# Security incident report –

# OS Hardening techniques

Nela-officer

Date: 05/12/2024

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocols involved in the accident is DNS and HTTP |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The logs show the following process:   * The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server. * The DNS replies with the correct IP address. * The browser initiates an HTTP request: It requests the **yummyrecipesforme.com** webpage using the IP address sent by the DNS server. * The browser initiates the download of the malware. * The browser initiates a DNS request for **greatrecipesforme.com**. * The DNS server responds with the IP address for greatrecipesforme.com. * The browser initiates an HTTP request to the IP address for greatrecipesforme.com   **Conclusion: The website was impacted by a brute force attack.**   * After checking the source code for the website, it was noticed that **javascript code** had been added to prompt website visitors to download an executable file. * Analysis of the downloaded file found a script that redirects the visitors’ browsers from **yummyrecipesforme.com** to the spoofed website **greatrecipesforme.com** * The disgruntled hacker was able to guess the password easily because the admin password was still set to the default password. * Additionally, there were no controls in place to prevent a brute force attack. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| * Implement password policies to guarantee admin password must to be changed and frequently updated but also include guidelines on how complex a password should be, how often users need to update passwords for all the user accounts. . |