Vulnerability assessment task

1. The device that used as a target: Metasploite2
2. I used the ***Nmap*** command with 3 types of scans:
   The full command:sudo nmap -sV -O --script vuln 192.168.1.1/24

- -***sV***: It specifies a particular scanning technique known as the service and version scan.

  Here's a breakdown of what each part of the flag means:

  - **-s:** This indicates that you're specifying a scan type.
  - **V:** This specifies the service and version scan, which attempts to determine the service running on an open port and, if possible, its version.
- ***-O***: It specifies a particular scanning technique known as OS detection.
- ***--script***: flag is used with the Nmap network scanning tool to enable the execution of Nmap scripts. Nmap scripts are small programs written in Lua that can be used to perform a variety of tasks

Findings:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	
514/tcp	open	tcpwrapped	
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Recommendations

- **Patch Management:** Ensure all services and applications are updated with the latest security patches to address known vulnerabilities.
- **Strong Password Policies:** Enforce strong password requirements, including length, complexity, and regular changes.
- **Secure Configurations:** Configure services with secure default settings and disable unnecessary features.
- **Input Validation:** Implement input validation to prevent injection attacks (SQL injection, XSS, etc.).
- **Regular Monitoring:** Monitor systems for suspicious activity and signs of compromise.
- **Security Training:** Educate users about security best practices to reduce the risk of human error.

Critical Vulnerabilities:

- **vsftpd 2.3.4:** This version is known to have multiple vulnerabilities, including backdoors that can allow remote attackers to gain root access. Update vsftpd to a supported and patched version.
- **OpenSSH:** While the specific version (4.7p1 Debian 8ubuntu1) may not have critical vulnerabilities at this time, it's essential to keep SSH updated to the latest version to protect against future exploits. Update OpenSSH to the latest version.

Specific Service Recommendations:

- **FTP:** If FTP is necessary, consider using a more secure protocol like SFTP (SSH File Transfer Protocol) or FTPS (FTP over SSL/TLS).
- **MySQL and PostgreSQL:** Ensure strong passwords for database accounts, limit network access, and regularly update the databases.
- **VNC:** If VNC is necessary, use strong passwords and consider using a secure protocol like SSH tunneling to encrypt traffic.
- **Java-RMI:** If Java-RMI is necessary, configure it securely to prevent remote code execution vulnerabilities.
- **NFS:** If NFS is necessary, configure it securely with appropriate export restrictions and authentication mechanisms.
- By following these recommendations, you can significantly improve the security posture of the target system and reduce the risk of exploitation.

.