# S9L5

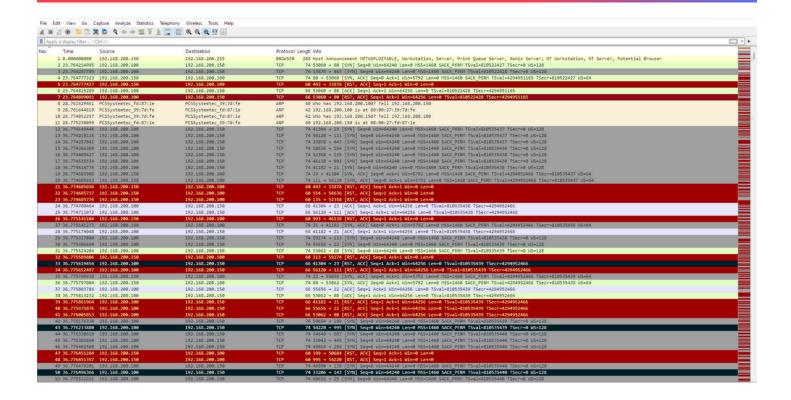


Data: 29/11/24

#### **INFORMAZIONI PRINCIPALI**

Traccia: Esercizio Threat Intelligence & IOC Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto. Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti: • Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso • In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati • Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

### **INIZIO ESERCIZIO**

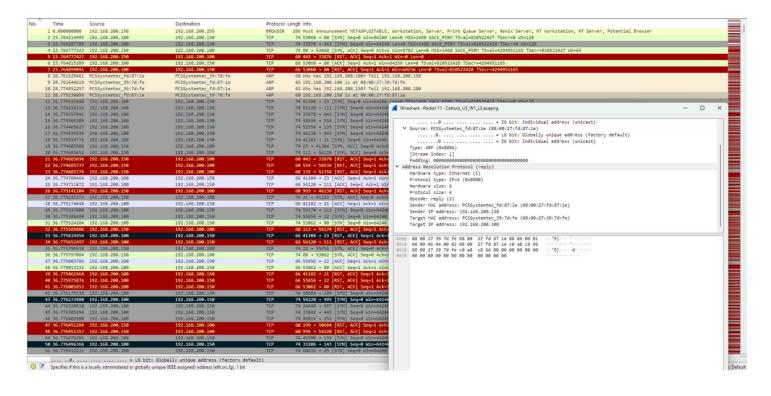


Dall'analisi svolta, un utente interno (192.168.200.100) Nella nostra stessa rete e stesi nomi delle macchine (hostnames). Ha eseguito una scansione delle porte sulla macchina con IP 192.168.200.150 utilizzando uno strumento come nmap. Questo comportamento è tipico di un'attività di ricognizione volta a individuare porte aperte e servizi attivi sul server, ma non risulta essere un attacco diretto come un DoS o DDoS.

I pacchetti catturati mostrano il classico schema del three-way handshake del protocollo TCP, con sequenze di pacchetti SYN, SYN-ACK e ACK, seguiti da risposte RST che chiudono le connessioni. Questo dimostra che non siamo di fronte a un attacco SYN Flood, poiché le connessioni non rimangono "half-open" (aperte a metà) e si chiudono regolarmente. Inoltre, la scansione non mostra cicli infiniti di connessioni aperte e chiuse, escludendo anche un TCP Flood, che si manifesterebbe con un flusso continuo di connessioni ripetute verso una o più porte, Inoltre non ci sono pacchetti UDP o ICMP evidenti, quindi non si tratta di un UDP Flood o ICMP Flood.

15 36.774366305 192.168.200.100	192.168.200.150	TCP	74 58636 + 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PERM TSval=010535438 TSecr=0 MS=128
16 36.774405627 192.168.200.100	192.168.200.150	TCP	/# 20030 * 324 [318] Seque Minedade Lenio rosalado sint, "CRI 13/48/06/353438 TSECTIO ROSALO 74 52358 + 135 [\$18] Seque Minedade Lenio rosalado Sint, "CRI 13/48/0535438 TSECTIO MS-120  ———————————————————————————————————
17 36,774535534 192,168,200,100	192,168,200,150	TCP	74 46138 + 993 [SYN] Seq-0 kilm64240 Lenno MSS-1460 SAKC PERN TSVal-810835448 TSecr-0 MS-128
18 36.774614776 192.168.200.100	192.168.200.150	TCP	74 41182 + 21 [SYN] Sequel Min-64240 Leney MS-1406 SACK PERM TSVal-810535438 TSecreb MS-128
19 36.774685505 192.168.200.150	192.168.200.100	TCP	74 4136 = 13   3   3   5   5   1   1   1   1   1   1   1   1
20 36.774685652 192.168.200.150	192.168.200.100	TCP	74 111 + 56120 [SVN, ACK] Seque Acks1 Win-5792 Lense RSS-1460 SACK_FEN 13923-4294952466 TSecr-818953437 WS-64
21 36.774685696 192.168.200.150	192.168.200.100	TCP	79 44 3 33272 [RST, ACC] Segri Acksi Minist Lenso
22 36.774685737 192.168.200.150	192,168,200,100	TCP	60 554 + 58636 [RST, ACK] Sequi Ackel Minist Lenso
23 36.774685776 192.168.200.150	192.168.200.100	TCP	60 135 + \$2358 [857, ACK] Seq-1 Ack-1 kin-0 Len-0
24 36.774700464 192.168.200.100	192.168.200.150	TCP	66 41384 ÷ 23 [AK, Sequi Ackel Win=64256 Len=0 Tsval=810535438 TSecr=4294952466
25 36.774711072 192.168.200.100	192.168.200.150	TCP	66 56120 + 111 [ACK] Seq=1 ACk=1 Win=64256 Len=0 TSvsl=610535438 TSecr=4294952466
26 36.775141104 192.168.200.150	192.168.200.100	TCP	00 903 + 46138 [85.7] XC[3 Seq. Arks. Militida Lend (
27 36,775141273 192,168,200,150	192,168,200,100	TCP	74 21 + 41182 [SYN, ACK] Seque Ack=1 Wine5792 Lene MSS=1460 SACK PERM TSVal=4294952466 TSecr=810535438 WS=64
28 36.775174048 192.168.200.100	192.168.200.150	TCP	66 41182 + 21 [A(K) Sequil Ackel Winne40256 Lene0 Tsval-810935438 TSecr-4294952466
29 36.775337800 192.168.200.100	192.168.200.150	TCP	74 59174 + 113 [574] Seq+0 Min+64240 Len+0 MSS+1460 SAKK PERN TSval+01053438 TSecn+0 MS+128
30 36.775386694 192.168.200.100	192.168.200.150	TCP	74 55656 + 22 [\$78] Seq+0 Min+6+240 Len+0 MSS+1400 SACK PERM TSvs1+810535439 TSecr+0 MS+128
31 36.775524204 192.168.200.100	192.168.200.150	TCP	74 53062 + 80 [SYN] Seg=0 Hin-64240 Len=0 NSS=1460 SACK_PERM TSval=810535439 TSecr=0 NS=128
32 36,775589806 192,168,200,150	192.168.200.100	TCP	60 113 + 59174 [857, ACK] Seq=1 Ack=1 Win+0 Len+0
33 36.775619454 192.168.200.100	192.168.200.150	TCP	66 41304 + 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=818535439 TSecr=4294952466
34 36.775652497 192.168.200.100	192,168,200,150	TCP	66 56120 + 111 [RST, ACK] Seq-1 Ack-1 Win-64256 Len-0 TSval-810535439 TSecr-4294952466
35 36.775796938 192.168.200.150	192.168.200.100	TCP	74 22 + 55656 [SYN, ACK] Seq+0 Ack+1 Min+5792 Len+0 MSS+1460 SACK PERM TSVal+4294952466 TSecr+810535439 MS+64
36 36.775797004 192.168.200.150	192,168,200,100	TCP	74 80 + 53062 [SYN, ACK] Seq=0 Ack=1 Nin=5792 Len=0 PSS=1460 SACK PERM TSval=4294952466 TSecr=810535439 NS=64
