

Forum:[Hack Forums](#)

Thread: [You've just hacked a router web interface using default creds. What next?](#)

mread - August 21, 2017, 9:09 am

This always puzzles me. So you hack the router, you really can't do much in terms of hacking the web interface itself and there usually isn't a command-line like application, so the best you can do (I think) is seeing if you can configure it in a way that allows you to attack the network deeper.

So far, I've thought of this:

->Routers usually have a page that states what devices are connected to its interfaces. You can check those and through trial and error use port forwarding until you get to an open port on those devices.

->You can somehow make the router use a VPN to your machine and capture their traffic, although many times such option isn't available.

Sometimes routers have ssh which makes this easier, but the most difficult routers for me usually have only Telnet and maybe a ftp server.

Summarizing, imagine that you have a router which:

->Has a web interface and maybe FTP and/or Telnet (if it doesn't they usually can be enabled from the web interface)

->No command-prompt like feature and no ssh

Can you run remotely a file that you upload through FTP?

Can you somehow use Telnet as a terminal? I've been running a honeypot and Mirai sends shell commands through Telnet, however Telnet usually has it's own... language? so how does Mirai do this?

What do you do in these cases?

EBizzle - August 21, 2017, 9:24 am

It depends what you're trying to do really.

Lots of business-class routers do have CLI. Cisco IOS for example.

If you gain access to the router, you can turn off the DHCP and set up your own DHCP via a VPN - this allows you to control DNS.

Which in turn allows you to redirect websites.

For example, you could set up a Facebook spoof login page that captures login credentials.

Is there something specific that you're trying to achieve?

mread - August 21, 2017, 9:33 am

(Aug 21, 2017 09:24 AM)EBizzle Wrote: [\[CITE\]](#) It depends what you're trying to do really.

Lots of business-class routers do have CLI. Cisco IOS for example.

Interesting.

Quote:If you gain access to the router, you can turn off the DHCP and set up your own DHCP via a VPN - this allows you to control DNS.

Which in turn allows you to redirect websites.

For example, you could set up a Facebook spoof login page that captures login credentials.

What if I can't use a VPN with the router?

Quote:Is there something specific that you're trying to achieve?

I'm just trying to find a more general approach.

?Jinx - August 21, 2017, 10:18 am

For me, I start pivoting to get to other devices and try to infect them or able to control them by using some exploits, if you want to start learning this then look up Armitage and Cobalt Strike (it's Linux based). Another thing I would try on a router is to see if the router has exploits for that certain router. If you want to check it out then go [\[Here\]](#). I would like to talk more about this subject but currently, I have to go somewhere so I might make a EDIT when I come back (depending on the thread).

EBizzle - August 22, 2017, 1:52 am

If you can't use VPN, then as Jinx says - you want to try and infect the machines connected to that network.

Once connected to those, there's a whole plethora of things you can do.

From social engineering for passwords etc, to inspecting packets, to ransomware or a RAT.

Figure out what your end goal is and then research from there. :)

LD_PRELOAD - August 22, 2017, 6:40 am

Attempt to reach arbitrary execution. If do, elevate privs until satisfied. Document everything and report.

mread - August 22, 2017, 6:55 am

(Aug 22, 2017 06:40 AM)LD_PRELOAD Wrote: [\[CITE\]](#) Attempt to reach arbitrary execution. If do, elevate privs until satisfied. Document everything and report.

How do I reach arbitrary execution?

(Aug 22, 2017 01:52 AM)EBizzle Wrote: [\[CITE\]](#) If you can't use VPN, then as Jinx says - you want to try and infect the machines connected to that network.

Yeah, the issue is that I don't know how without some sort of shell or pivoting. All I can think of in this case is port forwarding.

Faith Connors - August 22, 2017, 7:06 am

(Aug 22, 2017 06:55 AM)mread Wrote: [\[CITE\]](#) How do I reach arbitrary execution?
theres not one answer

LD_PRELOAD - August 22, 2017, 7:08 am

(Aug 22, 2017 06:55 AM)mread Wrote: [\[CITE\]](#) How do I reach arbitrary execution?You see what you get and attempt to work your way with it. Say, you logged in a CGI web panel of some sort. Look for the shell interface, whether it's displayed normally or hidden ("Install remote router update" also counts). Another way is just to look for vulnerabilities in the web service. There are lots.

mread - August 22, 2017, 7:17 am

(Aug 22, 2017 07:08 AM)LD_PRELOAD Wrote: [\[CITE\]](#) ("Install remote router update" also counts).
How so?

lwrist - August 22, 2017, 7:19 am

open up ports and command the whole router by hosting your payload on the network and the rest is easy from there

StopBackDooring - August 22, 2017, 7:45 am

You can always look at the devices list and spoof as one of the devices and grab that whatsapp by the ass.

_Pr0xy - August 23, 2017, 1:48 pm

I personally don't know if it is possible or not but if you have access to the router page then maybe install some custom firmware to the router? Maybe a backdoor or something?

LD_PRELOAD - August 23, 2017, 2:04 pm

(Aug 22, 2017 07:17 AM)mread Wrote: [\[CITE\]](#) How so?It's usually an available option. Not sure whether remotely or not, but sometimes you can update the router's firmware out of an http link or an sd card. That's code execution.

mread - August 23, 2017, 6:58 pm

(Aug 23, 2017 02:04 PM)LD_PRELOAD Wrote: [\[CITE\]](#) It's usually an available option. Not sure whether remotely or not, but sometimes you can update the router's firmware out of an http link or an sd card. That's code execution.

