Fake Inc.

Relatório de Avaliação de Vulnerabilidade de Host

Versão	Data	Nome
1.0	12/07/2025	Jonathan Park

Sumário

Resumo Executivo

A seguinte varredura credenciada de vulnerabilidade foi conduzida como uma avaliação geral das vulnerabilidades atuais às quais a máquina Linux (Metasploitable 2) da Fake Inc. (Cliente) com endereço IP 192.168.31.12 (“Host”) está exposto.

Metodología

Esta varredura foi conduzida com **nmap** e **Tenable Nessus Essentials**, em uma máquina Kali Linux conectado para a Host.

Scanners Usados

nmap: Um network scanner gratuito e com código aberto, desenhado para revelar o que hosts são à disposição (mesmo com redes grandes), e também uma infinidade de características sobre essas hosts (sistema de operação (OS), firewalls, serviços, etc.). Nmap é compatível com a maioria dos OSs, inclusive Windows, Mac, e Linux. nmap.org

Tenable Nessus: Um scanner comercial de vulnerabilidade. A versão gratuita, Tenable Nessus Essentials, permite varreduras de até 16 endereços IP. tenable.com/products/nessus

Resultados da Varredura

Os resultados originais e completos da varredura serão fornecidos no momento da entrega.

Avaliação de Risco

Este relatório enfatiza os riscos de segurança que podem impactar significativamente as aplicações de missão crítica que são essenciais para as operações diárias da empresa.
As varreduras em total revelaram **45** vulnerabilidades para a Host.

Crítica	Gravidade alta	Gravidade média	Gravidade baixa
11	1	39	8

Vulnerabilidades Críticas

Há **6** vulnerabilidades únicas que são críticas.

Name CVE/(CVSSv3.x score)	**Description**	**Solution**
Canonical Ubuntu Linux SEoL (8.04.x) (10.0)	This machine is run on a version of Canonical Ubuntu Linux that is no longer being supported.	Upgrade to a version of Canonical Ubuntu Linux that is currently supported (14.04+).
VNC Server 'password' Password (10.0)	VNC server is secured with a password of “password”.	Secure the VNC service with a stronger password.
vsFTP version 2.3.4 backdoor CVE-2011-2523 (9.8)	vsftpd 2.3.4 downloaded between 06/30/2011 and 07/03/2011 contains a backdoor which opens a shell on port 6200/tcp.	Upgrade vsftpd to latest version, and configure proper firewalling for port 6200/tcp.
SSL Version 2 and 3 Protocol Detection (9.8) ***Count: 2***	NIST has determined that SSL 3.0 is no longer acceptable for secure communications. The way web browsers implement SSL/TLS creates a risk of SSL POODLE attacks and others that downgrade the connection.	Disable SSL 2.0 and 3.0, and use TLS 1.2 or higher.
Bind Shell Backdoor Detection (9.8)	A shell is listening on the remote port without any authentication required.	Verify if remote host has been compromised, and reinstall system if necessary.
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness ***Count: 3***	The remote SSH host key is easily crackable due to a bug in the random number generator of this system’s OpenSSL library. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.	Regenerate all SSH, SSL, and OpenVPN key material. Assume all cryptographic material generated on the remote host to be guessable.
Apache Tomcat AJP Connector Request Injection (Ghostcat) CVE-2020-1745 (9.8) ***Count: 2***	A file read/inclusion vulnerability was found in the AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. If the vulnerable server allows file uploads, an attacker could also upload malicious JavaServer Pages (JSP) code embedded in a variety of file types and gain remote code execution.	Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Vulnerabilidades de Gravidade Alta

Há **1** vulnerabilidade de gravidade alta.

Name/CVE/(CVSSv3.x score)	**Description**	**Solution**
rlogin Service Detection CVE-1999-0651	The rlogin service has been detected as running on the remote host. rlogin is vulnerable as it passes data between client and server in cleartext, which a man-in-the-middle attacker could exploit to sniff logins and passwords. It can also allow poorly authenticated passwordless logins.	Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Vulnerabilidades de Gravidade Média

Há **22** vulnerabilidades únicas de gravidade média. Abaixo é uma tabela mostrando algumas vulnerabilidades de gravidade média que são mais urgentes.

Name/CVE/(CVSSv3.x score)	**Description**	**Solution**
ISC BIND Service Downgrade / Reflected DoS CVE-2020-8616 (8.6)	The instance of ISC BIND 9 running on the remote name server is vulnerable to performance downgrade and Reflected DoS attacks.	Upgrade to the ISC BIND version referenced in the vendor advisory.
SSL Medium Strength Cipher Suites Supported (SWEET32) CVE-2016-2183 (7.5) ***Count: 2***	This host supports the use of SSL ciphers that offer medium-strength encryption (key lengths of 64-112 bits, or else that uses the 3DES encryption suite, by Tenable Nessus's definition.) Even medium-strength encryption can be bypassed if an attacker is on the same physical network.	Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Vulnerabilidades de Gravidade Baixa

Há **8** vulnerabilidades únicas com gravidade baixa. Abaixo é uma tabela mostrando algumas vulnerabilidades de gravidade média que são mais urgentes.

Name/CVE/(CVSSv3.x score)	**Description**	**Solution**
SSL Anonymous Cipher Suites Supported CVE-2007-1858 (5.9)	This host supports the use of anonymous SSL ciphers. These allow an admin to set up a service that encrypts traffic without having to generate and configure SSL certificates, but it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.	Reconfigure the affected application if possible to avoid use of weak ciphers.
SSH Server CBC Mode Ciphers Enabled CVE-2008-5161 (3.7)	The SSH server is configured to support Cipher Block Chaining (CBC) encryption, which may allow an attacker to recover the plaintext message from the ciphertext. *(This only checks for the options of the SSH server and does not check for vulnerable software versions.)*	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Recomendações

Esta varredura de vulnerabilidades, como em todas varreduras deste tipo, é apenas um instrumento para avaliar a postura de segurança de uma rede ou host, e estes resultados devem não ser interpretados como uma avaliação definitiva da postura de segurança da Host. Para avaliar mais a postura de segurança da Fake Inc., se requer outros passos como revisto da política, revisto dos controles e procedimentos internos de segurança, e *red-team/penetration testing*.

Remediação

O seguinte é uma lista não completa das remediações mais urgentes que são recomendadas para resolver as vulnerabilidades mais críticas:

Action	Addresses: (CVE#)
Replace unsupported Ubuntu 8.04.x with a supported version (14.04+ or latest release).	n/a
Upgrade vsftpd to a secure version.	CVE-2011-2523
Upgrade Apache Tomcat to version 9.0.31+, and secure AJP connector.	CVE-2020-1745
Regenerate all SSH, SSL, and OpenVPN keys.	n/a
Disable SSL 2.0 and 3.0, and use TLS 1.2 or higher.	n/a
Secure the VNC service with a stronger password (change from “password”.)	n/a
Disable rlogin and replace with SSH.	CVE-1999-0651
Disable anonymous and medium-strength SSL ciphers.	CVE-2007-1858, CVE-2016-2183
Disable CBC mode ciphers in SSH, and replace with CTR or GCM mode ciphers.	CVE-2008-5161