37 36.775803786 192.168.200.100	192,168,200,150	TCP	66 55656 + 22 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38 36,775813232 192,168,200,100	192,168,200,150	TCP	66 53062 + 80 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39 36.775861964 192.168.200.100	192.168.200.150	TCP	66 41182 + 21 [RST, ACK] Seq=1 Ack=1 Win-64256 Len=0 TSval=810535439 TSecr=4294952466
40 36.775975876 192.168.200.100	192.168.200.150	TCP	66 55656 + 22 [RST, ACK] Segri Ack-1 Nin-64256 Len-0 TSval-810535439 TSecr-4294052466
41 36.776005853 192.168.200.100	192.168.200.150		66 53962 + 80 [RST, ACK] Seq=1 Ack=1 Min=64256 Len=0 TSval=810535439 TSecr=4294952466
			74 50684 + 199 [SYN] Seg=0 Min=64240 Len=0 MSS=1460 SACK PERM TSval=810535439 TSecr=0 MS=128
42 36.776179338 192.168.200.100	192.168.200.150	TCP	
42 36.776179338 192.168.200.100 43 36.776233880 192.168.200.100	192.168.200.150 192.168.200.150	TCP	74 54220 + 995 [SYN] Seq+0 Min-62404 Len+0 MSS-1460 SACK PEM TSV21-00005059 TSCC+0 MS-128
43 36.776233880 192.168.200.100	192.168.200.150	TCP	74 54220 + 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43 36.776233880 192.168.200.100 44 36.776338610 192.168.200.100	192.168.200.150 192.168.200.150	TCP	74 54220 + 993 [SYN] Seq+0 Nin-64240 Len+0 MSs-1460 SACK_PERM TSval+810535439 TSecr+0 NS-128 74 34648 + 587 [SYN] Seq+0 Nin-64240 Len+0 MSs-1460 SACK_PERM TSval+810535440 TSecr+0 NS-128
43 36.776233880 192.168.200.100 44 36.776330610 192.168.200.100 45 36.776385694 192.168.200.100	192.168.200.150 192.168.200.150 192.168.200.150	TCP TCP TCP	74 5420 + 995 [SYN] Seq+0 klin-64240 ken+0 KSS-1460 SACK_PERH TSVAL-810935439 TSECT-0 KS-128 74 34648 - 587 [SYN] Seq+0 klin-64240 ken+0 KSS-1460 SACK_PERH TSVAL-810935440 TSECT-0 KS-128 74 33042 - 445 [SYN] Seq+0 klin-64240 ken+0 KSS-1460 SACK_PERH TSVAL-810935440 TSECT-0 KS-128  ### STANDARD SACK SACK SACK SACK SACK SACK SACK SACK
43 36.776233880 192.168.209.100 44 36.776330610 192.168.209.100 45 36.776385694 192.168.209.100 46 36.776402590 192.168.209.100	192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP TCP TCP TCP	74 54278 + 995 [2711] sequé Unindé220 (enné 1765-1466 SACC, PERI TSVAL-18195749) Tiscrné US-128 74 34464 + 975 [2711] sequé Unindé220 (enné 1765-1466 SACC, PERI TSVAL-18195844) Tiscrné Uniformation (en 1765-1466 SACC, PERI TSVAL-18195844) Tiscrné Uniformation (en 1765-1466 SACC, PERI TSVAL-181955844) Tiscrné Uniformation (en 1765-1466 SACC, PERI TSVAL-181955844) Tiscrné Uniformation (en 1765-1466 SACC, PERI TSVAL-181958444) Tiscrné Uniformation (en 1765-1466 SACC, PERI TSVAL-1819584444) Tiscrné Uniformation (en 1765-1466 SACC, PERI TSVAL-1819584444444444444444444444444444444444
43 36.776/33880 192.165.209.109 44 36.776/33061 0 192.165.209.109 45 36.776/385694 192.168.209.109 46 36.776/32760 192.168.209.109 47 36.776/31284 192.168.209.159 48 36.776/31281 192.168.209.159 49 36.776/47201 192.168.209.109	192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100	TCP TCP TCP TCP TCP TCP TCP	74 5428 + 995 [271] Sequé Mine5220 (enté NS-1468 SACC_PEN TSVAL-18035439 Tiscrné MS-128 74 39448 + 975 [271] Sequé Mine5220 (enté NS-1469 SACC_PEN TSVAL-18035440 Tiscrné MS-128 74 3942 + 445 [571] Sequé Mine5220 (enté NS-1469 SACC_PEN TSVAL-18035440 Tiscrné MS-128 74 49814 + 256 [571] Sequé Mine5220 (enté NS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128 63 193 + 3964 [671, ACC] Sequé Acci Mine8 (enté (enté MS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128 64 995 + 44220 [687, ACC] Sequé Acci Mine8 (enté (enté MS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128 64 4990 + 219 [571] Sequé Mine5220 (enté MS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128
43 36,776233880 192,165,200,100 44 35,77633616 192,165,200,100 45 36,77643569 192,165,200,100 46 36,77645569 192,165,200,100 47 36,77645324 192,165,200,150 48 36,77645327 192,165,200,150 49 36,776476354 192,165,200,100 98 36,7764768546 192,165,200,100	192,168,200,150 192,168,200,150 192,168,200,150 192,168,200,150 192,168,200,100 192,168,200,100	TCP TCP TCP TCP TCP TCP TCP	74 \$4220 + 995 [271] seep@ ktm-64220 (em-0 PKS-1460 SACK_PERN TSVal-181095549) Tiscrn-0 KS-128 74 \$1464 + \$72 [271] seep@ ktm-64220 (em-0 PKS-1460 SACK_PERN TSVal-181095440 Tiscrn-0 KS-128 74 \$1942 + 445 [271] seep@ ktm-64220 (em-0 PKS-1460 SACK_PERN TSVal-1810955440 Tiscrn-0 KS-128 74 \$1984 + 575 [271] seep@ ktm-64220 (em-0 PKS-1460 SACK_PERN TSVal-1810955440 Tiscrn-0 KS-128 64 \$193 + \$9064 [857, ACK] seeq.1 Ack-1 ktm-0 Lem-0 69 \$95 + \$4020 [857, ACK] seeq.1 Ack-1 ktm-0 Lem-0 74 \$4990 + 130 [271] seep@ ktm-64220 (em-0 PKS-1460 SACK_PERN TSVal-1810955440 Tiscrn-0 KS-128 74 \$13260 + 131 [271] seep@ ktm-64220 (em-0 PKS-1460 SACK_PERN TSVal-1810955440 Tiscrn-0 KS-128
