Hacker vs Hacker

License

This work by Z. Cliffe Schreuders at Leeds Metropolitan University is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Contents

Preparation

These tasks can be completed on the LinuxZ IMS image. Download the Metasploitable and Backtrack Installed VMs using the download script. When prompted whether you want to run the VMs select "Yes".

Configuring the environment

Edit the settings of the two VMs, and confirm the VM networking is set to "Bridged".

Note IP addresses

Login to the Metasploitable VM (the username and password are displayed on screen when you start the VM), and run "`sudo dhclient`" on the Metasploitable VM to renew its IP address.

On your two VMs run ifconfig. Make a note of the two IP addresses. You will need these later.

Optional preparation (in advance of the lab session)

Run Snort (and/or Wireshark) on your Backtrack or Kali Linux VM (set to promiscuous mode -- refer to the Snort lab), to detect attacks.

Use msd5sum/shasum to record the state of the Metasploitable system, so you can detect what files have changed. (Md5sum is available on Metasploitable)

Configure Metasploitable to do remote logging, so that the attacker cannot modify your logs.

Create a backup of the files on your Metasploitable system, for later comparison.

Any other responsive or detection methods you like. You are *not allowed to increase defensive security*.

Hacker vs hacker!

In this session:

1. Share the IP address of your Metasploitable system with classmates
2. Exploit a vulnerability in someone else's Metasploitable system

   You could follow an online tutorial such as: http://securitypadawan.blogspot.co.uk/2011/10/metasploitable-backtrack-fun.html
   OR
   http://securitypadawan.blogspot.co.uk/2011/10/attacking-metasploitable-part-2.html
   OR
   Any other tutorial, or just find an exploit that works!

During the Hacker vs Hacker lab session, take a screenshot showing how you have compromised their system.

Label it or save it as "HackerVsHacker-1".

---

3. Edit a file on their compromised system: for example, /etc/syslog.conf or /etc/securetty

4. Create a user account on their compromised system (optionally install a rootkit or backdoor, but you may not have time to do this)

During the Hacker vs Hacker lab session, take screenshots showing the file(s) you have modified, and any backdoors you have created.

Label it or save it as “HackerVsHacker-2”.

---

5. On your own system, use all the skills you have learned in this module (and software tools of your choice) to figure out:

    a. The IP address of the attackers that have compromised your own system

---

During the Hacker vs Hacker lab session, take screenshot(s) showing the IP address of an attacker, and how you came to that conclusion (for example, a Snort alert, Syslog, Wireshark logs, network access, etc). This should preferably be using both online (network/process) and offline (logs and alerts) information.

Label it or save it as “HackerVsHacker-3”.

---

    b. How they exploited your system

During the Hacker vs Hacker lab session, take a screenshot showing evidence of how they compromised your system; for example, what exploit and/or software did they use to do the attack? What software did it target on your system?

Label it or save it as “HackerVsHacker-4”.

c. What files they changed, user accounts they created, or backdoors they left

During the Hacker vs Hacker lab session, take a screenshot showing which files they changed, user accounts they created, or backdoors they left and how you came to that conclusion (for example, using shasum output, Autopsy, mactime, diff, etc).

Label it or save it as “HackerVsHacker-5”.

What to show your tutor for XP rewards

Show your tutor each of the above (in red) evidences. You may be asked to justify your decisions. This will be used to allocate XP for the module. Further details of the XP rewards and requirements are available on the *My XP* site.