## VANCOUVER

Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Bsides Vancouver 2018 è una macchina progettata per creare un ambiente sicuro in cui è possibile eseguire Pen Test reali su un obbiettivo vulnerabile. La VM è configurata con un’interfaccia di rete NAT Network, cioè che può comunicare con altre VM nella stessa rete NAT, nonché con Internet. Ciò consente di simulare scenari realistici di Pen Test, in cui è possibile testare la sicurezza della VM bersaglio dall’interno della rete.

Le macchine da Oracle VM VirtualBox sono impostate su una scheda di rete solo host, Kali ha come configurazione un IP in dhcp, e non statico.

Con il comando sudo arp-scan --localnet eseguo una scansione della rete, analizzando gli indirizzi IP sulla mia rete locale, arp-scan utilizza il protocollo ARP (Address Resolution Protocol). --localnet è uno switch del comando che limita la scansione degli indirizzi IP all’interno della mia subnet.   
Immaginiamo la rete locale come un quartiere, in cui ogni dispositivo ha un indirizzo IP unico come un numero di casa e un indirizzo MAC unico come un numero di porta. Quando un dispositivo nella rete desidera comunicare con un altro dispositivo sa l’indirizzo IP del destinatario ma deve prima scoprire il suo indirizzo MAC per inviare effettivamente i dati. Il dispositivo A nella reta ha l’indirizzo IP del dispositivo B a cui vuole mandare i dati ma non conosce il suo indirizzo MAC. Il dispositivo A invia un messaggio ARP broadcast ( un messaggio a tutti i dispositivi nella rete) chiedendo: “chi ha l’indirizzo IP X?”. Tutti i dispositivi nella rete ricevono questo messaggio ARP, ma solo il dispositivo B con l’indirizzo IP corrispondente risponde direttamente ad A con il proprio indirizzo MAC. Il dispositivo A ora conosce l’indirizzo MAC di B e può inviare dati direttamente a B sulla rete locale. Tutta via, alcune reti o dispostivi potrebbero non rispondere a queste richieste, quindi non si potrebbe avere una lista completa.

Il comando sudo netdiscover -r 192.168.56.0/24 è utilizzato per rilevare e scoprire i dispositivi sulla rete locale, - r è un parametro che specifica un intervallo di indirizzi IP da esaminare, in modo da limitare la ricerca solo a quella gamma, invece di cercare in tutta la rete.  
Questo comando invia pacchetti ARP a tutti gli indirizzi all’interno dell’intervallo scelto. Gli ARP sono utilizzati per associare gli indirizzi IP agli indirizzi MAC sui dispositivi di rete. In pratica il comando sta cercando di ottenere una risposta dai dispositivi nella rete per identificare quali indirizzi IP sono utilizzati e quali dispositivi li possiedono. Quando un dispositivo nella rete riceve una richiesta ARP per il suo indirizzo IP, risponderà con un pacchetto ARP contenente il suo indirizzo MAC. Queste risposte vengono registrate da netdiscover e utilizzate per identificare i dispositivi.

Entrambi i comandi, sudo arp-scan --localnet e sudo netdiscover -r, sono strumenti di scansione della rete per rilevare i dispositivi nella mia rete locale, ma utilizzano approcci leggermente diversi per farlo.  
In breve, la principale differenza è che il primo invia richiesta ARP broadcast per cercare di ottenere informazioni, mentre il secondo invia pacchetti ARP diretti a tutti gli indirizzi IP nella gamma specificata (è una scansione più invasiva ma più completa). Una richiesta ARP broadcast è una richiesta inviata a tutti i dispositivi nella rete per ottenere una risposta, mentre un pacchetto ARP include richieste ARP e risposte ARP.

