16/02/2024

Friday

Podili sunil gopi
B.tech iv year, IT
208X1A1229
KALLAM
HARANADHAREDDY
INSTITUTE OF TECH.

TASK 6 (STEP-1)

Hostnames	abhayamshelter.com cpanel.abhayamshelter.com cpcalendars.abhayamshelter.com cpcontacts.abhayamshelter.com mail.abhayamshelter.com webdisk.abhayamshelter.com webmail.abhayamshelter.com www.abhayamshelter.com in3.fastwebhost.com mychoicesarees.com cpanel.mychoicesarees.com cpcalendars.mychoicesarees.com cpcontacts.mychoicesarees.com mail.mychoicesarees.com webdisk.mychoicesarees.com webmail.mychoicesarees.com www.mychoicesarees.com
Domains	ABHAYAMSHELTER.COM FASTWEBHOST.COM MYCHOICESAREES.COM
Country	United States
City	Los Angeles
Organization	ReliableSite.Net LLC
ISP	ReliableSite.Net LLC
ASN	AS23470

Step2-ports

Port 80(HTTP)-This port provides an unencrypted connection between the web browser and the web servers, which leaves the sensitive user data exposed to cybercriminals and may lead to severe data misuse.

Port 443 (HTTPS) - gain unauthorized access to sensitive information. SSL/TLS vulnerabilities

Port 2082(infowave)- it is the way of establishing an unencrypted connection to the server through http(hyper text transfer protocol) opens a connection to the port number 80 cPanel port number 2083

Port 2083(cPanel - SSL)-TCP port 2083 uses the Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. TCP is a connection-oriented protocol, it requires handshaking to set up end-to-end communications. Only when a connection is set up user's data can be sent bi-directionally over the connection.

Port 2086(gnunet)-List of vulnerabilities affecting any product of this vendor.

Port 2087(eli)- Some versions of WebHost Manager used port 2087 for secure connections before switching to the standard HTTPS port 443. Using an outdated version with known vulnerabilities on port 2087 could expose your system to potential attacks.

Port 2095(Webmail)- Phishing attacks: Deceptive emails tricking users into revealing credentials or clicking malicious links.Password vulnerabilities: Weak or reused passwords can be easily compromised.

Port 2096(Webmail - SSL)- Port 2096 is not the standard secure webmail port (HTTPS - 443). This often indicates a non-standard webmail service or configuration, which might lack the security measures of established ones.**SSL Version:** The specific SSL/TLS version used on port 2096 is crucial. Older versions like SSLv3 and TLSv1.0 are outdated and have known vulnerabilities, while newer versions like TLSv1.2 and TLSv1.3 are more secure.

Vulnerabilites

CVE-2023-51385 -potentially allowing attackers to execute arbitrary code through shell injection on vulnerable servers.

1. **CVE-2023-51384**: This CVE represents a specific vulnerability identified in a software or system in 2023, which likely requires attention and possibly a patch or mitigation to prevent exploitation.
2. **CVE-2023-48795**: This CVE indicates another vulnerability discovered in 2023, potentially posing a security risk that necessitates remediation to safeguard the affected software or system.
3. **CVE-2023-38408**: This CVE signifies a vulnerability disclosed in 2023, highlighting a potential weakness that could be exploited if left unaddressed, emphasizing the importance of prompt action to mitigate the risk.
4. **CVE-2021-36368**: Although older than the others, this CVE from 2021 still underscores the significance of addressing vulnerabilities, suggesting that even historical vulnerabilities can pose risks if not adequately addressed or patched.