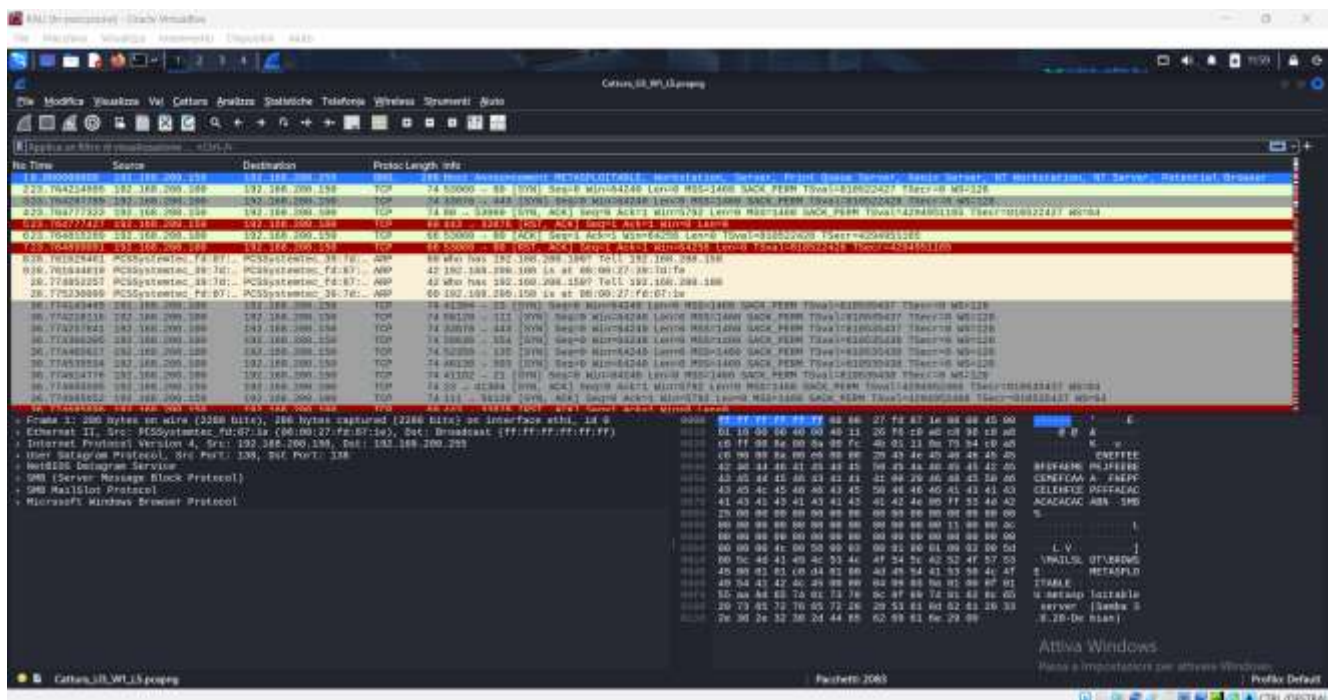


Threat Intelligence & IOC(progettoS9L5)



Lo scopo di questa analisi è esaminare una cattura di traffico di rete .pcapng per identificare potenziali Indicatori di Compromissione (IOC), formulare ipotesi sui vettori di attacco e proporre azioni di mitigazione e prevenzione.

Ho iniziato con la Gerarchia dei protocolli e ha rivelato che la maggior parte del traffico nella cattura è basata su **IPv4**, all'interno di questo, su **TCP (99.0%)**. Altri protocolli come UDP, ARP, SMB e NetBIOS sono presenti in percentuali minime. Quindi ci suggerisce un traffico di rete standard con un focus su comunicazioni tramite connessione.

