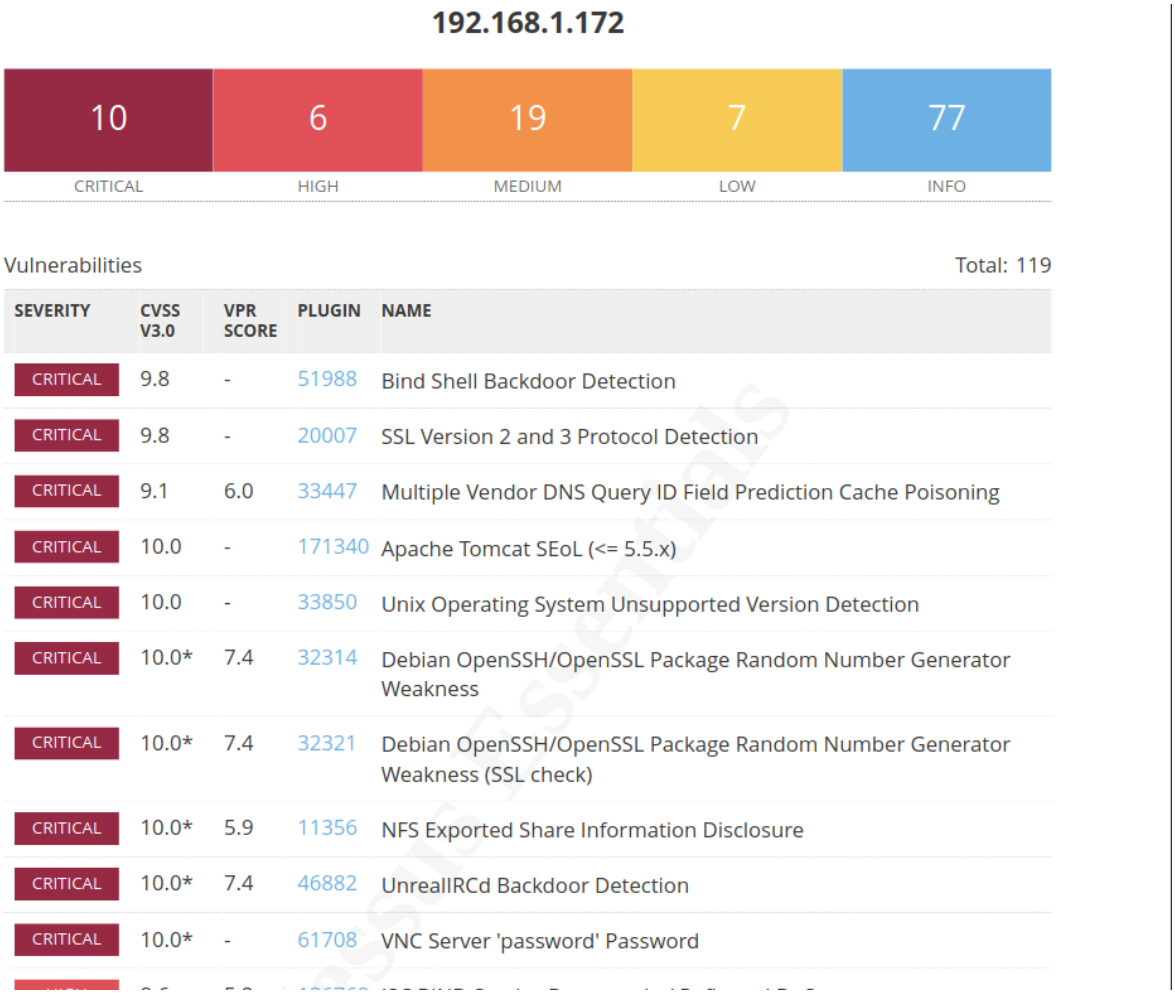
Pratica S5L4

Lo scopo dell'esercizio di oggi è eseguire un vulerability scanner usando il tool Nessus dalla macchina Kali verso la macchina Metasploitable. Dopo aver installato Nessus su Kali e avviato il servizio, sono andato a lanciare la scansione puntando al https://kali:8834. Ho eseguito la scansione su tutte le porte disponibili. Di seguito il report con le vulnerabilità maggiori riscontrate ed una breve spiegazione per le prime sei di esse:



192.168.1.172

10	6	19	7	77
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 119

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
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*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Bind Shell Backdoor detection:

Nessus ci informa che su meta una shell è in ascolto su una porta remota senza che venga richiesta un'autorizzazione. Questo è pericoloso perché un attaccante potrebbe connettersi e lanciare del codice sulla macchina senza prima autenticarsi. In questo caso la soluzione proposta da Nessus è solamente di verificare se il sistema è stato compromesso, e in caso affermativo non si può far altro che reinstallarlo.

SSL Version 2 and 3 Protocol Detection:

In questo caso la vulnerabilità è data dal fatto che Meta accetta SSL 2.0 e/o 3.0 come sistemi validi di cifratura. Questi due protocolli non sono considerati però sicuri in quanto sono stati compromessi rispettivamente nel 2011 e 2015. La soluzione in questo caso consiste nell'usare invece TLS 1.2 (o una versione più recente) per la cifratura delle connessioni e di disabilitare l'accettazione dell'SSL.

Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Il traffico DNS verso il server usato dalla macchina target non è sicuro in quanto non usa un numero

di porta sorgente casuale quando fa delle richieste DNS, inoltre queste richieste non vengono autenticate. Questo è un problema in quanto un attaccante potrebbe fingersi il Server DNS a cui la vittima sta facendo le richieste per reindirizzare il traffico a suo piacimento.

Apache Tomcat SEoL (<= 5.5.x)

Il servizio Apache Tomcat presente sulla macchina target risulta avere una versione inferiore alla 5.5.x, l'ultima supportata. Usare un software non più supportato è un rischio per la sicurezza perché eventuali vulnerabilità scoperte non vengono più risolte dal vendor tramite patch/aggiornamenti. La soluzione è quella di usare una versione supportata di Apache Tomcat.

Unix Operating System Unsupported Version Detection

La vulnerabilità è data dal fatto che la versione di Unix attualmente in uso sul sistema metasploitable non è più supportata. Non saranno disponibili quindi aggiornamenti/patch di sicurezza scaricabili dall'utente. La soluzione consiste nell'aggiornare il sistema corrente o, se non possibile, utilizzare un sistema che venga supportato dalla presenza di aggiornamenti. Ovviamente nel nostro esempio non è lo scopo inteso in quanto questa versione di linux è pensata proprio per essere un target di eventuali attacchi a fini di test.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

La vulnerabilità consiste nella debolezza delle chiavi usate per il protocollo SSH. A causa di questo, il protocollo SSH non dovrebbe essere utilizzato in quanto molto vulnerabile contro attacchi di tipo MITM, Questa vulnerabilità può essere risolta facendo l'aggiornamento del OpenSSH, una guida è disponibile all'indirizzo https://www.debian.org/security/key-rollover/