Turn In lab 10 – Ethan Roepke

1. **Submit a screenshot of the SSH brute force you performed from Lab 04.**

(5 points)

A screen shot of a computer

Description automatically generated

1. **Take a moment and list three potential services/options that could be configured to help mitigate brute-force attacks and why**

(5 points)

**MaxAuthTries**: the default number it is set to is 6, however if we lower this number, the likelihood of a brute force attack will be less effective because it limits the number of authentications attempts per user.

**LoginGraceTime:** having the LoginGraceTime at a lower timer will terminate the connection for being authenticated. Having at a low time will prevent brute attacks significantly.

**PermitRootLogin:** This options decides if they get root on login or if the root user needs to authenticate them through a non root user. This will make brute attack less effective as they would have to authenticate under non root user.

1. **Explain two additional methods we can use to prevent brute force attacks. Be specific.**

(5 points)

**Strong password policies:** Implementing password policies such as: minimum characters, uppercase/lowercase, and numbers/special characters which will be more resistant to brute force attacks as it will be harder to guess the password. We could implement a required password change very so often to keep passwords updated.

**Authentication limit per IP:** being able to restrict the number of authentication attempts from a specific IP and blocking that IP will help mitigate brute force attacks. We have tools such as IPTables that will automatically block IP addresses that fail ‘x’ amount of login tries.

1. **What does Event ID 4672 mean?  What privileges are assigned to somebody who logs in under this action? Be specific, no less than five sentences.**

(5 points)

Event id 4672 is a special privilege assigned to new logon. The user will be granted privileges in one or more groups. The event will be logged when a user’s group privilege is changed on the specific system such as being added/removed from a group or the permissions were modified. Somebody who logs in under this action would either have administrative access which would have full access and as well other groups below administrative.

1. **Take a screenshot of the failed NTLM login in Windows Event Viewer. What is the Event ID (four-digit0 code) of the failed login**

(5 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of modified password policy**

(5 points)

A screenshot of a computer

Description automatically generated

1. **What are the “complexity requirements” that we have enforced?**

(5 points)

The complexity requirements that are enforced if enabled means the password must meet certain minimum requirements. This includes not including users full/part of users account name, at least 6 characters, and include 3 of these 4 options(capital letter, lowercase letter, number from 0-9, and special character).

1. **Screenshot of successful telnet login**

(5 points)

A screenshot of a computer screen

Description automatically generated

1. **Screenshot of updated pfSense port-forwarding rules**

(5 points)

A screenshot of a computer

Description automatically generated

1. **Screenshot of failed telnet login**

(5 points)

A computer screen shot of a computer

Description automatically generated

1. **Screenshot of listening ports on XX.XX.XX.104**

(5 points)

A screen shot of a computer

Description automatically generated

1. **What service is running at port 3306?**

(5 points)

Port 3306 is associated with MySQL protocol. This port is used to connect to MySQL clients and utilities such as mysqldump.

1. **Screenshot of default incoming/outgoing UFW policies**

(5 points)

A black screen with white text

Description automatically generated

1. **Screenshot of newly created UFW rules**

(5 points)

A black screen with white text

Description automatically generated

1. **Screenshot of nmap scan results showing blocked port 3306**

(5 points)

A computer screen with white text

Description automatically generated

1. **Specify which domain these packages are being downloaded from.  Why?**

(5 points)

These packages are being downloaded from the domain “ubuntu”. We had to get the deb files from ubuntu to make sure the deb files are stable with other OS that are used with ubuntu, easy to install through ubuntu, and for a level of security to address vulnerabilities and bugs.

1. **Screenshot of upgraded kernel version**

(10 points)

A black screen with white text

Description automatically generated

1. **Screenshot of “hung” Dirty Cow**

(5 points)

A computer screen with white text

Description automatically generated

1. **Number of versions will you have to upgrade through from 13.10 to the current LTS**

(5 points)

5 versions