Report di Analisi della Cattura di Rete

Introduzione

Durante l'esercitazione pratica di oggi, ho analizzato una cattura di rete effettuata con Wireshark per identificare eventuali Indicatori di Compromissione (IOC) e formulare ipotesi sui potenziali vettori di attacco. Di seguito, descrivo in dettaglio i passaggi seguiti e le osservazioni fatte.

Configurazione della Macchina Virtuale e Trasferimento del File

1. **Creazione di una Cartella Condivisa**:
    - Ho aperto VirtualBox e selezionato la VM Kali Linux.
    - Ho navigato in Impostazioni -> Cartelle condivise e aggiunto una nuova cartella condivisa con il percorso specificato sul mio host. Ho nominato la cartella Cartella_condivisa e ho spuntato le opzioni Montaggio automatico e Rendi permanente.
2. **Avvio della VM e Accesso alla Cartella Condivisa**:
    - Ho avviato Kali Linux e aperto il terminale.
    - Ho montato la cartella condivisa:

```
sudo mount -t vboxsf Cartella_condivisa /media/cartella_condivisa
```

    - Ho verificato la presenza del file nella cartella condivisa:

```
ls /media/cartella_condivisa
```

3. **Copia del File sul Desktop di Kali**:
    - Ho copiato il file .pcapng dal percorso condiviso al desktop di Kali:

```
cp -r /media/cartella_condivisa/Cattura_U3_W1_L3 ~/Desktop/
```

4. **Verifica del Contenuto e Apertura del File**:
    - Ho verificato il contenuto della directory copiata:

```
ls ~/Desktop/Cattura_U3_W1_L3
```

    - Ho aperto il file Cattura_U3_W1_L3.pcapng con Wireshark.

Analisi della Cattura con Wireshark

1. **Apertura del File con Wireshark**:
    - Ho fatto doppio clic sul file Cattura_U3_W1_L3.pcapng sul desktop per aprirlo con Wireshark.
2. **Filtri di Base in Wireshark**:
    - Una volta aperto il file in Wireshark, ho utilizzato i seguenti filtri per iniziare l'analisi delle comunicazioni sospette:

```
ip.addr == 192.168.200.150  # IP target

ip.addr == 192.168.200.100  # IP sospetto

tcp.flags.syn == 1 && tcp.flags.ack == 0  # Pacchetti SYN

tcp.flags.rst == 1  # Pacchetti RST
```

3. **Identificazione degli Indicatori di Compromissione (IOC)**:
    - **Richieste SYN Ripetute**:
        - Ho filtrato i pacchetti SYN inviati dall'attaccante (192.168.200.100) al target (192.168.200.150):

```
ip.src == 192.168.200.100 && ip.dst == 192.168.200.150 && tcp.flags.syn == 1 && tcp.flags.ack == 0
```

        - Ho osservato molte richieste SYN verso porte diverse, indicando una scansione delle porte.
    - **Risposte RST/ACK**:
        - Ho filtrato i pacchetti RST/ACK inviati dal target all'attaccante:

```
ip.src == 192.168.200.150 && ip.dst == 192.168.200.100 && tcp.flags.rst == 1 && tcp.flags.ack == 1
```

        - Un numero elevato di risposte RST indica che molte porte sono chiuse e l'attaccante sta eseguendo una scansione delle porte.

Formulazione delle Ipotesi sui Vettori di Attacco

Dall'analisi della cattura, le richieste SYN ripetute su porte diverse suggeriscono che è in corso una scansione delle porte da parte dell'host 192.168.200.100 verso il target 192.168.200.150. Questa ipotesi è supportata dal fatto che per alcune richieste si ricevono risposte SYN/ACK (porte aperte) e per altre risposte RST (porte chiuse). Questo comportamento è tipico di una scansione delle porte eseguita per identificare i servizi in ascolto sul target.