Ho fatto questa distinzione in quanto ho avuto problemi nello svolgimento.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Scansione non invasiva di Nmap

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

-sS esegue una scansione SYN, non invasiva in quanto non completa l’handshake TCP  
-sV rileva le versioni dei servizi in esecuzione sulle porte aperte  
-Pn ignora il Ping, cioè non tenta di determinare se l ’host è online prima di eseguire la scansione delle porte  
-p- scansiona tutte le porte da 1 a 65535

Dalla scansione trovo delle informazioni:

1. Indirizzo IP macchina 192.168.56.102
2. 65532 Porte chiuse, il sistema ha provato a stabilire una connessione con queste porte, ricevendo una risposta di reset, vuol dire che la porta è chiusa e il sistema remoto ha respinto la connessione.
3. Le porte aperte sono tre:
   * Porta 21/tcp servizio FTP versione vsftpd 2.3.5
   * Porta 22/tcp servizio SSH versione OpenSSH 5.9p1
   * Porta 80/tcp servizio HTTP versione Apache 2.2.22
4. Mac Address 08:00:27:1C:B2:33

TCP sta per “Transfer Control Protocol” ed è uno dei principali protocolli di comunicazione utilizzati nella trasmissione di dati su reti informatiche, inclusa Internet; l’altro è UDP (User Datagram Protocol).  
TCP è affidabile nella consegna dei dati, crea una connessione tra i due dispositivi (mittente e destinatario) attraverso il processo “handshake”, garantendo che i dati vengano consegnati correttamente e in ordine.

Scansione aggressiva di Nmap

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

-sC esegue uno script di default, che includono controlli di sicurezza comuni e individuare le vulnerabilità  
-sV rilevazione delle versioni dei servizi in esecuzione sulle porte aperte  
-A scansione dei servizi e di identificazione del sistema operativo e raccoglie informazioni sui servizi in esecuzione  
-p- scansiona tutte le porte   
-T4 imposta la velocità di scansione “aggressiva”  
--open visualizza solo le porte aperte

Dalla scansione ho ottenuto delle informazioni:

1. L’indirizzo IP della macchina target è 192.168.56.102
2. Ci sono tre porte aperte:
   * Porta 21 (FTP) è in esecuzione un server vsftpd 2.3.5. Leggo che, il login FTP anonimo è consentito, inoltre all’interno cè una cartella drwx-xr-x public, dove, “d indica che è una directory cioè una cartella, “rwx” sono i permessi del proprietario del file, di lettura (read) scrittura (write) e esecuzione (execute), “xr” sono i permessi degli utenti del gruppo, mentre “x” i permessi degli altri utenti.  
     Si potrebbe entrare come anonymous e aprire la cartella.   
     FTP sta per File Transfer Protocol ed è un protocollo utilizzato per trasferire file da un computer a un altro attraverso una rete, come Internet o una rete locale. La porta 21 è generalmente associata al servizio FTP. Quando la porta è aperta è possibile utilizzare un client FTP per connettersi a quella macchina e trasferire file avanti e indietro. Inoltre, è consentito il login FTP anonimo, quindi non è necessario fornire un nome utente o password per accedere al server FTP.  
     Il server FTP è una versione vsftpd 2.3.5
   * Porta 22 (SSH) è in esecuzione un server OpenSSH 5.9p1 su Ubuntu Linux.  
     SSH sta per Secure Shell è un protocollo crittografico generalmente associato alla porta 22. Consente di accedere in modo sicuro a un computer sulla rete, ed è utilizzato per controllare un computer da remoto.  
     Server OpenSSH versione 5.9p1.

Informazioni sulle chiavi di crittografia utilizzate del server SSH: DSA, RSA,ECDSA

* + Porta 80 (http) è in esecuzione un server Apache httpd 2.2.22 su Ubuntu. All’interno di questa porta vedo che c’è un file robots.txt, ma l’entrata è disabilitata, inoltre cè un backup\_wordpress.  
    La porta 80 è associata al protocollo HTTP, utilizzato per la navigazione sui siti web, è in esecuzione su un server Apache httpd 2.2.22.