43 36.776/33880 192.168.209.109 44 36.776/33061 0 192.168.209.109 45 36.776/385694 192.168.209.109 46 36.776/43280 192.168.209.109 47 36.776/45/1284 192.168.209.159 48 36.776/45/1284 192.168.209.159 49 36.776/47/201 192.168.209.109	192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100	TCP TCP TCP TCP TCP TCP TCP	74 5428 + 995 [271] Sequé Mine5220 (enté NS-1468 SACC_PEN TSVAL-18035439 Tiscrné MS-128 74 39448 + 975 [271] Sequé Mine5220 (enté NS-1469 SACC_PEN TSVAL-18035440 Tiscrné MS-128 74 3942 + 445 [571] Sequé Mine5220 (enté NS-1469 SACC_PEN TSVAL-18035440 Tiscrné MS-128 74 49814 + 256 [571] Sequé Mine5220 (enté NS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128 63 193 + 3964 [671, ACC] Sequé Acci Mine8 (enté (enté MS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128 64 995 + 44220 [687, ACC] Sequé Acci Mine8 (enté (enté MS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128 64 4990 + 219 [571] Sequé Mine5220 (enté MS-1469 SACC_PEN TSVAL-81035440 Tiscrné MS-128
43 56, 776233880 192, 165, 200, 100 43 56, 776336161 192, 165, 200, 100 45 36, 77643564 192, 165, 200, 100 46 36, 776455264 192, 165, 200, 100 47 36, 776451284 192, 165, 200, 150 48 36, 776451287 192, 165, 200, 150 49 36, 776457261 192, 165, 200, 100 59 36, 776450566 192, 165, 200, 100	192,166,200,150 192,168,200,150 192,168,200,150 192,168,200,150 192,168,200,100 192,168,200,100 192,168,200,150 192,168,200,150	TCP	74 \$4220 + 995 [271] Seepé Min-64220 (enné 1763-1466 SACC, PERT TSVal-181055440 TSccr-10 KS-128 74 \$1846 + 975 [271] Seepé Min-64220 (enné 1763-1466 SACC, PERT TSVal-181055440 TSccr-10 KS-128 74 \$1842 + 445 [271] Seepé Min-64220 (enné 1763-1469 SACC, PERT TSVal-1810555440 TSccr-10 KS-128 64 199 + 96064 [657, ACC] Seepl Acch Min-9 Lenné 69 99 + 94062 [657, ACC] Seepl Acch Min-9 Lenné 74 48990 + 139 [271] Seepé Min-64220 (enné 1763-1469 SACC, PERT TSVal-1810555440 TSccr-10 KS-128 74 48990 + 139 [271] Seepé Min-64220 (enné 1763-1469 SACC, PERT TSVal-1810555440 TSccr-10 KS-128 74 18306 × 130 [271] Seepé Min-64220 (enné 1763-1469 SACC, PERT TSVal-1810555440 TSccr-10 KS-128 74 48954 + 130 [271] Seepé Min-64220 (enné 1763-1469 SACC, PERT TSVal-1810555440 TSccr-10 KS-128 74 48954 + 130 [271] Seepé Min-64220 (enné 1763-1469 SACC, PERT TSVal-1810555440 TSccr-10 KS-128
43 36,776231889 192,165,200,100 44 36,776336161 92,165,200,100 45 36,776355694 192,165,200,100 46 36,776455264 192,165,200,150 47 36,7764551284 192,165,200,150 48 36,7764551275 192,165,200,150 49 36,77645566 192,165,200,100 59 36,7764566 192,165,200,100 51 36,77645566 192,165,200,100	192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150	TCP	74 \$4220 + 995 [271] Seepé Minés220 Lené NSS-1466 SACC_PEN TSVAL-18035439 Tiscrné MS-128 74 \$14648 + 75 [271] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-18035540 Tiscrné MS-128 74 \$1942 + 445 [271] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 8014 + 75 [271] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 64 199 + 50654 [KST, ACC] Seepi Ackel Miné Lené 64 955 + 54220 [KST, ACC] Seepi Ackel Miné Lené 64 955 + 54220 [KST, ACC] Seepi Ackel Minés Lené 74 46900 + 179 [771] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 33206 + 143 [271] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 06932 + 25 [371] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 06932 + 25 [371] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 06934 + 110 [271] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 37222 + 35 [371] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128 74 75 37222 + 35 [371] Seepé Minés220 Lené NSS-1460 SACC_PEN TSVAL-180355440 Tiscrné MS-128
43 36,776231869 192,165,200,100 44 35,77633616 192,165,200,100 45 36,77643569 192,165,200,100 46 36,77645520 192,165,200,100 47 36,77645324 192,165,200,150 48 36,77645327 192,165,200,150 49 36,77645221 192,165,200,100 51 36,77645221 192,165,200,100 52 36,77655221 192,165,200,100 53 36,77651221 192,165,200,100 53 36,77651221 192,165,200,100 54 36,776571271 192,165,200,100 54 36,776671271 192,165,200,100 54 36,776671271 192,165,200,100	192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150	TCP	74 \$4220 • 995 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-018075490 TSCC-70 MS-128 74 \$18464 • \$72 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-018075440 TSCC-70 MS-128 74 83942 • 445 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-018075440 TSCC-70 MS-128 64 1991 • 59062 [657] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 69 995 • 59022 [657] ACC] Seepl Acch Min-90 Lenné 74 49990 • 139 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 33260 • 133 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 69052 • 25 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 49054 • 110 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 3722 • 35 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 49054 • 110 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 3722 • 35 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 74 54808 • 500 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 75 54808 • 500 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 75 54808 • 500 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 75 54808 • 500 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128 75 54808 • 500 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVA1-0180755440 TSCC-70 MS-128
43 56,776233880 192,165,200,100 44 36,77633610 192,165,200,100 45 36,77635664 192,165,200,100 45 36,77645520 192,165,200,100 47 36,77645520 192,166,200,150 48 36,77645520 192,166,200,150 49 36,776475201 192,166,200,150 59 36,776475201 192,166,200,160 59 36,77645526 192,166,200,160 59 36,77645526 192,166,200,160 59 36,77645526 192,166,200,160 59 36,77645525 192,166,200,160 59 36,77645525 192,166,200,160 59 36,776452521 192,166,200,160 59 36,776452521 192,166,200,160 59 36,776451213 192,166,200,160 59 36,776451323 192,168,200,160	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150	TCP	74 \$4224 • 995 [271] Seepé Minés220 Lené NSS-1468 SACC_PEN TSVAL-110353439 Tiscrné MS-128 74 \$14648 • 75 [271] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 74 \$1942 • 445 [271] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 74 \$1942 • 75 [271] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 74 \$1954 • 5422 [457, ACC] Seep Ack-1 Miné Lené 74 \$1955 • 5422 [457, ACC] Seep Ack-1 Miné Lené 74 \$1956 • 5422 [457, ACC] Seep Ack-1 Miné Lené 75 \$1956 • 5422 [571] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 76 \$1926 • 75 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 77 \$1956 • 75 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 78 \$1956 • 75 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 78 \$1956 • 75 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 78 \$1956 • 75 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 78 \$1958 • 900 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 78 \$1958 • 900 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 78 \$1958 • 900 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 8 \$1956 • 900 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 8 \$1956 • 900 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128 8 \$1956 • 900 [371] Seepé Minés220 Lené NSS-1469 SACC_PEN TSVAL-110355440 Tiscrné MS-128
43 56,776231869 192,165,200,100 43 56,776336161 192,165,200,100 45 36,77643564 192,165,200,100 47 36,77645364 192,165,200,100 47 36,77645327 192,165,200,150 49 36,77645327 192,165,200,150 49 36,77645327 192,165,200,100 53 36,77645321 192,165,200,100 53 36,77645321 192,165,200,100 53 36,77654221 192,165,200,100 53 36,77654221 192,165,200,100 53 36,77654321 192,165,200,100 53 36,77654321 192,165,200,100 53 36,77643121 192,165,200,100 55 36,77643121 192,165,200,100	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150	TCP	74 \$4220 • 995 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-18103540 TSCC-70 MS-128 74 31642 • 445 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-18103540 TSCC-70 MS-128 74 31942 • 445 [271] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-181035540 TSCC-70 MS-128 64 1991 • 50624 [657] ACC) Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVAL-1810355400 TSCC-70 MS-128 69 995 • 45022 [657] ACC) Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVAL-1810355400 TSCC-70 MS-128 74 4990 • 139 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-1810355400 TSCC-70 MS-128 74 4990 • 139 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-1810355400 TSCC-70 MS-128 74 4990 • 130 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-181035540 TSCC-70 MS-128 74 4990 • 130 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 74 4990 • 130 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 74 3932 • 393 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 75 54800 • 390 [271] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 69 97 • 34648 [657] ACC] Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 69 97 • 34648 [657] ACC] Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 69 97 • 34648 [657] ACC] Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128 69 97 • 34648 [657] ACC] Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVAL-1810355440 TSCC-70 MS-128