Raccomandazioni per Ridurre gli Impatti dell'Attacco

- **Configurazione del Firewall**:
    - Ho configurato il firewall per bloccare l'IP dell'attaccante:

```
sudo iptables -A INPUT -s 192.168.200.100 -j DROP
```

    - Ho bloccato tutte le porte non necessarie per prevenire la scoperta dei servizi in ascolto:

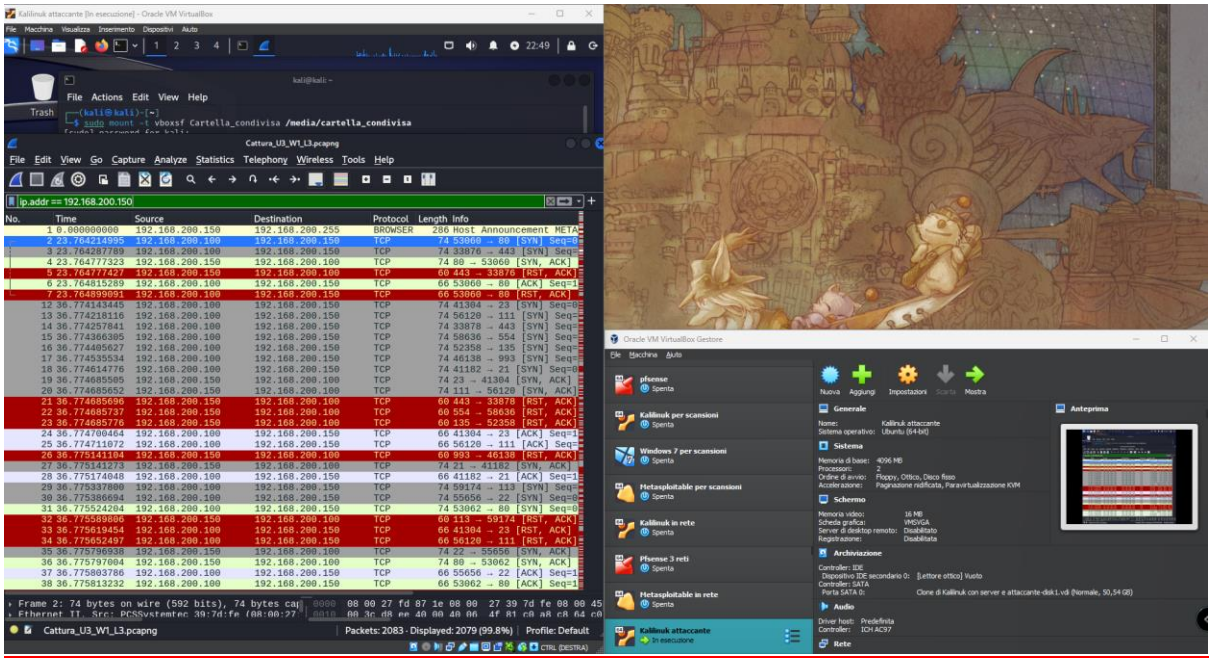
```
sudo iptables -P INPUT DROP
```

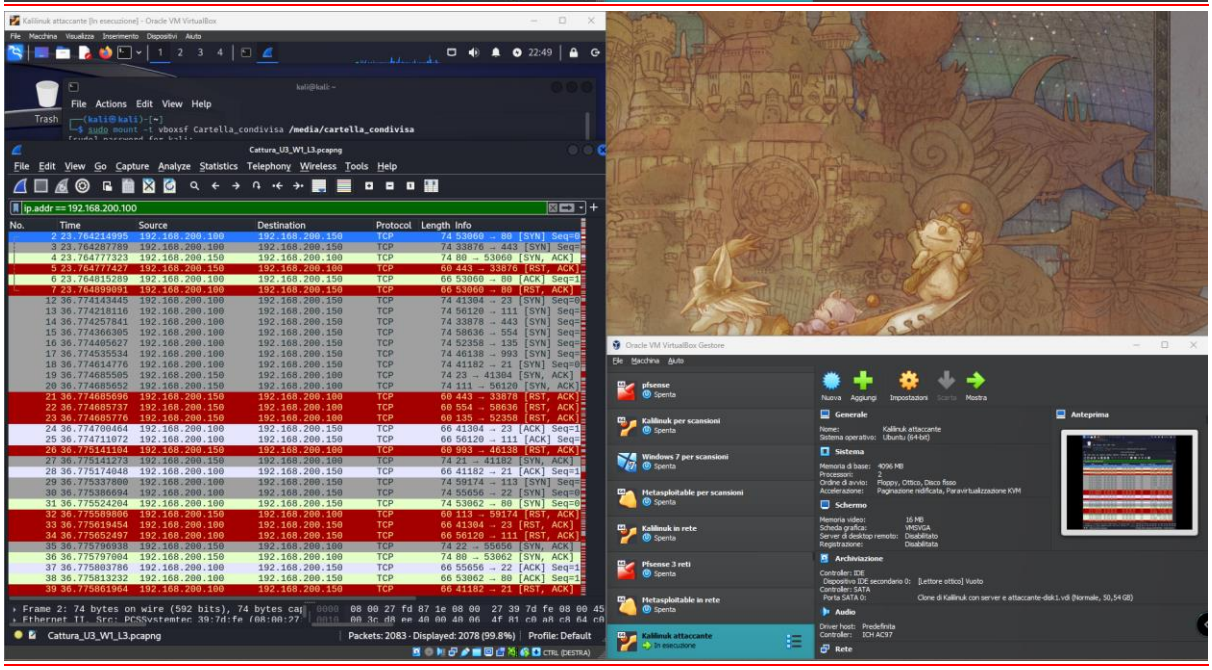
```
sudo iptables -A INPUT -p tcp --dport [porta] -j ACCEPT  # Aggiungi regole per le porte necessarie
```