Protocollo	Percentuale pacchetti	Pacchetti	Percentuale byte	Byte	Bit/s	Pacchetti finali	Byte finali	Bit/s finali	PDU
Frame	100.0	2083	100.0	138972	30 k	0	0	0	2083
Ethernet	100.0	2083	25.2	35276	7.652	0	0	0	2083
Internet Protocol Version 4	99.8	2079	29.7	41580	5.079	0	0	0	2079
User Datagram Protocol	0.0	1	0.0	8	1	0	0	0	1
NetBIOS Datagram Service	0.0	1	0.1	82	17	0	0	0	1
SMB (Server Message Block Protocol)	0.0	1	0.1	162	35	0	0	0	1
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0	1
Microsoft Windows Browser Protocol	0.0	1	0.1	76	16	1	76	16	1
Transmission Control Protocol	99.8	2078	44.8	62652	13 k	2078	62652	13 k	2078
Address Resolution Protocol	0.2	4	0.1	112	24	4	112	24	4

Vedendo le conversazioni a livello IPv4 ci dice che la stragrande maggior parte del traffico si concentra tra due indirizzi IP interni alla stessa sottorete: **192.168.200.100** e **192.168.200.150**

Indirizzo A	Indirizzo B	Pacchetti	Byte	ID flusso	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B	Bits/s B → A
192.168.200.100	192.168.200.150	2,078	139 KB	1	1,052	78 KB	1,026	62 KB	23.764215	13.1147	47 kbps	37 kbps
192.168.200.150	192.168.200.100	1	286 byte	0	1	286 byte	0	0 byte	0.000000	0.0000		

Invece le conversazioni TCP ,da qui, è stato confermato che 192.168.200.100 è la sorgente che avvia la maggior parte delle connessioni verso 192.168.200.150 su diverse porte.

Indirizzo A	Porta A	Indirizzo B	Porta B	Pacchetti	Byte	ID flusso	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Inizio Rel	Durata	Bits/s A → B
192.168.200.100	32792	192.168.200.150	445	2	134 byte	520	1	74 byte	1	60 byte	36.829887	0.0002	
192.168.200.100	32794	192.168.200.150	445	2	134 byte	931	1	74 byte	1	60 byte	36.870238	0.0002	
192.168.200.100	32820	192.168.200.150	445	2	134 byte	518	1	74 byte	1	60 byte	36.828836	0.0001	
192.168.200.100	32862	192.168.200.150	445	2	134 byte	948	1	74 byte	1	60 byte	36.871950	0.0002	
192.168.200.100	32896	192.168.200.150	445	2	134 byte	837	1	74 byte	1	60 byte	36.838788	0.0000	
192.168.200.100	32910	192.168.200.150	445	2	134 byte	287	1	74 byte	1	60 byte	36.806271	0.0003	
192.168.200.100	32922	192.168.200.150	445	2	134 byte	909	1	74 byte	1	60 byte	36.870958	0.0002	
192.168.200.100	32950	192.168.200.150	445	2	134 byte	74	1	74 byte	1	60 byte	36.782275	0.0003	
192.168.200.100	32976	192.168.200.150	445	2	134 byte	754	1	74 byte	1	60 byte	36.848345	0.0003	
192.168.200.100	32986	192.168.200.150	445	2	134 byte	425	1	74 byte	1	60 byte	36.818978	0.0003	
192.168.200.100	32950	192.168.200.150	445	2	134 byte	809	1	74 byte	1	60 byte	36.855530	0.0002	
192.168.200.100	33050	192.168.200.150	445	2	134 byte	626	1	74 byte	1	60 byte	36.857281	0.0002	
192.168.200.100	32956	192.168.200.150	445	2	134 byte	157	1	74 byte	1	60 byte	36.792679	0.0002	
192.168.200.100	33058	192.168.200.150	445	2	134 byte	270	1	74 byte	1	60 byte	36.804777	0.0002	
192.168.200.100	33058	192.168.200.150	445	2	134 byte	911	1	74 byte	1	60 byte	36.828573	0.0003	
192.168.200.100	33102	192.168.200.150	445	2	134 byte	74	1	74 byte	1	60 byte	36.782583	0.0003	
192.168.200.100	33114	192.168.200.150	445	2	134 byte	262	1	74 byte	1	60 byte	36.803843	0.0002	
192.168.200.100	33206	192.168.200.150	445	2	134 byte	18	1	74 byte	1	60 byte	36.776496	0.0004	
192.168.200.100	33250	192.168.200.150	445	2	134 byte	299	1	74 byte	1	60 byte	36.807513	0.0002	
192.168.200.100	33280	192.168.200.150	445	2	134 byte	234	1	74 byte	1	60 byte	36.807427	0.0003	
192.168.200.100	33393	192.168.200.150	445	2	134 byte	368	1	74 byte	1	60 byte	36.812553	0.0003	
192.168.200.100	33284	192.168.200.150	445	2	134 byte	640	1	74 byte	1	60 byte	36.820439	0.0002	
192.168.200.100	33420	192.168.200.150	445	2	134 byte	193	1	74 byte	1	60 byte	36.796398	0.0003	
192.168.200.100	33452	192.168.200.150	445	2	134 byte	744	1	74 byte	1	60 byte	36.848410	0.0001	
192.168.200.100	33480	192.168.200.150	445	2	134 byte	673	1	74 byte	1	60 byte	36.842749	0.0002	
192.168.200.100	33566	192.168.200.150	445	2	134 byte	303	1	74 byte	1	60 byte	36.808437	0.0002	