43 36,776233863 192,165,200,100 43 36,776336161 92,165,200,100 45 36,77635664 192,165,200,100 45 36,776455264 192,165,200,100 47 36,776455264 192,165,200,100 48 36,776455261 192,165,200,150 49 36,776457261 192,166,200,150 51 36,776572721 192,166,200,150 51 36,776572721 192,166,200,100 51 36,776572721 192,166,200,100 53 36,776572721 192,166,200,100 53 36,776673273 192,166,200,100 53 36,776643223 192,166,200,100 55 36,776643223 192,166,200,100 57 36,776643223 192,166,200,100	192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,160 192,162,200,160 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150 192,162,200,150	TCP	74 \$4220 + 995 [271] Seepé Min-64200 Lenné PISS-1460 SACC_PERT Toval-18105540 Tiscre 10 KS-128 74 33464 + 595 [271] Seepé Min-64200 Lenné PISS-1460 SACC_PERT Toval-181055440 Tiscre 10 KS-128 74 33462 + 445 [571] Seepé Min-64200 Lenné PISS-1460 SACC_PERT Toval-181055440 Tiscre 10 KS-128 64 199 + 30664 [837, ACC] Seepì Acchi Min-64200 Lenné PISS-1460 SACC_PERT Toval-1810535440 Tiscre 10 KS-128 69 95 + 43026 [837, ACC] Seepì Acchi Min-10 Lenné 74 40900 - 139 [571] Seepè Min-64200 Lenné PISS-1460 SACC_PERT Toval-1810535440 Tiscre 10 KS-128 74 40900 - 139 [571] Seepè Min-64200 Lenné PISS-1460 SACC_PERT Toval-1810535440 Tiscre 10 KS-128 74 60900 - 130 [571] Seepè Min-64200 Lenné PISS-1460 SACC_PERT Toval-1810535440 Tiscre 10 KS-128 74 60904 - 130 [571] Seepè Min-64200 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 75 40904 - 130 [571] Seepè Min-64200 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 75 40904 - 100 [571] Seepè Min-64200 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 75 54908 - 800 [570] Seepè Min-6420 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 76 5474 - 4475 [571] Seepè Min-6420 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 76 4455 - 330 Seepè Min-6420 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 76 4455 - 330 Seepè Min-6420 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 76 5474 - 4475 [571] Seepè Min-6420 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128 76 5475 - 4487 [571] Seepè Min-6420 Lenné PISS-1460 SACC_PERT Toval-181053540 Tiscre 10 KS-128
43 36,776231880 192,165,200,100 44 35,77633616 192,165,200,100 45 36,77635650 192,165,200,100 45 36,77645520 192,165,200,100 47 36,7764520 192,165,200,150 48 36,77645201 192,165,200,150 49 36,77645201 192,165,200,100 51 36,77645201 192,165,200,100 52 36,77655201 192,165,200,100 53 36,77651201 192,165,200,100 53 36,77651201 192,165,200,100 53 36,77651201 192,165,200,100 53 36,77661201 192,165,200,100 53 36,77661201 192,165,200,100 53 36,77661201 192,165,200,100 53 36,77661201 192,165,200,100 53 36,77664421 192,165,200,150 53 36,776649421 192,165,200,150 53 36,776694922 192,165,200,150	102,162,200,150 102,162,200,150	TCP	74 \$4220 • 995 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-18035401 TSccr-0 MS-128 74 31642 • 445 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-18035401 TSccr-0 MS-128 74 31642 • 445 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-18035440 TSccr-0 MS-128 64 1991 • 90642 [657], ACK] Seep1 Ack-1 Min-9 Len-0 69 995 • 94022 [657], ACK] Seep1 Ack-1 Min-9 Len-0 74 45990 • 139] [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 74 45990 • 139] [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 74 133064 · 131 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 74 45954 • 131 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 74 45954 • 131 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 74 15954 • 960 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 75 15954 • 960 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 75 15954 • 960 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 75 15954 • 967 [2771] Seep@ Min-64220 Len-0 PKS-1460 SACK_PERI TSVal-180355440 TSccr-0 MS-128 76 5507 • 34648 [657], ACK] Seep@ Ack-1 Min-9 Len-0 76 5507 • 34648 [657], ACK] Seep@ Ack-1 Min-9 Len-0 76 5505 • 34642 [657], ACK] Seep@ Ack-1 Min-9 Len-0 76 5505 • 3604 [657], ACK] Seep@ Ack-1 Min-9 Len-0 76 5505 • 3604 [657], ACK] Seep@ Ack-1 Min-9 Len-0 76 5505 • 3604 [657], ACK] Seep@ Ack-1 Min-9 Len-0 77 5505 • 3605 •
