OS Hardening Incident Report

Objective: Analyze an incident involving brute-force login and web malware injection.

Summary: A server was compromised through weak credentials, allowing the attacker to inject malicious scripts that redirected users to an external site. DNS and HTTP logs showed indicators of tampering.

Tools: Manual log review, basic Linux commands, incident template

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident : DNS, HTTP and IP

Section 2: Document the incident
The incidence occurred when the admin only have weak password, and then, the login was leaked with brute force attack, and the attacker succeeded login and create code for run malware downloadable when customer visit web, and then the malware redirect the web. The evidence is of the incident is *tcpdum*b logs. **Findings**: ● Brute-force login was successful against an admin account without MFA ● Web defacement occurred via remote code execution ● No login alerting or rate-limiting was in place

Section 3: Recommend one remediation for brute force attacks
To prevent brute force we can implement several action, these 3 of them : 1. Requiring strong passwords : prevent from brute force attack t guess the password. Use combination of alphabet, number, symbol, lowercase and uppercase. 2. Limiting the number of login attempts : this can prevent from force attack to. For example, if 3 times attempts login with wrong password, the account can be lock. 3. Enforcing two-factor authentication (2FA) : if the password was leak, we can secure it with 2FA. It will confirm to the admin using email, phone number or other method the login when login activity was occurred. Other recommend is Monitoring login attempts, Requiring more frequent password changes, Disallowing previous passwords from being used.