Tutorial:

Trovare falle per la sicurezza nella rete con nmap

Sul tema dell'isolamento
Ai firewall

Dietro ogni porta aperta nella rete si nasconde un programma server che contiene con grande probabilità errori. Fra questi vi sono errori così gravi da poter essere sfruttati, per spiare o sabotare il rispettivo sistema o persino per eseguire codici nocivi. Per questo motivo il passo più importante per ottenere una maggiore sicurezza nella vostra rete aziendale è controllare le porte aperte e, ove necessario, chiuderle.

Istruzioni: Esplorare la rete con nmap

Con l'aiuto di programmi di analisi della rete l'utente può farsi una panoramica sui possibili punti deboli nella sua rete aziendale. Queste istruzioni presentano tre tecniche analitiche basilari con il port scanner nmap. Servono a identificare terminali e a scoprire che servizi offrono. Infine presentiamo due tecniche con le quali è possibile garantire i punti deboli riscontrati.

Con il programma **nmap** è possibile esaminare la struttura della propria rete. Questo strumento viene considerato il "tool degli hacker" per eccellenza, perché utilizza anche dettagli di implementazione da vari protocolli di rete. Trova terminali nella rete, li analizza in base a programmi server e rileva di che programmi si tratta. In questo modo nmap vi rivela numerosi dettagli sulla vostra rete aziendale.

Nota:
Lavorate sempre in modo accurato e analizzate solo reti per le quali siete autorizzati a svolgere analisi!

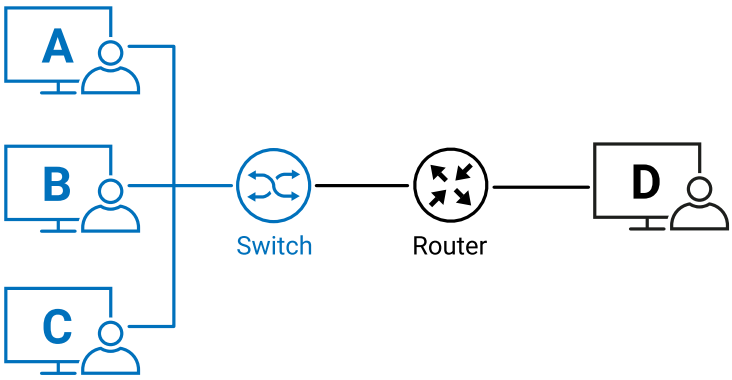
Installare e utilizzare Nmap

Potete scaricare il programma al sito nmap.org. Mentre nmap stesso è un programma di righe di comando, con Zenmap l'utente dispone di un'interfaccia utente grafica.

Per alcune delle tecniche descritte di seguito nmap invia pacchetti di dati grezzi mediante diversi strati nella rete. Dal momento che deve aggirare lo stack di rete del sistema operativo, per l'esecuzione avete bisogno di diritti root e di amministratore.

Tecnica di analisi 1:
Trovare terminali nella rete con nmap

Con l'aiuto della prima tecnica tutti i terminali vengono trovati nello stesso dominio broadcast. Ciò significa p. es. che tutti i computer sono collegati fra loro nella stessa ethernet mediante interruttori e non sono separati fra loro tramite router (quindi a livello IP). È vero che si potrebbe in alternativa inviare una richiesta echo ICMP (ping) all'indirizzo di trasmissione del segmento di rete, ma per motivi di sicurezza i nuovi terminali in genere non vi rispondono.



Il computer A, B e C sono collegati tra loro mediante un interruttore e si trovano dunque nello stesso dominio di broadcast. Il computer A è in grado di trovare il computer B e C con l'aiuto di interrogazioni ARP nella rete. Il computer D è collegato alla rete tramite router. Tuttavia non viene raggiunto dalle interrogazioni ARP.

Se si desidera inviare un pacchetto IP ad un altro computer nella stessa Ethernet, è possibile farlo tramite un frame Ethernet, che viene sostituito tra due interfacce di rete. Per far questo è necessario essere a conoscenza dell'indirizzo dell'hardware del destinatario. Il meccanismo che assegna il relativo indirizzo hardware o MAC ad un indirizzo IP, È messo a disposizione dall'Adress Resolution Protocol (ARP).