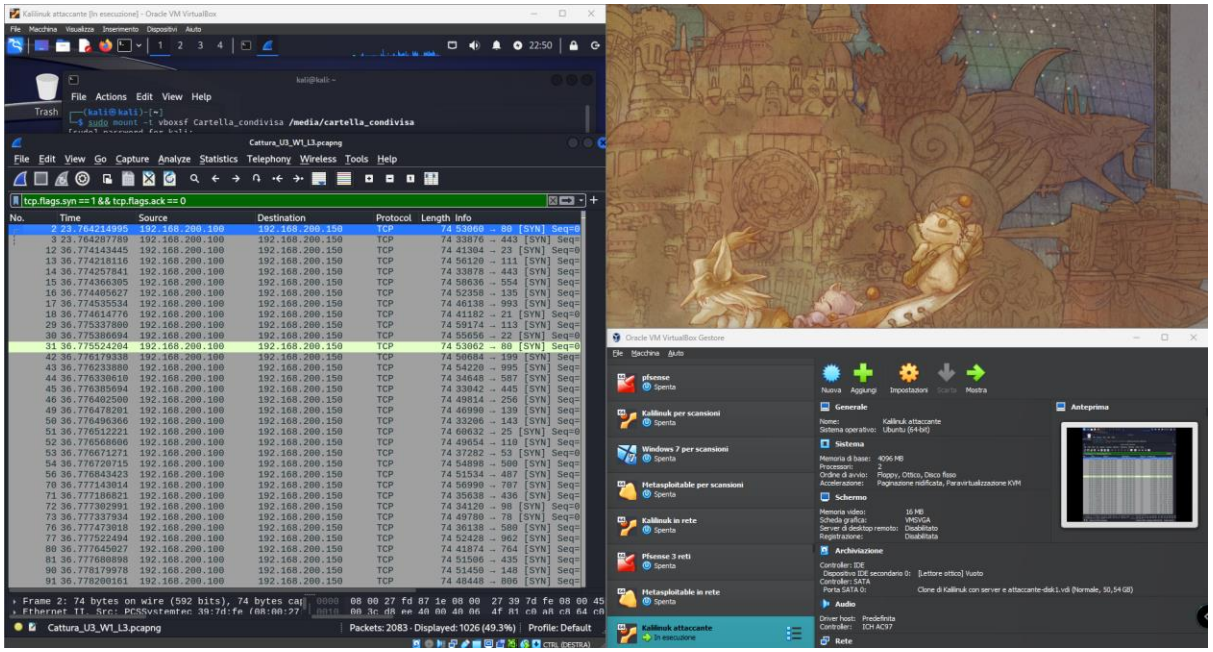
Conclusione

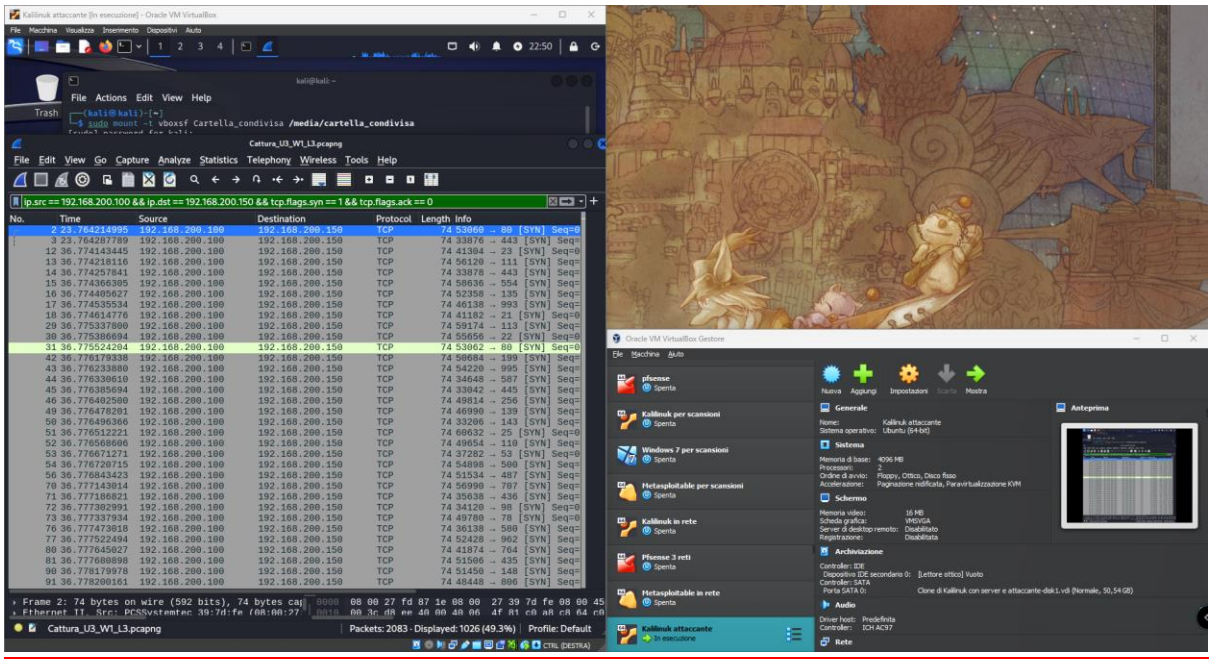
L'analisi della cattura di rete ha rivelato un numero elevato di richieste TCP (SYN) su porte diverse, suggerendo una scansione delle porte in corso da parte dell'host 192.168.200.100 verso il target 192.168.200.150. Ho implementato regole firewall per bloccare l'attaccante e mitigare l'impatto dell'attacco. Le misure preventive possono includere il monitoraggio continuo del traffico di rete e l'implementazione di strumenti IDS/IPS per rilevare e rispondere rapidamente a potenziali minacce.

