Report Metasploitable

metasploitable

Wed, 23 Aug 2023 19:58:52 CEST

TABLE OF CONTENTS

192.168.50.2

Vulnerabilities

- 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)
- 51988 - Bind Shell Backdoor Detection
- 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
- 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
- 11356 - NFS Exported Share Information Disclosure
- 20007 - SSL Version 2 and 3 Protocol Detection
- 20007 - SSL Version 2 and 3 Protocol Detection
- 33850 - Unix Operating System Unsupported Version Detection
- 61708 - VNC Server 'password' Password
- 136769 - ISC BIND Service Downgrade / Reflected DoS
- 42256 - NFS Shares World Readable
- 42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
- 90509 - Samba Badlock Vulnerability
- 11213 - HTTP TRACE / TRACK Methods Allowed
- 139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

31705 - SSL Anonymous Cipher Suites Supported

57608 - SMB Signing not required

52611 - SMTP Service STARTTLS Plaintext Command Injection

90317 - SSH Weak Algorithms Supported

51192 - SSL Certificate Cannot Be Trusted

51192 - SSL Certificate Cannot Be Trusted

15901 - SSL Certificate Expiry

45411 - SSL Certificate with Wrong Hostname

89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

57582 - SSL Self-Signed Certificate

26928 - SSL Weak Cipher Suites Supported

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

104743 - TLS Version 1.0 Protocol Detection

70658 - SSH Server CBC Mode Ciphers Enabled

153953 - SSH Weak Key Exchange Algorithms Enabled

71049 - SSH Weak MAC Algorithms Enabled

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

10407 - X Server Detection

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)