Vulnerability Assessment Report

Vulnerability	Risk Level	Recommended Resolution
Nmap found ftp on 21/tcp	**High**	Disable FTP or use secure SFTP with authentication.
Nmap found ssh on 22/tcp	**Low**	Review and secure this service.
Nmap found smtp on 25/tcp	**Medium**	Apply spam filters and enable authentication.
Nmap found domain on 53/tcp	**Low**	Review and secure this service.
Nmap found http on 80/tcp	**Medium**	Use HTTPS and update web server software.
Nmap found rpcbind on 111/tcp	**Low**	Review and secure this service.
Nmap found netbios-ssn on 139/tcp	**Low**	Review and secure this service.
Nmap found netbios-ssn on 445/tcp	**Low**	Review and secure this service.
Nmap found java-rmi on 1099/tcp	**Low**	Review and secure this service.
Nmap found nfs on 2049/tcp	**Low**	Review and secure this service.
Nmap found ftp on 2121/tcp	**High**	Disable FTP or use secure SFTP with authentication.
Nmap found mysql on 3306/tcp	**Low**	Review and secure this service.
Nmap found postgresql on 5432/tcp	**Low**	Review and secure this service.
Nmap found vnc on 5900/tcp	**Low**	Review and secure this service.
Nmap found x11 on 6000/tcp	**Low**	Review and secure this service.
Nmap found irc on 6667/tcp	**Low**	Review and secure this service.
Nmap found ajp13 on 8009/tcp	**Low**	Review and secure this service.
Nmap found http on 8180/tcp	**Medium**	Use HTTPS and update web server software.
Nikto: + /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options	**Medium**	Use HTTPS and update web server software.
Nikto: + /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	**Medium**	Use HTTPS and update web server software.
Nikto: + /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing	**High**	Use HTTPS and update web server software.

Nikto: + /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184	**Medium**	Use HTTPS and update web server software.
Nikto: + /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184	**Medium**	Use HTTPS and update web server software.
Nikto: + /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184	**Medium**	Use HTTPS and update web server software.
Nikto: + /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184	**Medium**	Use HTTPS and update web server software.
Enum4linux: Password ..... ''	**Medium**	Enforce strong password policies.
Enum4linux: [+] ■[0m■[32mServer 192.168.56.102 allows sessions using username '', password ''	**Medium**	Enforce strong password policies.
Enum4linux: ■[34m ==========(■[0m■[32mPassword Policy Information for 192.168.56.102■[0m■[34m)==========	**Medium**	Enforce strong password policies.
Enum4linux: [+] Password Info for Domain: METASPLOITABLE	**Medium**	Enforce strong password policies.
Enum4linux: [+] Minimum password length: 5	**Medium**	Enforce strong password policies.
Enum4linux: [+] Password history length: None	**Medium**	Enforce strong password policies.
Enum4linux: [+] Maximum password age: Not Set	**Medium**	Enforce strong password policies.
Enum4linux: [+] Password Complexity Flags: 000000	**Medium**	Enforce strong password policies.
Enum4linux: [+] Domain Refuse Password Change: 0	**Medium**	Enforce strong password policies.
Enum4linux: [+] Domain Password Store Cleartext: 0	**Medium**	Enforce strong password policies.
Enum4linux: [+] Domain Password Lockout Admins: 0	**Medium**	Enforce strong password policies.
Enum4linux: [+] Domain Password No Clear Change: 0	**Medium**	Enforce strong password policies.

Enum4linux: [+] Domain Password No Anon Change: 0	**Medium**	Enforce strong password policies.
Enum4linux: [+] Domain Password Complex: 0	**Medium**	Enforce strong password policies.
Enum4linux: [+] Minimum password age: None	**Medium**	Enforce strong password policies.
Enum4linux: [+] ■[0m■[32mRetieved partial password policy with rpcclient:	**Medium**	Enforce strong password policies.
Enum4linux: ■[0mPassword Complexity: Disabled	**Medium**	Enforce strong password policies.
Enum4linux: Minimum Password Length: 0	**Medium**	Enforce strong password policies.
Enum4linux: [+] ■[0m■[32mEnumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''	**Medium**	Enforce strong password policies.