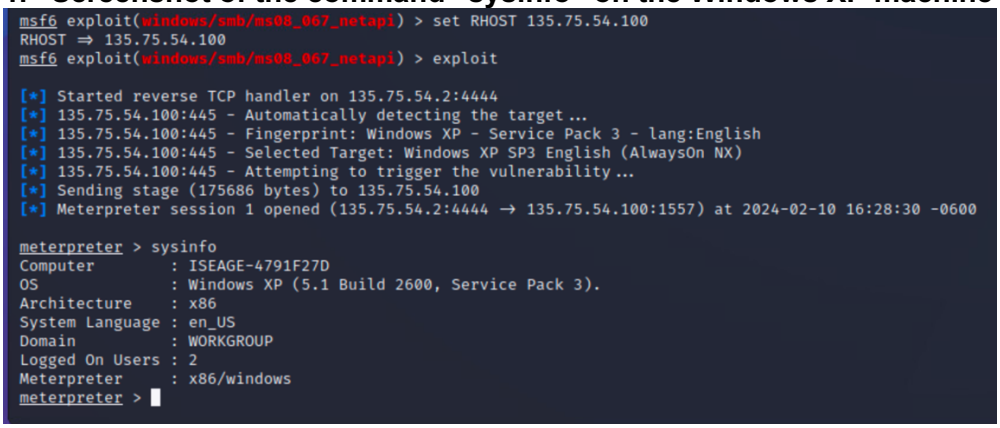
Lab Template – Ethan Roepke

1. Screenshot of the command "sysinfo" on the Windows XP machine (10 points)



2. Identify at least five commands that could be used in an attack. Explain how each of these five commands could be useful to you as an attacker. (10 points)

1. Screenshare
    1. While user is active, attacker is able to view activity, applications used, and possible sensitive information.
2. Hashdump
    1. This will allow the attacker to extract password hashes which can include user accounts, domain names and be able to get the plaintext passwords. Being able to obtain the password hashes, they will be able use across other systems in the network and gain more privileges.
3. Getsystem
    1. The getsystem command tries to gain access to the SYSTEM level, which will give the attacker full access to the system. This will allow the attacker to gain sensitive files. As well they can hide from security detections since they have highest level privileges.
4. Keyscan_start
    1. This command is very useful for attackers by gathering key logs from the victim. This can give away usernames/passwords, Credit Cards and many more personal information. You can also get sensitive messages that the user has sent and much more.
5. Idletime
    1. Idletime can allow attackers to know when users have been idle on a network. This benefits the attacker to let him know when the system will be monitored with less activity. This will minimize the detection of attacks by timing it when least active.

3. Run "getuid". What user are you running as? What permissions does this user have? (10 points)

1. We are running as NT AUTHORITY\SYSTEM. This user has permissions to everything.

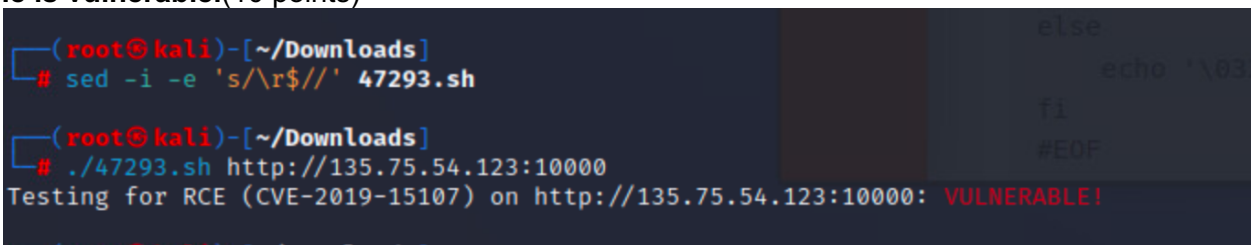
4. Identify two more post-exploitation commands and explain how the information could be used. (10 points)

1. arp_scanner
    1. Using the arp_scanner is useful if gain access into root. The attacker would be able to identify IP/MAC addresses, understand network topology and identify protentional attacks. This information will also help the attacker gain access to other machines.
2. enum_logged_on_users
    1. Being able to know what users are active and if users are idle will minimize the risk of detection. As well as knowing what users have greater privileges will give the attacker knowledge to target their machine when idle.

5. What is this service running on port 10000? What is it used for? (3 sentences minimum) (10 points)

1. The service that is running on port 10000 is Webmin, which is a web based administration tool that is used for managing unix-like systems. It is a GUI that perform many administration tasks, such as file system configuration, network configuration, user account management and more. It makes administration tasks easier since it is remote and no need to access the server.

