

Forum:[Hack Forums](#)

Thread: [Gaining root on the same LAN \(school homework\)](#)

longgone - February 3, 2020, 6:25 am

Hi guys.

I'm very very beginner in all this stuff. :) Please could anyone show me a direction how to gain root on the Linux server machine on the same LAN remotely using Kali. My prof gave us just .ova with victim machine VM, no other files or hints. From Kali I can ping it and running nmap I see 3 open ports:

22 open ssh OpenSSH 7.4 (protocol 2.0)

80 open http Apache/2.4.6 (CentOS) PHP/5.4.16

3306 open mysql MariaDB (unauthorized)

One of restrictions of this homework is that we can't use bruteforce ('auxiliary/scanner/ssh/ssh_login' is impossible).

Please help me with some advises.

I can give a link on my Dropbox with .OVA file of victim Linux machine in PM (because I don't have right to post links directly here)...

IP of victim machine is 192.168.100.171 host only.

CyberStrike - February 3, 2020, 6:50 am

Start out with googling each service and version from that nmap scan, you more than likely will find an exploit (eg php version is older as well as OpenSSH). Either way start Googling, next that Apache have you looked to see what it serves up? Look at the source you may find a password or something else equally as silly, either way there are probably a few entry points. Is this a public VM or no? I ask this only because it doesn't help if we do the work, as learning is the most important thing.

longgone - February 3, 2020, 7:48 am

(Feb 3, 2020 07:50 AM)CyberStrike Wrote: [\[CITE\]](#) Start out with googling each service and version from that nmap scan, you more than likely will find an exploit (eg php version is older as well as OpenSSH). Either way start Googling, next that Apache have you looked to see what it serves up? Look at the source you may find a password or something else equally as silly, either way there are probably a few entry points. Is this a public VM or no? I ask this only because it doesn't help if we do the work, as learning is the most important thing.

Thank you for answer! Yes, that what I do already 3 days non-stop but no success. :(Everywhere what I find people use auxiliary/scanner/ssh/ssh_login but it's not a good way in this case because victime-machine doesn't use silly pwd (I have tried already to bruteforce it using silly pwd FILE_PASS.txt). And my prof has warned us that root pwd is quite complex.

Also I tried to exploit "MariaDB Server versions and the Remote Root Code Execution Vulnerability CVE-2016-6662" but ut I didn't succeed. :(As I said all these is absolutely new for me and I can't imagine what I can do more, I'm totally stucked.

I will send you in PM download link if you agree, maybe you'll have some idea what I cad do... Thank you so much!

Unfortunately I don't have yet rights to send PM. So I can't send you a link. (((Could you send me a

PM please? Maybe I'll have possibility to answer there... Thx...

CyberStrike - February 3, 2020, 8:36 am

(Feb 3, 2020 08:48 AM)longgone Wrote: [\[CITE\]](#) Thank you for answer! Yes, that what I do already 3 days non-stop but no success. :(Everywhere what I find people use auxiliary/scanner/ssh/ssh_login but it's not a good way in this case because victime-machine doesn't use silly pwd (I have tried already to bruteforce it using silly pwd FILE_PASS.txt). And my prof has warned us that root pwd is quite complex.

Also I tried to exploit "MariaDB Server versions and the Remote Root Code Execution Vulnerability CVE-2016-6662" but ut I didn't succeed. :(As I said all these is absolutely new for me and I can't imagine what I can do more, I'm totally stucked.

I will send you in PM download link if you agree, maybe you'll have some idea what I cad do... Thank you so much!

Unfortunately I don't have yet rights to send PM. So I can't send you a link. (((Could you send me a PM please? Maybe I'll have possibility to answer there... Thx...

Do you know the name of the VM? Chance is that it's public. Either way sometimes exploits take a few tries remember you may have an application or service crash along with your exploit.

longgone - February 3, 2020, 8:54 am

```
msf5 exploit(multi/http/php_cgi_arg_injection) > run
```

```
[*] Started reverse TCP handler on 192.168.100.181:4444
```

```
[*] Exploit completed, but no session was created.
```

Nothing also.

CR300E-2020-hackmev4.ova

But I don't think it's public. I've receive the link on Dropbox from my prof.

To find what is running on Apache I can use dirb?

