VTCSEC VULNHUB CTF: WRITEUP

GOAL: BREAK INTO LINUX SYSTEM WIITH ROOT PRIVILEGE

TOOLS USED:

- nmap (network and host scanning)
- john the ripper (hash cracking)
- nikto (website scanning)
- wpscan (scan vulnerabilities in wordpress sites)
- metasploit (pen testing tool)
- pentestmonkey (scans for privilege escalation vectors (misconfigurations) in linux systems

STEPS DONE IN THIS CTF:

- RECONNAISSANCE:
    1. SCANNED NETWORK USING NMAP PING SCAN.
    2. SCANNED HOST USING NMAP AGGRESSIVE SCAN. GAINED INFORMATION LIKE OPEN PORTS (21, 22, 80), VERSIONS RUNNING.
    3. USED NIKTO FOR SCANNING SERVICE RUNNING ON PORT 80. GOT HIDDEN PAGES. WORDPRESS WAS USED.
    4. USED WPSCAN AND GOR WORDPRESS VERSIONS AND CHECKED FOR USERNAMES AND PASSWORDS USING THE FOLLOWING COMMAND:
       wpscan --url http://192.168.56.103/secret/ --enumerate u
    5. AFTER GETTING USERNAME CHECK FOR PASSWORD:
       wpscan --username admin --url http://vtcsec/secret/wp-login.php --wordlist /usr/share/wordlists/metasploit/http_default_pass.txt --wp-content-dir http://vtcsec/secret/wp-content/ --threads 20
- EXPLOITATION:
    1. USE THE ADMIN SHELL UPLOAD EXPLOIT IN METASPLOIT AND RUN IT.

2. OPEN INTERACTIVE SHELL USING **python -c 'import pty; pty.spawn("/bin/bash")'**

- PRIVILEGE ESCALATION
  1. CHECK FOR PERMISSIONS IN **/etc/passwd** (CONTAIN USER INFORMATION) OR **/etc/shadow** (CONTAIN HASH PASSWORDS)
  2. OR RUN THE PENTESTMONKEY ON THE METERPRETER: **upload /usr/bin/unix-privesc-check /tmp/unix-privesc-check** THEN RUN THE FILE IN /tmp DIRECTORY.
     ./unix-privesc-check standard | grep WARNING CHECK IN WARNINGS FOR MISECONFIGURATIONS
  3. GET THE HASH AND CRACK IT USING JOHN THE RIPPER
     john -single hashed_password.txt
  4. USE SSH FOR GAINING ACCESS TO THE SYSTEM
     ssh username@10.182.21.4

METHOD 2:

1. FTP WAS OPEN WITH VERSION PROFTPD 1.3.3C RUNNING.
2. USE proftpd_133c_backdoor(CHECK VULNERABILITY FOUND SECTION) EXPLOIT IN METASPLOIT. IT ALLOWS UNAUTHENTICATED REMOTE CODE EXECUTION VIA SPECIALLY CRAFTED FTP COMMAND: **HELP ACIDBITCHEZ** . THIS SPAWNS A ROOT SHELL AND CONNECTS BACK TO THE MACHINE. (REVERSE SHELL)

VULNERABILITIES FOUND:

- WEAK / DEFAULT CREDENTIALS
- MISCONFIGURATIONS (LIKE ALLOWING NORMAL USERS TO READ AND EDIT CRITICAL FILES)
- proftpd_133c_backdoor VULNERABILITY: MALICIOUS CODE (BACKDOOR) CAN BE INJECTED INTO THE PROFTPD SOURCE CODE. The ProFTPD 1.3.3c VERSION HAS A KNOWN BACKDOOR

THAT RESPONDS TO THE **HELP ACIDBITCHEZ** COMMAND, WHICH SPAWNS A ROOT SHELL.

- WORDPRESS REVERSE ADMIN SHELL VULNERABILITY
- LEGACY PLATFORMS AND OUTDATED VERSIONS

MITIGATION

- DISABLE OR UPGRADE VULNERABLE SERVICES LIKE PROFTPD 1.3.3C.
- USE STRONG AND UNIQUE PASSWORDS.
- RESTRICT USER PERMISSIONS.
- REGULARLY PATCH AND UPDATE THE SYSTEM.
- USE TOOLS LIKE FAIL2BAN OR IPTABLES TO LIMIT BRUTE-FORCE ATTACKS.

FINAL TAKEAWAY

THIS CTF DEMONSTRATED THE IMPORTANCE OF STRONG CREDENTIAL HYGIENE AND SYSTEM CONFIGURATION. OUTDATED SERVICES AND DEFAULT CREDENTIALS REMAIN ONE OF THE BIGGEST ATTACK SURFACES. REGULAR AUDITS AND UPDATES ARE CRUCIAL.