43 36,776238880 192,165,200,100 44 36,77633616 192,165,200,100 45 36,77635664 192,165,200,100 45 36,776455264 192,165,200,100 47 36,77645264 192,165,200,100 48 36,77645264 192,165,200,150 49 36,77645264 192,165,200,100 51 36,77645264 192,165,200,100 51 36,776536566 192,165,200,100 52 36,776536566 192,165,200,100 53 36,776536575 192,165,200,100 55 36,77654724 192,165,200,100 55 36,77654724 192,165,200,100 55 36,77654724 192,165,200,100 55 36,77664942 192,165,200,150 55 36,77664942 192,165,200,150 55 36,77664942 192,165,200,150	102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_150 102_160_200_160	TO TOP TOP TOP TOP TOP TOP TOP TOP TOP T	74 \$4220 + 995 [2771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 74 33464 + 445 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 74 33462 + 445 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 64 199 + 30624 [857, ACC] Seepì Acchi Min-81 Lenné 64 199 + 30624 [857, ACC] Seepì Acchi Min-81 Lenné 74 40900 + 139 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 74 40900 + 139 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 74 40900 + 139 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 74 60954 + 130 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 74 60954 + 130 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-81035440 TSCC-rei MS-128 75 40954 + 100 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 75 45954 + 4095 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 75 45954 + 4095 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 5134 + 447 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 4455 + 30914 [557, ACC] Seepà Acchi Min-98 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 5134 + 447 [5771] Seepé Min-64220 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 4355 + 40914 [557, ACC] Seepà Acchi Min-98 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 5136 + 40914 [557, ACC] Seepà Acchi Min-98 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 5136 + 40914 [557, ACC] Seepà Acchi Min-98 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128 76 5136 + 40914 [557, ACC] Seepà Acchi Min-98 (enné PISS-1469 SACC, PERT TSVA1-810355440 TSCC-rei MS-128
43 36,776231863 192,165,200,100 44 35,77633616 192,165,200,100 45 36,77635650 192,165,200,100 45 36,77645520 192,165,200,100 47 36,7764520 192,165,200,150 48 36,7764520 192,165,200,150 49 36,7764520 192,165,200,150 53 36,7764520 192,165,200,100 53 36,7765520 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7766120 192,165,200,100 53 36,7766120 192,165,200,100 53 36,7766120 192,165,200,150 53 36,776649421 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160	TO TOP TOP TOP TOP TOP TOP TOP TOP TOP T	74 \$4220 • 995 [277] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVal-181055440 TSCC-rel MS-128 74 33462 • 445 [277] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVal-181055440 TSC-rel MS-128 74 33942 • 445 [277] Seepé Min-64220 Lenné PISS-1460 SACC, PERI TSVal-181055440 TSC-rel MS-128 69 199 • 59624 [657] ACC) Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 69 199 • 59624 [657] ACC) Seepì Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 4990 • 139 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 4990 • 139 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 4990 • 130 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 4994 • 130 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 4994 • 130 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 1994 • 137 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 69 527 • 34044 [657] ACC) Seepè Acci Min-6420 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 15354 • 475 [577] Seepè Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 15354 • 475 [577] Seepè Acci Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 15354 • 475 [577] Seepè Acci Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 15354 • 475 [577] Seepè Acci Min-64220 Lenné PISS-1460 SACC, PERI TSVal-1810535440 TSC-rel MS-128 74 15354 • 45909 [577], ACC) Seepè Acci Min-972 Lenné PISS-1460 SACC, PERI TSVal-181045340 TSC-rel MS-128 61 143 • 33908 [657], ACC) Seepè Acci Min-972 Lenné PISS-1460 SACC, PERI TSVal-1810453406 TSC-rel MS-13053440 US-64 61 143 • 33908 [657], ACC) Seepè Acci Min-972 Lenné PISS-1460 SACC, PERI TSVal-181045040 SEEPÈ MS-14640 MS-6440 SEEPÈ MS-6440 SE