Alcune porte di destinazione su 192.168.200.150 mi hanno fatto attirare l'attenzione ovvero:

- **Porta 445 (SMB):** Un servizio comune per la condivisione file Windows, che è usato anch come bersaglio.
- **Porta 381:** Una porta insolita per una rete IT standard, che è associata a dispositivi specifici.

No	Time	Source	Destination	Protoc	Length	Info
38	0.000000	192.168.200.100	192.168.200.150	TCP	74	44538 → 381 [SYN] Seq=1400000000 Win=0 Len=0
39	0.000000	192.168.200.150	192.168.200.100	TCP	60	381 → 44538 [RST, ACK] Seq=1400000000 Win=0 Len=0

The image shows a Wireshark packet capture with the filter 'tcp.port == 445'. The packet list shows several packets between 192.168.200.100 and 192.168.200.150. The packet details pane shows a TCP segment with Seq=64256, Win=0, Len=0, and a Reset flag set.

No.	Time	Source	Destination	Protocol	Length	Info
36	7.76395094	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=64256 Len=0 MSS=1460 SACK_PERM TSval=810525448 Tsecr=0 Win=0
37	7.77184028	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, RST] Seq=64256 Win=0 Len=0 MSS=1460 SACK_PERM TSval=810525448 Tsecr=810525448 Win=0
38	7.776914772	192.168.200.100	192.168.200.150	TCP	66	33842 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810525448 Tsecr=4294952408
39	7.777992288	192.168.200.100	192.168.200.150	TCP	98	33842 → 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSval=810525448 Tsecr=4294952408

Mi sono concentrato tra 192.168.200.100 e 192.168.200.150.

Porta 381 Il traffico mostra un handshake TCP (SYN, SYN, ACK) seguito immediatamente da un reset (RST) da parte di 192.168.200.100. Ha indicato che il servizio sulla porta 381 su 192.168.200.150 è in ascolto ma la connessione è stata interrotta subito dopo la sua instaurazione, senza scambi.

Porta 445 (SMB) la connessione TCP è stata stabilita con successo. Un'analisi approfondita dello stream TCP non ha rivelato alcuno scambio di dati applicativi SMB significativo dopo l'handshake. La connessione viene poi chiusa.