Screenshot


File Actions Edit View Help
sudo mount -t vboxsf Cartella_condivisa /media/cartella_condivisa
Cattura_U3_W1_L3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.200.150
No. Time Source Destination Protocol Length Info
Frame 2: 74 bytes on wire (592 bits), 74 bytes cap
Ethernet II, Src: PCSSystemtec 39:7d:fe (08:00:27
Cattura_U3_W1_L3.pcapng
Packets: 2083 · Displayed: 2079 (99.8%)
Profile: Default
Oracle VM VirtualBox Gestore
File Macchina Aiuto
pfsense
Kalilinuk per scansioni
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Rete
Anteprima


File Actions Edit View Help
sudo mount -t vboxsf Cartella_condivisa /media/cartella_condivisa
Cattura_U3_W1_L3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.200.100
No. Time Source Destination Protocol Length Info
Frame 2: 74 bytes on wire (592 bits), 74 bytes cap
Ethernet II, Src: PCSSystemtec 39:7d:fe (08:00:27
Cattura_U3_W1_L3.pcapng
Packets: 2083 · Displayed: 2078 (99.8%)
Profile: Default
Oracle VM VirtualBox Gestore
File Macchina Aiuto
pfsense
Kalilinuk per scansioni
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Sistema
Schermo
Archiviazione
Audio
Rete
Anteprima


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo mount -t vboxsf Cartella_condivisa /media/cartella_condivisa
Cattura_U3_W1_L3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.syn == 1 && tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 → 80 [SYN] Seq=0
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 → 443 [SYN] Seq=
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 → 23 [SYN] Seq=0
13 36.774218116 192.168.200.100 192.168.200.150 TCP 74 56120 → 111 [SYN] Seq=0
14 36.774257841 192.168.200.100 192.168.200.150 TCP 74 33878 → 443 [SYN] Seq=
15 36.774366305 192.168.200.100 192.168.200.150 TCP 74 58636 → 554 [SYN] Seq=
16 36.774405627 192.168.200.100 192.168.200.150 TCP 74 52358 → 135 [SYN] Seq=
17 36.774535534 192.168.200.100 192.168.200.150 TCP 74 46138 → 993 [SYN] Seq=
18 36.774614776 192.168.200.100 192.168.200.150 TCP 74 41182 → 21 [SYN] Seq=0
29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 59174 → 113 [SYN] Seq=
30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 → 22 [SYN] Seq=0
31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 → 80 [SYN] Seq=0
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=
44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=
45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=
49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=
50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=
51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=
70 36.777143014 192.168.200.100 192.168.200.150 TCP 74 56990 → 767 [SYN] Seq=
71 36.777186821 192.168.200.100 192.168.200.150 TCP 74 35638 → 436 [SYN] Seq=
72 36.777302991 192.168.200.100 192.168.200.150 TCP 74 34120 → 98 [SYN] Seq=0
73 36.777337934 192.168.200.100 192.168.200.150 TCP 74 49780 → 78 [SYN] Seq=0
76 36.777473018 192.168.200.100 192.168.200.150 TCP 74 36138 → 580 [SYN] Seq=
77 36.777522494 192.168.200.100 192.168.200.150 TCP 74 52428 → 962 [SYN] Seq=
80 36.777645627 192.168.200.100 192.168.200.150 TCP 74 41874 → 764 [SYN] Seq=
81 36.777680898 192.168.200.100 192.168.200.150 TCP 74 51506 → 435 [SYN] Seq=
90 36.778179978 192.168.200.100 192.168.200.150 TCP 74 51450 → 148 [SYN] Seq=
91 36.778200161 192.168.200.100 192.168.200.150 TCP 74 48448 → 806 [SYN] Seq=
Frame 2: 74 bytes on wire (592 bits), 74 bytes cap
Ethernet II, Src: PCSSystemtec 39:7d:fe (08:00:27
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45
Cattura_U3_W1_L3.pcapng
Packets: 2083 · Displayed: 1026 (49.3%)
Profile: Default
Oracle VM VirtualBox Gestore
File Macchina Aiuto
pfsense Spenta
Kalilinuk per scansioni Spenta
Windows 7 per scansioni Spenta
Metasploitable per scansioni Spenta
Kalilinuk in rete Spenta
Pfsense 3 reti Spenta
Metasploitable in rete Spenta
Kalilinuk attaccante In esecuzione
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Nome: Kalilinuk attaccante
Sistema operativo: Ubuntu (64-bit)
Sistema
Memoria di base: 4096 MB
Processori: 2
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata, Paravirtualizzazione KVM
Schermo
Memoria video: 16 MB
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata
Archiviazione
Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: Clone di Kalilinuk con server e attaccante-disk1.vdi (Normale, 50,54 GB)
Audio
Driver host: Predefinita
Controller: ICH AC97
Rete
Anteprima