43 36,776233830 102,165,200,100 44 36,776336161 02,165,200,100 45 36,77635664 102,165,200,100 45 36,77645564 102,165,200,100 47 36,77645564 102,165,200,100 48 36,77645564 102,165,200,150 49 36,77645564 102,165,200,150 53 36,77645564 102,165,200,100 53 36,77655621 102,165,200,100 53 36,77655621 102,165,200,100 53 36,776551221 102,165,200,100 53 36,77657121 102,165,200,100 53 36,77657121 102,165,200,100 53 36,77657122 102,165,200,100 53 36,77657122 102,165,200,100 53 36,77665422 102,165,200,150 53 36,77665640 102,165,200,150 53 36,77665640 102,165,200,150 53 36,7766640 102,165,200,150 53 36,7766640 102,165,200,150 53 36,7766640 102,165,200,150 53 36,7766640 102,165,200,150 63 36,7766640 102,165,200,150 63 36,7766640 102,165,200,150	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160	TO T	74 \$4224 - 995 [271] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-1803540 Tiscrné Mis-128 74 33464 - 945 [271] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 33462 - 445 [271] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 64 199 - 90064 [457, ACX] Seepì Ack-I Mine Lenné 64 199 - 90064 [457, ACX] Seepì Ack-I Mine Lenné 74 40000 - 130 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 40000 - 130 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 40004 - 130 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 60004 - 130 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 50024 - 55 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 50024 - 55 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 50034 - 147 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 51354 - 447 [571] Seepé Mine6220 Lenné 1953-1469 SACC_PERT Toval-18035440 Tiscrné Mis-128 74 4555 - 40014 [557] ACX] Seepé Ack-Mine9 Lenné 74 455 - 40014 [557] ACX] Seepé Ack-Mine9 Lenné 74 455 - 40014 [557] ACX] Seepé Ack-Mine9 Lenné 74 455 - 40014 [557] ACX] Seepé Ack-Mine9 Lenné 74 455 - 40014 [457] ACX] Seepé Ack-Mine9 Lenné 74 119 - 44096 [771], ACX] Seepé Ack-Mine9 Lenné 74 119 - 44096 [771], ACX] Seepé Ack-Mine9 Lenné 74 139 - 44096 [771], ACX] Seepé Ack-Mine9 Lenné 74 25 - 40002 [771] ACX] Seepé Ack-Mine9 Lenné 74 25 - 4002 [771] ACX] Seepé Ack-Mine9 Lenné
43 36,776238880 192,165,200,100 44 35,776336510 192,165,200,100 45 36,77635650 192,165,200,100 45 36,77645520 192,165,200,100 47 36,7764520 192,165,200,150 48 36,7764520 192,165,200,150 49 36,7764520 192,165,200,150 53 36,7764520 192,165,200,100 53 36,7765520 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,150 53 36,77664421 192,165,200,150 53 36,776649421 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776696942 192,165,200,150 63 36,776696942 192,165,200,150 63 36,776696942 192,165,200,150 63 36,776696942 192,165,200,150	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160	TO T	74 \$4224 • 995 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 33642 • 445 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 33642 • 445 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 64 1991 • 59052 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 65 1991 • 59052 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 49094 • 139 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 49094 • 139 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 69052 • 25 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 49054 • 130 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 19054 • 130 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 75 1908 • 900 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 75 1908 • 900 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 76 1908 • 900 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 76 1908 • 900 [277] Seque MS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 77 1908 • 900 [277] Seque MS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 78 1908 • 900 [277] Seque MS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 79 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=18055440 SACC_PERI TSVal=18055440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=18055440 SACC_PERI TSVal=18055440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] A
43 36,776233830 102,165,200,100 44 36,776336161 02,165,200,100 45 36,77635664 102,165,200,100 45 36,77645564 102,165,200,100 47 36,77645564 102,165,200,150 48 36,776455261 102,165,200,150 58 36,776455261 102,165,200,100 58 36,776455261 102,165,200,100 58 36,77655221 102,165,200,100 58 36,77655221 102,165,200,100 58 36,77655221 102,165,200,100 58 36,77655221 102,165,200,100 58 36,77655221 102,165,200,100 58 36,77654521 102,165,200,100 58 36,77665422 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77664042 102,165,200,150 58 36,77669642 102,165,200,150 58 36,77669642 102,165,200,150 58 36,77669642 102,165,200,150 58 36,77669642 102,165,200,150	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160	TO T	74 \$4220 + 995 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TOVAL-1803540 TSCCCT-0 MS-128 74 33464 + 945 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TOVAL-18035440 TSCCCT-0 MS-128 74 39362 + 445 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035440 TSCCCT-0 MS-128 64 199 + 90624 [857, ACX] Sequi Ack-1 Mine0 Lenne 64 995 + 9422 [857, ACX] Sequi Ack-1 Mine0 Lenne 74 40900 + 139 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-180355440 TSCCCT-0 MS-128 74 40900 + 139 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-180355440 TSCCCT-0 MS-128 74 40900 + 130 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-180355440 TSCCCT-0 MS-128 74 40904 + 130 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-180355440 TSCCCT-0 MS-128 74 5722 + 53 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-180355440 TSCCCT-0 MS-128 74 5722 + 53 [2771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-180355440 TSCCCT-0 MS-128 74 5724 + 4864 [457] ACX] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 75 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 75 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 75 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 76 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 76 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 76 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 77 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 77 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 77 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 77 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT TSVAL-18035540 TSCCCT-0 MS-128 77 1575 + 4875 [5771] Seque Mine6220 (enne) NSS-1460 SACC_PERT
43 36,776238880 192,165,200,100 44 35,776336510 192,165,200,100 45 36,77635650 192,165,200,100 45 36,77645520 192,165,200,100 47 36,7764520 192,165,200,150 48 36,7764520 192,165,200,150 49 36,7764520 192,165,200,150 53 36,7764520 192,165,200,100 53 36,7765520 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,100 53 36,7765120 192,165,200,150 53 36,77664421 192,165,200,150 53 36,776649421 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776694921 192,165,200,150 53 36,776696942 192,165,200,150 63 36,776696942 192,165,200,150 63 36,776696942 192,165,200,150 63 36,776696942 192,165,200,150	102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,150 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160 102,162,200,160	TO T	74 \$4224 • 995 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 33642 • 445 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 33642 • 445 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 64 1991 • 59052 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 65 1991 • 59052 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 49094 • 139 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 49094 • 139 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 69052 • 25 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 49054 • 130 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 74 19054 • 130 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 75 1908 • 900 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 75 1908 • 900 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 76 1908 • 900 [277] Seque Mine6220 Lene PISS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 76 1908 • 900 [277] Seque MS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 77 1908 • 900 [277] Seque MS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 78 1908 • 900 [277] Seque MS-1469 SACC_PERI TSVal=18055440 TSccree MS-128 79 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=18055440 SACC_PERI TSVal=18055440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=18055440 SACC_PERI TSVal=18055440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] ACX Seque Accid Mine570 Lene PISS-1469 SACC_PERI TSVal=1804993460 TSccree 180555440 US-64 8 1909 [277] A

Nei pacchetti non è presente nessuna richiesta HTTP, come GET o POST, quindi è chiaro che l'attività non è stata effettuata tramite un browser. È Confermata che la scansione è stata avviata con un comando nmap, nmap -sT -Pn -p 80,443, per sondare le porte 80 e 443. Il traffico ARP presente indica che la macchina attaccante ha effettuato una risoluzione automatica degli indirizzi MAC, comportamento standard durante una scansione di rete. E poco dopo nmap -sT -Pn -p 0,1023 per uno scan esclusivo su queste porte (note). Deve essere per forza -sT perchè altrimenti non completerebbe la "handshake". -Pn perchè tratta tutte le connessioni come attive e non ci sono pacchetti icmp. Nmap invia pacchetti ICMP (ping), TCP SYN o ARP per determinare se un host è attivo prima di iniziare una scansione delle porte (hence why it can't be without -Pn)



Il traffico catturato evidenzia una velocità elevata delle connessioni, suggerendo l'uso di una scansione in modalità T4 (alta velocità. a me risulta identico uno scan con nmap -T4 Ma non siamo nel pc dell'attacante). