

Forum:[Hack Forums](#)

Thread: [Basic recon for website exploitation. Episode 1.](#)

Mr. Robot - December 10, 2019, 2:06 am

Alright let's just get started because nobody cares about a whole story.

Do you have physical access to a device the target uses at any point in time?
Are you able to go near (not enter) their house? Such as reaching their WiFi network from a car or close by.

Do you not have any of the above?

//These will be covered at a later point. I'll give you the run down/short on each here:

The main objective would be to exploit their WiFi and run a man in the middle attack or exploit machines on their network -

Otherwise you would want to install a RAT locally to the machine and monitor it if you have even a few seconds of physical access -

Finally you have steps such as fake emails and infecting them via links and/or downloaded files.

>> Step 1 of any hack can be put down to 3 things.

1a) What information can we find about the target?

1b) What information are we hoping to obtain about the target?

1c) What is the end goal for the mission at hand.

Let's identify a target and walk through what we would do. Let's say we want to hack a website with the end goal being to have access to the admin panel. These are some of the steps I would take depending on how badly I needed access and how big/small the site is.

Chapter 1. Identifying information about the target.

Quick, dirty and easy.

Spoiler ([Click to View](#))

Head to <https://weleakinfo.com/> and put in the domain.

Write down all the emails and passwords we find if any before we go any further. List them as Email:Password or each on a line.

You will also want to search the name of the website as a username and an email prefix shown in the images below.

Where shall the mail be going and what are you running?

Spoiler ([Click to View](#))

Now we need to identify what the website is running and where their mail server is. For this I would use the following respectively.

<https://builtwith.com/>

<https://mxtoolbox.com/>

Who be hosting yarr site? ?

Spoiler ([Click to View](#))

After that we will want to head to shodan.io and look for any services running. First we will want to find the IP of the website if we can and the easiest ways to do this when possible are the following:

Ping the website using CMD

And if using cloudflare try the following in Kali Linux:

[/b][b]

Code git clone <https://github.com/m0rtem/CloudFail.git>

cd CloudFail

sudo apt-get install python3-pip

pip3 install -r requirements.txt

python3 cloudfail.py --target hackforums.net

Then head to Shodan.io and put in the IP address you locate.

What be ye' hiding from me?

Spoiler ([Click to View](#))

Now we want to use Sublist3r to find any additional subdomains for the website such as mail.hackforums.net or admin.hackforums.net

A good alternative is also SubBrute which can be effective.

Have you heard the Word? About the Word?

Spoiler ([Click to View](#))

If the website is running wordpress, we want to identify if it is vulnerable at any point within the site itself. For that run wpscan.

Code wpscan --url <https://hackforums.net> --enumerate vpCode wpscan --url <https://hackforums.net> --enumerate vt

Or try and identify users/usernames that we can then look back up on weleakinfo.com

Code wpscan --url <https://hackforums.net> --enumerate u

>>Some last notes for this basic recon.

Spoiler ([Click to View](#))

Make sure you run tor on Kali Linux while you are doing this.

```
Code git clone https://github.com/susmithHCK/torghost.git
cd torghost
chmod +x install.sh
./install.sh Then run
Code torghost startOr
Code torghost stopOr
Code torghost switch respectively.
```

>>After you identify any emails from weleakinfo search them on Facebook as well as Skype to find real names. Also don't be afraid to search unique passwords you find to associate different emails for the target as well as IP addresses and usernames. This can be helpful to find gmails/hotmails and other from a domain email for the target.

>>These are very basic recon techniques that in most cases prove to be succesful when targeting smaller or local websites rather than anything large.
We haven't covered any 'intrusive' scanning besides wpscan which is on the lighter side

And if you really want to skid it all up even further- use the following
Spoiler ([Click to View](https://github.com/Anon-Exploiter/SiteBroker.git))<https://github.com/Anon-Exploiter/SiteBroker.git>

Please remember these barely scratch the surface of what is to come, these are just the first steps you should take in identifying what the target is and the goal at hand.

Tokyo - December 10, 2019, 2:41 am

Simple but informative recon guide, great stuff Mr. Robot.

Mr. Robot - December 11, 2019, 3:08 am

(Dec 10, 2019 03:41 AM)Tokyo Wrote: ([CITE](#)) Simple but informative recon guide, great stuff Mr. Robot.

Well thanks for your input/

Trialz - December 11, 2019, 5:37 pm

I hope you don't live near my house lmfaol but good thread man enjoyed it

tux1 - December 12, 2019, 10:48 am

Nice tutorial, would like to see the next part.

It's also worth mentioning looking at the robots.txt file because occasionally you find something interested in there.

Mr. Robot - December 13, 2019, 1:06 am

(Dec 12, 2019 11:48 AM)tux1 Wrote: ([CITE](#)) Nice tutorial, would like to see the next part.

It's also worth mentioning looking at the robots.txt file because occasionally you find something interested in there.

As well as sitemap.xml but it's all dependent on the site.

ETH - January 2, 2020, 7:36 am

The user changed his github name please update on thread
git clone <https://github.com/SusmithKrishnan/torghost.git>

Dhoroty - January 2, 2020, 8:15 am

I would also look for the security.txt. Not widely used yet, but if it exists, it should contain a contact

information, than can also be targeted.

Lor?d - *January 2, 2020, 8:22 am*

Very nice thread, thanks for this contribution!

Anonfriendz - *January 5, 2020, 11:39 am*

Nice thread..

Gonna give it a trial.

JamalNazamAli - *January 12, 2020, 11:00 am*

Simple tutorial and the same so good! GJ again, dude. =))

dedsec - *January 15, 2020, 4:10 pm*

Thanks for this tutorial robot, very well explained.