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo mount -t vboxsf Cartella_condivisa /media/cartella_condivisa
Cattura_U3_W1_L3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src == 192.168.200.100 && ip.dst == 192.168.200.150 && tcp.flags.syn == 1 && tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 → 80 [SYN] Seq=0
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 → 443 [SYN] Seq=
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 → 23 [SYN] Seq=0
13 36.774218116 192.168.200.100 192.168.200.150 TCP 74 56120 → 111 [SYN] Seq=0
14 36.774257841 192.168.200.100 192.168.200.150 TCP 74 33878 → 443 [SYN] Seq=
15 36.774366305 192.168.200.100 192.168.200.150 TCP 74 58636 → 554 [SYN] Seq=
16 36.774405627 192.168.200.100 192.168.200.150 TCP 74 52358 → 135 [SYN] Seq=
17 36.774535534 192.168.200.100 192.168.200.150 TCP 74 46138 → 993 [SYN] Seq=
18 36.774614776 192.168.200.100 192.168.200.150 TCP 74 41182 → 21 [SYN] Seq=0
29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 59174 → 113 [SYN] Seq=
30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 → 22 [SYN] Seq=0
31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 → 80 [SYN] Seq=0
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=
44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=
45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=
49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=
50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=
51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=
70 36.777143014 192.168.200.100 192.168.200.150 TCP 74 56990 → 767 [SYN] Seq=
71 36.777186821 192.168.200.100 192.168.200.150 TCP 74 35638 → 436 [SYN] Seq=
72 36.777302991 192.168.200.100 192.168.200.150 TCP 74 34120 → 98 [SYN] Seq=0
73 36.777337934 192.168.200.100 192.168.200.150 TCP 74 49780 → 78 [SYN] Seq=0
76 36.777473018 192.168.200.100 192.168.200.150 TCP 74 36138 → 580 [SYN] Seq=
77 36.777522494 192.168.200.100 192.168.200.150 TCP 74 52428 → 962 [SYN] Seq=
80 36.777645627 192.168.200.100 192.168.200.150 TCP 74 41874 → 764 [SYN] Seq=
81 36.777680898 192.168.200.100 192.168.200.150 TCP 74 51506 → 435 [SYN] Seq=
90 36.778179978 192.168.200.100 192.168.200.150 TCP 74 51450 → 148 [SYN] Seq=
91 36.778200161 192.168.200.100 192.168.200.150 TCP 74 48448 → 806 [SYN] Seq=
Frame 2: 74 bytes on wire (592 bits), 74 bytes cap
Ethernet II, Src: PCSSystemtec 39:7d:fe (08:00:27
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45
Cattura_U3_W1_L3.pcapng
Packets: 2083 · Displayed: 1026 (49.3%)
Profile: Default
Oracle VM VirtualBox Gestore
File Macchina Aiuto
pfsense Spenta
Kalilinuk per scansioni Spenta
Windows 7 per scansioni Spenta
Metasploitable per scansioni Spenta
Kalilinuk in rete Spenta
Pfsense 3 reti Spenta
Metasploitable in rete Spenta
Kalilinuk attaccante In esecuzione
Nuova Aggiungi Impostazioni Scarta Mostra
Generale
Nome: Kalilinuk attaccante
Sistema operativo: Ubuntu (64-bit)
Sistema
Memoria di base: 4096 MB
Processori: 2
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: Paginazione nidificata, Paravirtualizzazione KVM
Schermo
Memoria video: 16 MB
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata
Archiviazione
Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: Clone di Kalilinuk con server e attaccante-disk1.vdi (Normale, 50,54 GB)
Audio
Driver host: Predefinita
Controller: ICH AC97
Rete
Anteprima