Questo comportamento ripetuto di "connetti e chiudi subito" su diverse porte indica chiaramente una scansione delle porte da parte di 192.168.200.100 per capire quali servizi sono attivi su 192.168.200.150

Il più importante Indicatore di Compromissione (IOC) scoprendolo analizzando un pacchetto di annuncio di rete presente nella cattura



Questo pacchetto ha rivelato che l'indirizzo 192.168.200.150 si identificava come "METASPLOITABLE". Metasploitable è una macchina virtuale creata apposta per essere vulnerabile e viene usata per test di attacchi e sicurezza(ma noi facciamo finta). Ci conferma che 192.168.200.150 è un bersaglio progettato per essere attaccato.

Esamino un pacchetto che appartiene al "NetBIOS Datagram Service". Vedo che si tratta di un datagramma di tipo "Direct group datagram" e la sua dimensione è di 230 byte. La cosa interessante è che la sorgente è 192.168.200.150 e si riferisce a "metasploitable" con la destinazione "workgroup" qui mi fa pensare che si tratti di una VM

```

- NetBIOS Datagram Service
  Message Type: Direct_group datagram (17)
  Flags: 0x0a, This is first fragment, Node Type: M node
  Datagram ID: 0x75b4
  Source IP: 192.168.200.150
  Source Port: 138
  Datagram length: 238 bytes
  Packet offset: 8 bytes
  Source name: METASPLOITABLE<00> (Workstation/Redirector)
  Destination name: WORKGROUP<id> (Local Master Browser)
- SMB (Server Message Block Protocol)
  - SMB Header
    Server Component: SMB
    SMB Command: Trans (0x25)
    Error Class: Success (0x00)
    Reserved: 00
    Error Code: No Error
  - Flags: 0x00
    0... .. = Request/Response: Message is a request to the server
    .0... .. = Notify: Notify client only on open
    ..0... .. = Oplocks: OpLock not requested/granted
    ...0... .. = Canonicalized Pathnames: Pathnames are not canonicalized
    ....0... .. = Case Sensitivity: Path names are case sensitive
    .....0... .. = Receive Buffer Posted: Receive buffer has not been posted
    .....0... .. = Lock and Read: Lock&Read, Write&Unlock are not supported
  - Flags2: 0x0000
    0... .. = Unicode Strings: Strings are ASCII
    .0... .. = Error Code Type: Error codes are DOS error codes
    ..0... .. = Execute-only Reads: Don't permit reads if execute-only
    ...0... .. = Dfs: Don't resolve pathnames with Dfs
    ....0... .. = Extended Security Negotiation: Extended security negotiation is not supported
    .....0... .. = Reparse Path: The request does not use a BCNT reparse path
    .....0... .. = Long Names Used: Path names in request are not long file names

```

```

    .....0... .. = Long Names Used: Path names in request are not long file names
    .....0... .. = Security Signatures Required: Security signatures are not required
    .....0... .. = Compressed: Compression is not requested
    .....0... .. = Security Signatures: Security signatures are not supported
    .....0... .. = Extended Attributes: Extended attributes are not supported
    .....0... .. = Long Names Allowed: Long file names are not allowed in the response
  Process ID High: 0
  Signature: 0000000000000000
  Reserved: 0000
  Tree ID: 0
  Process ID: 0
  User ID: 0
  Multiplex ID: 0
- Trans Request (0x25)
  Word Count (WC): 17
  Total Parameter Count: 8
  Total Data Count: 76
  Max Parameter Count: 8
  Max Data Count: 8
  Max Setup Count: 0
  Reserved: 00
- Flags: 0x0000
  .....0... .. = One Way Transaction: Two way transaction
  .....0... .. = Disconnect TID: Do NOT disconnect TID
  Timeout: Return immediately (0)
  Reserved: 0000
  Parameter Count: 8
  Parameter Offset: 8
  Data Count: 76
  [Bytes remaining until TDC: 0]
  Data Offset: 86
  Setup Count: 3
  Reserved: 00
  Byte Count (BCC): 93

```

Abbiamo SMB All'interno dello stesso pacchetto. Vedo che il comando è un "Trans (0x25)" e l'operazione ha avuto successo. Analizzando i flag, noto alcune cose, indicando che è una richiesta inviata al server e che le stringhe utilizzate sono in formato ASCII.

Andando avanti mi mostra l'attività legata al SMB MailSlot Protocol. Qui indica che il sistema metasploitable sta scrivendo a un mailslot specifico per scopi di Browse di rete.

```

  Byte Count (BCC): 93
  Transaction Name: \MAILSLOT\BROWSE
- SMB MailSlot Protocol
  Opcode: Write Mail Slot (1)
  Priority: 1
  Class: Unreliable & Broadcast (2)
  Size: 93
  Mailslot Name: \MAILSLOT\BROWSE

```


Il "Host Comment" "metasploitable server (Samba 3.0.20-Debian)" è la conferma: METASPLOITABLE.

```
+ Microsoft Windows Browser Protocol
Command: Host Announcement (0x01)
Update Count: 1
Update Periodicity: 2 minutes
Host Name: METASPLOITABLE
Windows version:
OS Major Version: 4
OS Minor Version: 9
- Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser
```

```
+ Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser
...1 = Workstation: This is a Workstation
...1 = Server: This is a Server
...0 = SQL: This is NOT an SQL server
...0 = Domain Controller: This is NOT a Domain Controller
...0 = Backup Controller: This is NOT a Backup Controller
...0 = Time Source: This is NOT a Time Source
...0 = Apple: This is NOT an Apple host
...0 = Novell: This is NOT a Novell server
...0 = Member: This is NOT a Domain Member server
...1 = Print: This is a Print Queue server
...0 = Dialin: This is NOT a Dialin server
...1 = Xenix: This is a Xenix server
...1 = NT Workstation: This is an NT Workstation
...0 = WFW: This is NOT a WFW host
...1 = NT Server: This is an NT Server
...1 = Potential Browser: This is a Potential Browser
...0 = Backup Browser: This is NOT a Backup Browser
...0 = Master Browser: This is NOT a Master Browser
...0 = Domain Master Browser: This is NOT a Domain Master Browser
...0 = OSF: This is NOT an OSF host
...0 = VMS: This is NOT a VMS host
...0 = Windows 95+: This is NOT a Windows 95 or above host
...0 = DFS: This is NOT a DFS server
...0 = Local: This is NOT a local list only request
...0 = Domain Enum: This is NOT a Domain Enum request
Browser Protocol Major Version: 15
Browser Protocol Minor Version: 1
Signature: 0xaa55
Host Comment: metasploitable server (Samba 3.0.20-Debian)
```

IPOTESI: Dato che 192.168.200.150 è una macchina Metasploitable, l'aggressore 192.168.200.100 e quindi sta cercando di sfruttare le sue vulnerabilità note. Sulle porte come la **381** l'attaccante potrebbe tentare exploit specifici per quei servizi. Sulla **porta 445 (SMB)**, qui ci sono tentativi di indovinare le password per accedere alle condivisioni, o tramite comandi a distanza.

Qui l'attaccante sta cercando il modo migliore per entrare nel sistema.

CONSIGLI PER RIDURRE GLI IMPATTI E PREVENIRE ATTACCHI FUTURI: La prima cosa che farei è isolare la macchina 192.168.200.150 dalla rete. Essendo una macchina volutamente vulnerabile, rappresenta un rischio abbastanza alto e potrebbe compromettere altri sistemi.

Bisogna mantenere tutti i sistemi e i programmi sempre aggiornati con le ultime patch di sicurezza. Chiudere le porte, almeno quelle non necessarie in modo da non avere altri punti deboli. Configurare sempre il firewall per bloccare il traffico. Fare una segmentazione di rete con le

VLAN così da dividere la rete in sezioni più piccole e isolate ed essere più protetti. Usare password complessi. Attivando IDS/IPS per mettere in rete una maggiore prevenzione delle intrusioni per bloccare automaticamente le scansioni. Infine controllare sempre log di sistema e il traffico di rete per vedere se ci sono attività abbastanza sospette.