Mediante l'indirizzo MAC broadcast nella rete, a tutti i terminali nel dominio broadcast viene inviata la domanda: "Chi ha il seguente indirizzo IP?" Il terminale che riceve i pacchetti per questo indirizzo IP, riinvia il suo indirizzo MAC. Adesso l'interfaccia di rete può indirizzare dati esattamente a questo partecipante.

Durante l'inventarizzazione di un segmento di rete con impiego di ARP viene effettuata questa domanda per ogni singolo indirizzo IP nel segmento di rete indicato. Se un apparecchio è integrato nella rete, deve obbligatoriamente rispondere a questa interrogazione.

Il seguente comando trova tutti gli apparecchi funzionanti con gli indirizzi IP da 192.168.1.1 a 192.168.1.254 in un dominio broadcast comune:

```
nmap -PR 192.168.1.0/24
```

Tecnica di analisi 2:
Trovare porte aperte senza accesso diretto all'apparecchio

Se avete accesso diretto al sistema di destinazione, potete visualizzare porte aperte in Linux, MacOS e Windows tramite il comando "netstat". In molti casi però non è possibile. Per questi casi nmap offre alternative per cercare porte aperte nel sistema di destinazione.

Trovare porte TCP aperte

Dietro ad ogni porta aperta è attivo un programma server che riceve i dati e li valuta. In TCP l'identificazione di porte aperte è semplice. Dato che il protocolla funziona in modo orientato al collegamento, Occorre introdurre solo l'handshake a tre vie per stabilire una connessione (trovate ulteriori informazioni sull'handshake a tre vie nel nostro libro gratuito "TCP/IP Ethernet fino a Web-IO"). A tal scopo viene inviato un semplice pacchetto SYN alla destinazione. A seconda della risposta ottenuta, è possibile rilevare lo stato della porta:

- **Nessuna risposta:**
  La porta non è aperta oppure è filtrata
- **Reset:**
  Il sistema operativo riceve domande di collegamento per la porta, ma le respinge perché perché sulla porta non è attiva nessuna applicazione del server.
- **Viene accettata la connessione:**
  La porta è aperta e rappresenta in alcune situazioni un rischio alla sicurezza.

Con il seguente comando eseguite una scansione TCP-SYN sull'host con l'indirizzo IP 192.168.1.200:

```
nmap -sS 192.168.1.200
```

Trovare porte UDP aperte

Trovare porte UDP aperte è notevolmente più difficile. Contrariamente a TCP UDP funziona non orientato alla connessione. Poichè non è presente nessun handshake a tre vie, la reazione dell'altra parte non è prevedibile.

Nel caso più semplice, il sistema operativo del sistema di destinazione risponde che la porta non è raggiungibile. In questo caso viene contrassegnato come chiuso. Se non viene inviata nessuna risposta, non è possibile dire se il pacchetto è stato accettato da un'applicazione server o è stato respinto sulla strada. Nessuna risposta significa di conseguenza che la porta è aperta o è filtrata.

Il sistema invia un pacchetto specifico di servizio ai "soliti sospetti" fra le porte. Se il mittente riceve una risposta, sa che la porta è aperta. Ciò funziona ad esempio alla risoluzione di normi di computer tramite DNS, alla domanda di configurazione IP tramite via DHCP o agli aggiornamenti temporali via NTP.

Con questo comando si esegue una semplice scansione UDP:

```
nmap -sU 1 192.168.1.200
```

Come accennato sopra questa scansione non trova sempre tutte le porte UDP aperte - per una prima panoramica però spesso è sufficiente.

Trovare porte TCP e UDP nello stesso processo

Per rilevare contemporaneamente porte TCP e UDP, potete anche combinare fra loro i comandi.

```
nmap -sS -sU 192.168.1.200
```