But you'd have to have access to the original firmware so that you could modify it, right?

If not and if I am not mistaken, firmware files are .bin files, so technically you could just save some shellcode directly to a .bin file and upload it and have it run as a firmware update? Wouldn't that crash the router or something?

omarscar - August 24, 2017, 4:49 am

(Aug 22, 2017 07:45 AM)StopBackDooring Wrote: [\[CITE\]](#) You can always look at the devices list and spoof as one of the devices and grab that whatsapp by the ass.

could you explain more please ^_^

_bengi - August 24, 2017, 5:08 pm

(Aug 21, 2017 09:09 AM)mread Wrote: [\[CITE\]](#) This always puzzles me. So you hack the router, you really can't do much in terms of hacking the web interface itself and there usually isn't a command-line like application, so the best you can do (I think) is seeing if you can configure it in a way that allows you to attack the network deeper.

Most SOHO routers let you enable the telnet and/or SSH service in the web interface. If not, you can usually get code running on the device either through a vulnerability in the web interface or via various other tricks.

(Aug 21, 2017 09:09 AM)mread Wrote: [\[CITE\]](#) Summarizing, imagine that you have a router which:
->Has a web interface and maybe FTP and/or Telnet (if it doesn't they usually can be enabled from the web interface)

->No command-prompt like feature and no ssh

Can you run remotely a file that you upload through FTP?

Can you somehow use Telnet as a terminal? I've been running a honeypot and Mirai sends shell commands through Telnet, however Telnet usually has it's own... language? so how does Mirai do this?

What do you do in these cases?

Think of telnet as unencrypted SSH. Everything you can do through SSH, you can do through

telnet. Telnet doesn't have its own "language" in the sense that it has its own shell scripting language, it simply pipes all network input to the configured shell.

Anyway, there's several ways to compromise networks using the router as a pivot but it depends on the features the router has. You can usually reconfigure the primary and secondary DNS servers to point to a malicious server that replies to queries to targeted domains with forged responses. This can be used to perform phishing attacks or serve malware, for example. If you get shell access, you can upload cross compiled and statically linked tools to the device for pivoting and intercepting network traffic (e.g. port scanners, proxies for tunneling, packet sniffers, etc). Again, there's a bunch of different things you can do when you have access to a router, but it depends on the features that the router has and your level of access.

(Aug 23, 2017 06:58 PM)mread Wrote: [\[CITE\]](#) But you'd have to have access to the original firmware so that you could modify it, right?

If not and if I am not mistaken, firmware files are .bin files, so technically you could just save some shellcode directly to a .bin file and upload it and have it run as a firmware update? Wouldn't that crash the router or something?

Most embedded device manufacturers make their firmware available for download on their website for update purposes but there's other ways to get it through technical means. You can extract the filesystem from the firmware image (which is usually squashfs), modify it to include your tools and then repackage it. You can even get it to run a backdoor every time the device boots up by modifying an init/startup script. From here, assuming the manufacturer of the device doesn't cryptographically sign their firmware, you can flash it on to the device through the web interface. In the somewhat rare case where they actually do sign their firmware, you can usually write a command line tool that implements the flashing/firmware updating logic and use that to get your evil firmware image on to the device (this is assuming the cryptographic process for verifying the integrity of the firmware image isn't implemented at the hardware level).

Side note, I've actually written several post-exploitation tools that are designed specifically for sniffing and manipulating network traffic at the router level.

mread - August 28, 2017, 7:26 pm

(Aug 24, 2017 05:08 PM)_bengi Wrote: [\[CITE\]](#) Most embedded device manufacturers make their firmware available for download on their website for update purposes but there's other ways to get it through technical means. You can extract the filesystem from the firmware image (which is usually squashfs), modify it to include your tools and then repackage it. You can even get it to run a backdoor every time the device boots up by modifying an init/startup script. From here, assuming the manufacturer of the device doesn't cryptographically sign their firmware, you can flash it on to the device through the web interface. In the somewhat rare case where they actually do sign their firmware, you can usually write a command line tool that implements the flashing/firmware updating logic and use that to get your evil firmware image on to the device (this is assuming the cryptographic process for verifying the integrity of the firmware image isn't implemented at the hardware level).

Thanks a lot for your post, very informative and useful.

Probably a noob question, but if I were to do that how would I pack the firmware again afterward?

And my router only has Telnet available, not SSH, and this weird command line that looks nothing like the linux command line. I guess it's some custom one from my ISP. That's why I got confused.

_bengi - August 29, 2017, 5:11 pm

(Aug 28, 2017 07:26 PM)mread Wrote: [\[CITE\]](#) Thanks a lot for you post, very informative and useful.

Probably a noob question, but if I were to do that how would I pack the firmware again afterward?

And my router only has Telnet available, not SSH, and this weird command line that looks nothing like the linux command line. I guess it's some custom one from my ISP. That's why I got confused. dd, binwalk, RPEF (re: <https://github.com/mncoppola/rpef>), etc can be used for (re)packaging firmware images. And yes, that's common. See what commands are available and then see if you can take advantage of any of them. There's usually a command for dropping into a shell.