1. Il sistema operativo della macchina target esegue una distribuzione Linux con kernel 3.X o 4.X
2. Informazioni sulla rete: la distanza di rete è 1 hop, la macchina target è direttamente raggiungibile sulla stessa subnet.
3. L’indirizzo MAC della macchina target è 08:00:27:1C:B2:33, che è associato a una scheda di rete virtuale Oracle VirtualBox.

## Svolgimento

Mi connetto alla porta 21 scrivendo ftp 192.168.56.102, dove mi verrà richiesto solo l’ID in quanto anonymous.

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

All’interno cerco la cartella public, spostandomi e visualizzando con i comandi cd e ls -l. Prendo il file trovato con il comando get users.txt.bk

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Esco dal server ftp e digito il comando cat user.txt.bk per visualizzare il documento. Dato che il documento si chiama user, presumo che i nomi trovati all’interno siano i nomi utenti, trovandone 5.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Avendo la porta SSH aperta, una porta che permette di connettersi da remoto, faccio dei tentatavi di accesso. Quattro di questi, mi negano i permessi, mentre l’utente anne è l’unico che mi chiede la password.  
Nella porta 80, abilitata per i servizi web, c’è una pagina chiamata backup\_wordpress, dal nome deduco che possa aiutarmi a trovare le password utenti. Utilizzo la versione grafica di Hydra, aprendolo con il comando xhydra, e imposto l’interfaccia. Nel Target inserisco l’IP della macchina in single target, come protocollo uso ftp, spunto Be Verbose (registra le azioni svolte) e Show Attempts (registra i tentativi fatti). Nella finestra Password imposto l’username anne e come password list carico rockyou.txt, che è una libreria per decriptare. Nella finestra Specific specifico l’indirizzo url. Avvio il programma.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamenteImmagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

xHydra non mi ha dato una password valida, però me ne ha tirate fuori 16. A tentativi, partendo dalla prima password “123456” ho provato il login sull’ID anne, quella funzionante è “princess”.

Immagine che contiene testo, schermata, software, Carattere

Descrizione generata automaticamente

Una volta effettuato l’accesso nell’account di anne, per diventare root bisogna eseguire il comando sudo su, “sudo” è un comando che esegue comandi con privilegi di amministratore o superutente, “su” è un’abbreviazione di “switch user” (cambia utente) e viene utilizzato per effettuare l’accesso come un altro utente. Combinando questi due comandi si chiede di passare alla shell dell’utente root. Reinserisco la password di anne, già soltanto così si può vedere che sono all’interno della macchina come utente root, per conferma utilizzo il comando whoami, che  
restituisce il nome dell’utente che ha avviato la shell corrente. Con il profilo root cerco eventuali directory con i comandi ls -l e cd, trovo la flag.txt, la rubo con get e la visualizzo con cat.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Ci sono altri modi per ottenere i permessi da root.

Ho ottenuto i nomi utenti, so che le password sono all’interno di backup\_wordpress, quindi utilizzo il tool WPScan, che non è altro che una scansione di WordPress (un popolare sistema di gestione dei contenuti (CMS) utilizzato per creare e gestire siti web), che consente di identificare e valutare le vulnerabilità potenziali presenti in un sito web WordPress.  
Ho utilizzato il comando wpscan –url <http://192.168.56.102/backup_wordpress/> --enumerate per fare una scansione del sito.

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Scansionando il sito ho trovato:

Un url, funzionante.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, Software multimediale, software, schermata

Descrizione generata automaticamente

E due possibili account

Immagine che contiene testo, Carattere, schermata

Descrizione generata automaticamente

Per trovare la password di john avviato wpscan –url http://192.168.56.102/backup\_wordpress --username john –password /usr/share/wordlist/rockyou.txt

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Immagine che contiene testo, software, Icona del computer, Software multimediale

Descrizione generata automaticamente

Immagine che contiene testo, Carattere, schermata, design

Descrizione generata automaticamente



Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software

Descrizione generata automaticamente

Immagine che contiene testo, Carattere, software, schermata

Descrizione generata automaticamente