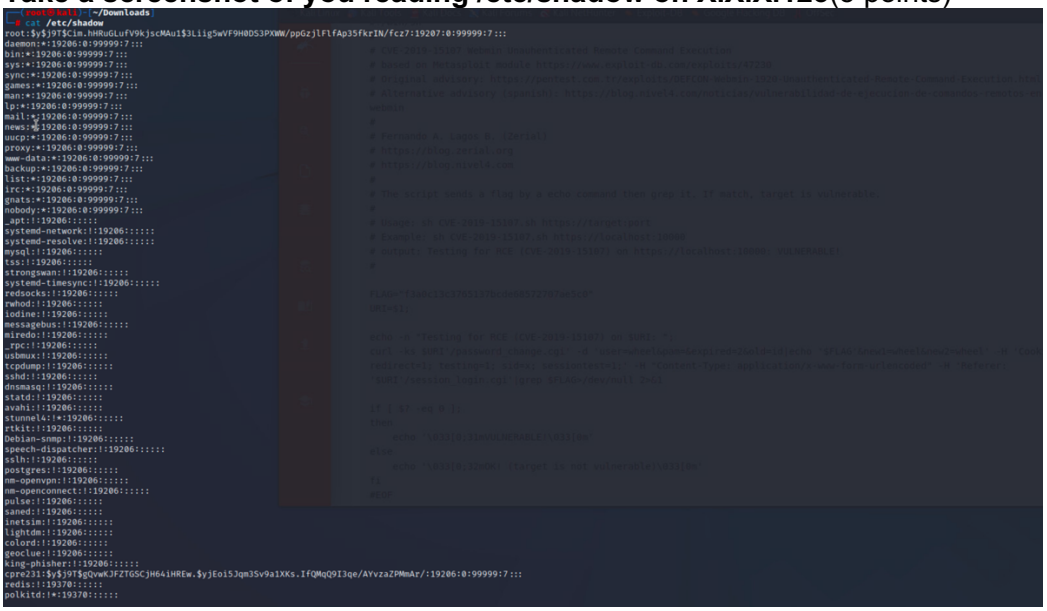
6. Run the script ./47293.sh. Take a screenshot of the output that confirms the machine is vulnerable.(10 points)



7. Answer the following questions about CVE-2019-15107: (10 points)

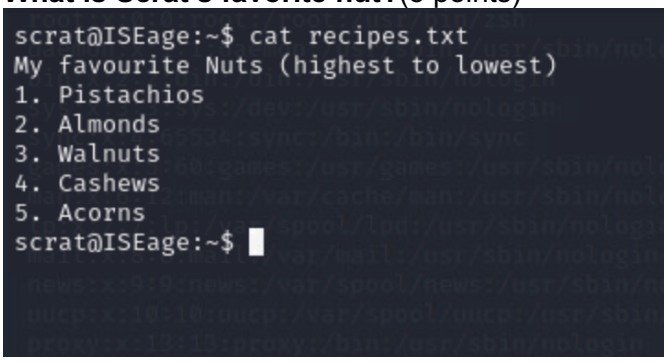
1. *How did this vulnerability come to exist?*
    1. This vulnerability came to exist to a flaw in the password change functionality of Webmin's Usermin, which was an interface used for email and change their passwords. It allowed an attacker to send a HTTP post request in the email password change which would lead to the executions of commands on the server.
2. *What version of Webmin was initially released with this vulnerability enabled by default?*
    1. Webmin 1.882
3. *What user does the remote code injection run as?*
    1. The remote code injection was running on the root user
4. *How severe is this CVE based on NVD CVSS 3.X standards?*
    1. The severity on this was critical because it gave the attacker access to root user which allows complete access to all servers.

8. **Take a screenshot of you reading /etc/shadow on X.X.X.123**(5 points)

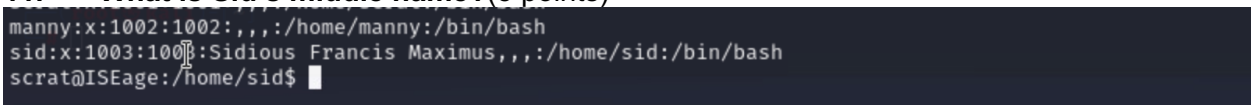


9. **What is the EoL date of this Ubuntu release on X.X.X.104?** (5 points)
End of life: May 16, 2014

10. **What is Scrat's favorite nut?**(5 points)

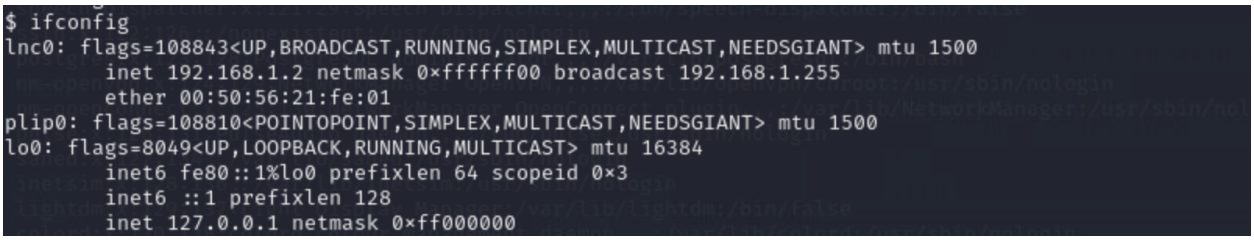


11. **What is Sid's middle name?**(5 points)



Middle name is Francis

12. **What is the local IP address of "Manny's Home"?** (5 points)



13. What is the name of Manny's Nana?(5 points)
Grandma Fur