Esercizio 4 Settimana 5

Report Nessus

Dopo aver visto NMAP per la scansione di rete, oggi andiamo a vedere le funzionalità di NESSUS come Vulnerability Scanner. Esso è uno strumento per trovare le vulnerabilità di un determinato target; NESSUS identifica le vulnerabilità andandole a confrontare con un database sempre aggiornato e classificandole in base al livello di rischio (critical, high, medium, low e info). Attraverso il software possiamo anche andare ad eseguire degli attacchi veri e proprio di test come la BRUTE FORCE.

Andiamo ora a sviscerare le prime 4 riportate nel report consultabile tramite link https://github.com/Eindr/report-nessus/blob/main/meta_6vrd44.pdf :

1. Apache Tomcat A JP Connector Request Injection (Ghostcat): con questo tipo di criticità è possibile essere attaccati da remoto per leggere file da un web application server vulnerabile così da permettere il caricamento di file malevoli e il controllo di esecuzioni da remoto.
   Una possibile soluzione può essere quella di aggiornare le configurazioni e di aggiungere un fattore di autenticazione. È inoltre consigliabile configurare il server Tomcat per registrare attività sospette o tentativi di attacco.

   È possibile consultare i seguenti link in merito:
   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: è sintomo della creazione di una BACKDOOR che crea un canale di comunicazione tra un sistema remoto e uno compromesso. In questo caso bisogna agire immediatamente effettuando un'analisi e un monitoraggio generale della macchina (porte, file di sistema, account utente, traffico di rete etc..). Una volta individuata si può cercare di eliminarla andando ad arrestare/eliminare programmi dannosi e file malevoli. A volte può comportare la reinstallazione del sistema.

3. SSL Version 2 and 3 Protocol Detection: le version SSL 2 e 3 sono protocolli obsoleti di sicurezza che presentano molte vulnerabilità (POODLE e BEAST). Un attaccante può eseguire una tecnica MAN-IN-THE-MIDDLE per cercare di intercettare pacchetti e comunicazioni sensibili. Bisogna quindi andare a

disattivare tali protocolli e usarne uno di tipo TLS per avere più sicurezza alle comunicazioni tra client e server. È inoltre pratica comune scansionare la rete ed esaminare i file di Log.
È possibile consultare i seguenti link in merito:
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. Apache Tomcat SEoL (<= 5.5.x): questa vulnerabilità indica che la versione del software uguale o inferiore a quella citata non viene più supportata dal provider e che gli aggiornamenti non saranno più disponibili. Le nuove patch e plug-in non saranno installati e questo rende la sicurezza a rischio. L'unica soluzione è quella di installare un nuovo software aggiornato tramite canali ufficiali di provider certificati. Biosgna inoltre restare sempre aggiornati sulle novità e sulle nuove versioni.
   Link utile:
   https://tomcat.apache.org/tomcat-55-eol.html