Updated: 3/4/2022

Lab 7.1 - Exploiting pippin.shire.org (10.0.5.25)

Active Recon and Service Enumeration

Conduct Active Reconnaissance against pippin. Answer the following.

`Deliverable 1. Provide screenshots of open ports, their services and versions.`

`Deliverable 2. Provide screenshots of the services as they respond to client applications like web browsers and command line clients.`

`Deliverable 3. Have you found any of the services particularly interesting? Please explain using annotated screenshots and brief captions or descriptions.`

Remote Code Execution

One of the services had been configured by a grossly incompetent systems administrator. If you are persistent, you should be able to create your own files on the remote host.

`Deliverable 4. Upload a test file (give it a distinctive Safe for Work name) and provide proof that you've done so in the form of screenshots of commands and output.`

`Deliverable 5. Provide evidence of remote code execution such that you can output the systems /etc/passwd file. How did you do this? Are there any accounts of interest? (At this point you should at least have the privileges of the attacked service)`

Hint 1 Video (to be watched after you are confident that you completed the deliverables to the best of your ability or you are tired of banging your head against the wall)

Loot

By leveraging a permissions issue in a misconfigured service, you should be able to find sensitive data if you look hard.

Deliverable 6. What did you find and how did you find it? Can you leverage this data to your advantage?

Deliverable 7. You should be able to get into pippin as an authorized user. Provide a screenshot showing your session and cat the user-flag.

Challenge: can you use your malicious upload to provide a reverse shell to your kali system running in the context of the apache user?

Elevation

Now, the web server has an application, and that application stores its data in yet another service that you likely did not see during your active reconnaissance. Leverage some of the secret data you've found to interact with this internal service to see if there is any other information about users that you might be able to use?

Deliverable 8. Enumerate this internal data source to determine where and in what fields useful data might exist. You very likely learned about this system in SYS255,265 and SEC260. Break out your old notes and get on with it. Describe what you found. In the end, you are looking for a new identity and a credential.

Deliverable 9. The credentials you've found are not terribly useful by themselves, you will need to use advanced hash cracking techniques to get what you need. There are very few references on how to get this done, but the following link might push you in the right direction and might possibly make you $25.

- The crack is not trivial and will likely take a couple hours once you figure it out
  - tip: the password starts with a lowercase 'p'.
  - it is also in rockyou
- Cracking in a lowly provisioned VM is slow. Try using humpty.cyber.local or your own physical system.
- Do this over the course of the week as opposed to asking your buddy. Provide a screenshot of your tool of choice cracking the password.

Deliverable 10. Prove that you have interactive access as root and can display the root flag.

Hint 2 Video (Only if you need it!, you may notice that there are some differences in user names and passwords)

Updated: 3/4/2022

Cleanup

If indeed you achieved root compromise, clean up any files you've uploaded.

Deliverable 11. Tech Journal and Reflection. Submit a video of you walking through your technical documentation and reflection for this week. Record voice and make sure quality is 720p or greater. Take your time and rehearse a couple times before you go live. Submit a link to your googledrive or panopto based video. Make sure your instructor has access.

- Your technical documentation should cover anything new learned in this lab and the various commands used to achieve root compromise.

- Your reflection should consider the mistakes made by Pippin's systems administrator and how they might be remedied. You should also note those areas where you need help from the hint videos, peers or instructor.