But I understand nothing here... what I can use...

I found that WordPress is running on vm...

CyberStrike - February 3, 2020, 4:07 pm

(Feb 3, 2020 09:54 AM)longgone Wrote: [\[CITE\]](#) msf5 exploit(multi/http/php_cgi_arg_injection) > run

```
[*] Started reverse TCP handler on 192.168.100.181:4444
```

```
[*]Exploit completed, but no session was created.
```

Nothing also.

```
[*]
```

CR300E-2020-hackmev4.ova

But I don't think it's public. I've receive the link on Dropbox from my prof.

```
[*]
```

To find what is running on Apache I can use dirb?

But I understand nothing here... what I can use...

[*]

I found that WordPress is running on vm...

I would actually have ZAP or Burp running and navigate the site, you can use dirb as well of course pay attention to your rates when requesting if there is a WAF it can block you. This said I would start exploring that WordPress finding the different plugins and so forth. There is a saying that WordPress is a backdoor with blogging functionality.

longgone - February 3, 2020, 8:15 pm

Unfortunately I didn't understand a thing what have you written... I have to read about all these ZAP, Burp, WAF... because it's first time I here about... Thank you a lot!

CyberStrike - February 4, 2020, 1:37 am

(Feb 3, 2020 09:15 PM)longgone Wrote: [\[CITE\]](#) Unfortunately I didn't understand a thing what have you written... I have to read about all these ZAP, Burp, WAF... because it's first time I here about... Thank you a lot!

That's okay learning is important a WAF is a firewall used for protecting webapps, perhaps it limits request rates or it looks for certain common attempts to inject a sql query and prevents it. ZAP and Burp are both intercepting proxies and are common to use in a web application penetration testing. I am sure that such things must have been covered in your course before handing out this VM lab.

longgone - February 4, 2020, 6:59 am

/I am sure that such things must have been covered in your course before handing out this VM lab.

Unfortunately not. It's just first CR300E Introduction to Cybersecurity course where they explain us what is hash, symmetric and asymmetric encryption, nothing more... Nothing about the things you told about...

ubernewb - February 4, 2020, 9:31 am

Hard to believe that they would throw out an assignment having given nothing that would provide insight prior. Start simple. There is probably something obvious that you've overlooked.

longgone - February 4, 2020, 4:08 pm

Yeh it's hard to believe for me too but unfortunately that is the situation I live... Problem is that my course is online, no personal communication in the class, when we can exchange with colleagues or prof.

pybug - February 4, 2020, 5:16 pm

(Feb 3, 2020 05:07 PM)CyberStrike Wrote: [\[CITE\]](#) I would actually have ZAP or Burp running and navigate the site, you can use dirb as well of course pay attention to your rates when requesting if there is a WAF it can block you. This said I would start exploring that WordPress finding the different plugins and so forth. There is a saying that WordPress is a backdoor with blogging functionality.

Burp suite, GO/DIRbuster. I see someone knows what they are talking about and is a genuine exploiter. ;)

CyberStrike - February 5, 2020, 4:12 am

(Feb 4, 2020 06:16 PM)pybug Wrote: [\[CITE\]](#) Burp suite, GO/DIRbuster. I see someone knows what they are talking about and is a genuine exploiter. ;)

There are several others here who also are knowledgeable, much more than myself, I probably should have included WPSeku/WPscan, but then again you learn little from automated tools. Actually looking at the source will give more of a feel as well as giving one an option for

Enumeration and testing ACLs/Authentication/..etc.

longgone - February 5, 2020, 5:26 am

Thank you for all your advises! This weekend I'll try them all! I'll write after if I could get to the end. :)

Manks - February 5, 2020, 5:29 am

(Feb 4, 2020 10:31 AM)ubernewb Wrote: [\[CITE\]](#) Hard to believe that they would throw out an assignment having given nothing that would provide insight prior. Start simple. There is probably something obvious that you've overlooked.

I agree with him; there must be something easy that you just strangely overlooked.

tulamba - February 5, 2020, 1:49 pm

(Feb 5, 2020 06:26 AM)longgone Wrote: [\[CITE\]](#) Thank you for all your advises! This weekend I'll try them all! I'll write after if I could get to the end. :)

Hello, could you post a link to the course website or share the vm and assignment document. I might try along with you