) I liked your tutorial. The only problem I have is the fact you described having to use proxychains but you weren't very elaborate about how to keep yourself anonymous. Are you using the predefined configuration from when you install proxychains or are you setting up specific proxy lists?

Pre-defined configuration with TOR.

I am just using proxychains as a convenient means to invoke TOR, no additional proxy configured.

Obfuscatedcode - July 6, 2019, 5:15 am

(Jul 6, 2019 03:14 AM)Asdethprime Wrote: [\[CITE\]](#) Pre-defined configuration with TOR.

I am just using proxychains as a convenient means to invoke TOR, no additional proxy configured. Thanks for the clarification. Although I strongly advise against using tor network for any form of reconnaissance if these tests are being conducted without the owners consent. For educational purposes you have composed a top quality guide. I appreciate your share bro!

Asdethprime - July 6, 2019, 8:24 am

(Jul 6, 2019 05:15 AM)Obfuscatedcode Wrote: [\[CITE\]](#) Thanks for the clarification. Although I strongly advise against using tor network for any form of reconnaissance if these tests are being conducted without the owners consent. For educational purposes you have composed a top quality guide. I appreciate your share bro!

Thanks for the kind words.

Our of curiosity, why not use TOR though? You wanna hide your IP TOR is the best tool out there really.

Obfuscatedcode - July 7, 2019, 4:03 am

(Jul 6, 2019 08:24 AM)Asdethprime Wrote: [\[CITE\]](#) Thanks for the kind words.

Our of curiosity, why not use TOR though? You wanna hide your IP TOR is the best tool out there really.

Tor is one of the most deceitful networks. People who think they are safe when using tor network don't understand just how much governance pressence is there. Let's say you infiltrated someone like Microsoft or IBM using tor network are you really safe? You didn't realise that tor actually leaked nodes and exposed your real IP address. And with the government presence on the tor network it's easy to locate people and track them down even through a solid chain of proxies. This is my opinion based on past experiences.

HSGM - July 8, 2019, 1:46 pm

I dont think you understand how Tor works.

What do you mean "government presence on the Tor network"? Tor was a government project and is likely still used by the government to carry out non-attributable activity ..

Tor by design doesn't "expose" your IP. Its doing things like running javascript/flash/java content on webpages that often deanonymize users. Although there are types of attacks that can cause

resource exhaustion on various tor servers that allow for deanonymization ,that have to do with servers running the Tor service, often not the end user connecting to the node as one of their hops.

Tor is far safer than any VPN or any other technology you can use, dont fill peoples heads with nonsense.

Bastille - *July 8, 2019, 1:56 pm*

Just leaving a comment in order to read it thoroughly when I will have more time.

Thanks for this thread OP ?

Last_viking - *July 12, 2019, 10:28 am*

Very good tutorial. Very basic so that every body can understand. Leaving a post here looking forward to see more HQ thread by you