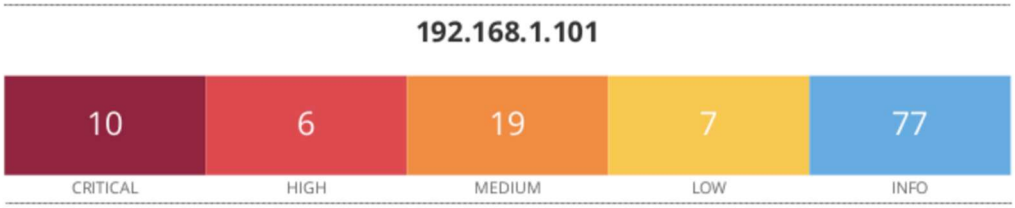
REPORT VULNERABILITÀ METASPLOITABLE

L'esercizio chiedeva di eseguire una scansione Nessus di base sulla macchina metasploitable.

Ne sono risultate diverse vulnerabilità, a partire dal livello critico fino a scendere di rischio.

Allego uno screen di una pagina del report (di circa 9 pagine totali).



Vulnerabilities Total: 119

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

LE PRIME QUATTRO VULNERABILITÀ CRITICHE

1 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Riscontrata vulnerabilità nel connettore AJP (protocollo di comunicazione tra un server web e un server di applicazioni). Un black hat o una persona non autorizzata potrebbe trovare e leggere dei

file di applicazioni web da un server vulnerabile. Inoltre, nel caso che il server vulnerabile permettesse l'upload di file, l'attaccante potrebbe nascondere tra i file un codice malevolo JSP(java server pages) che gli permetta di acquisire il controllo remoto.

SOLUZIONE

La soluzione proposta da Nessus è quella di aggiornare la configurazione AJP in modo che esso chieda l'autorizzazione all'accesso, è anche consigliato di aggiornare il Tomcat server (ha la funzione di ospitare molte applicazioni web basate su java) alle versioni successive.

Nessus fornisce anche dei link ufficiali per aiutare con la risoluzione

See Also
http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

2 Bind Shell Backdoor Detection

In questa vulnerabilità viene rilevata una Shell, o un'applicazione di sistema, che si trova in ascolto su una porta per accesso remoto (22 o 23 per esempio) senza che sia necessaria alcuna autentificazione. Un attaccante potrebbe usare la backdoor per inviare comandi diretti passando per la porta di remoto.

SOLUZIONE

In questo caso Nessus propone di verificare se l'Host da remoto sia stato compromesso e nel caso di reinstallare il sistema.

3 SSL Version 2 and 3 Protocol Detection

Il servizio da remoto accetta connessioni tramite SSL 2.0 e/o SSL 3.0. Queste versioni di SSL però presentano dei problemi di criptografia:

-Lo schema “padding” a cifratura CBC è vulnerabile

-Vulnerabilità del sistema di ripresa e rilocazione

L’attaccante potrebbe usare degli attacchi man in the middle sfruttando questi problemi oppure potrebbe decriptare la comunicazione tra il client e il servizio.

SSL ha la capacità di utilizzare il protocollo più aggiornato (userà le versioni più datate solo nel caso non ci sia altra possibilità) ma molti browser web implementano questa funzione in modo che sia facile per l’attaccante downgradare il protocollo ad una vecchia versione.

SOLUZIONE

Si consiglia di disabilitare i servizi e usare TLS 1.2 o superiore.

See Also
https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

4 Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Il server remoto DNS non utilizza porte causali quando fa richieste, o comunque entra in contatto, con server DNS di terze parti. Questo porta alla vulnerabilità che consiste nella possibilità, da parte del black hat, di attaccare il server DNS e modificare il traffico dati dirottandolo a sua scelta.

SOLUZIONE

Contattare il fornitore del servizio DNS per avere una patch.

See Also
https://www.cnet.com/news/massive-coordinated-dns-patch-released/
https://www.theregister.co.uk/2008/07/21/dns_flaw_speculation/