PenTest Lab Exercise Ex0b0 – Pivot

Goal

Learn about pivots by connecting to an otherwise inaccessible web server on devbox.artstailor.com. Along the way, use a chisel socks proxy to nmap a host and forward a port.

Tasks

1. Log in to the ndg box and schedule an Ex0b0 lab.

2. Pentest lead, Hank Hacker, discussed access to the artstailor.com internal network with Art and Otto and they have made several changes to their systems.

   To better secure the network, Otto modified the admin password on innerouter.artstailor.com.

   To help you gain effective access to their network (and save them time and money), they have added a local administrator account pr0b3 with password H4ckB4ckJ4ck on costumes.artstailor.com. They have also enabled remote procedure call as well as file and printer sharing (via SMB) on that machine. They are also forwarding ports 135, 139, 445, and 3389 from innerouter to costumes if the access originates from kali.pr0b3.com. This means you should now be able use rdesktop and psexec with pr0b3's credentials against innerouter to gain local administrative access to costumes from kali.

   Hank has asked you to use chisel to nmap host devbox.artstailor.com to see what kind of machine it is (Windows or Linux) and if there might be a development version of the artstailor.com web site running there.

   Compiled chisel executables for Linux and Windows can be found in directory /home/kali/Chisel on kali. Hank says you should disable host discovery on any nmap because chisel's SOCKS5 proxy does not tunnel ICMP packets. Make sure to nmap as few ports as you can that will most reliably tell you if this is a Windows or Linux host and use version detection to help narrow this down.

3. If you do find a web server on `devbox`, forward a local port on `kali` there and open that page with your web server. Report the apparent status of development of Art's web application.

4. Submit a report with an attack narrative answering Hank's questions and describing your activities in sufficient detail for a knowledgeable person such as your instructor or a TA to be able to understand and replicate your results.

5. And yes, a key is available, but you need to pay attention in order to find it.