Tecnica di analisi 3:
Determinare sistema operativo e programmi del server

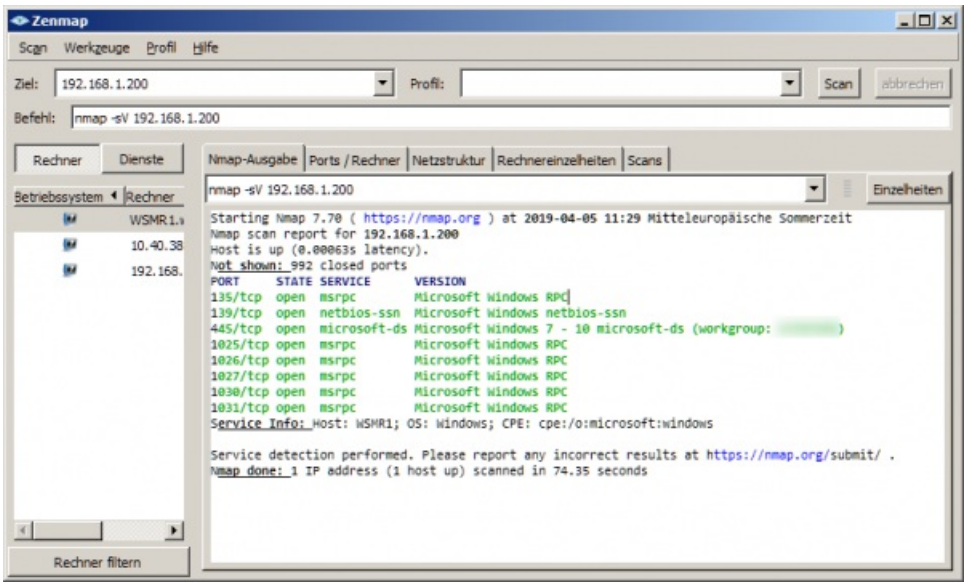
Nmap sa fare di più che non solo trovare terminali e porte: Nell'implementazione di protocolli di rete gli sviluppatori godono di determinate libertà. Questo comporta che ogni sistema operativo presenti un'impronta digitale specifica mediante la quale può essere identificato.

Non sempre è possibile determinare il sistema operativo Nella maggior parte dei casi, tuttavia, il risultato è coerente.

```
nmap -0 192.168.1.200
```

Per scoprire quali servizi sono in funzione in un terminale, nmap può analizzare le risposte delle porte aperte. Spesso questi programmi comunicano autonomamente un gran numero di informazioni, per esempio a che livello della versione si trovano o quali protocolli supportano. Nmap valuta queste informazioni e le riassume.

```
nmap -Sv 192.168.1.200
```



Tenete presente che: Se utilizzate sV insieme a sU, ovvero la scansione UDP, nmap Bainvia una batteria di test completi ad ogni singola porta UDP. Ciò vi può fornire ulteriori informazioni sulle porte UDP aperte, però può durare molto!

Chiudere le porte, aumentare la sicurezza

Dopo che ora sono noti gli eventuali rischi legati a porte aperte, nel prossimo passo si intende ridurli al minimo.

Tecnica di sicurezza 1:
Terminare applicazioni del server

Nel primo passo dovete disattivare tutte le applicazioni del server non necessarie. Per scoprire quale applicazione apre una porta, potete anche utilizzare il comando "netstat". In molti casi non è possibile terminare le applicazioni del server sul terminale per chiudere le porte, per esempio in caso di assenza di diritti d'accesso, in caso di software incorporato o quando le applicazioni del server vengono avviate in maniera dinamica all'occorrenza. In questo caso viene in aiuto la tecnica di isolamento descritta nel prossimo capitolo.

Tecnica di sicurezza 2:
Semplice ed efficace - l'isolamento con Microwall

In caso di impiego della tecnica di isolamento i sistemi potenzialmente a rischio, nei quali non è possibile chiudere le porte aperte, vengono isolati in un apposito segmento della rete. La comunicazione con questo segmento viene controllata, limitata e protocollata. Inoltre viene installato un router firewall come il W&T Microwall tra i sistemi interessati e la rete circostante. Il traffico dati IP trasmesso attraverso questo router viene filtrato in base a regole.

- Il filtro pacchetto del Microwall seleziona la comunicazione indesiderata e rigetta pacchetti. Persino se una porta del terminale è aperta, non può essere raggiunto.
- Nella modalità NAT vengono nascosti tutti i terminali sull'isola dietro al Microwall. Nella rete è visibile solo Microwall che inoltra e monitora la comunicazione.
- I terminali isolati si trovano in un altro dominio broadcast. Una domanda ARP e altri attacchi a livello di rete vengono soppressi efficacemente.

Trovate informazioni dettagliate sulla strategia di isolamento sulla Pagina tematica.

Potete contattare telefonicamente i nostri tecnici al numero +49 202/2680-110 (Lun-Ven. 8-17)

W&T
www.WuT.de

Saremo lieti di fornirvi una consulenza personalizzata!

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel.: +49 202/2680-110 (Lun-Ven. 8-17)
Fax: +49 202/2680-265
info@wut.de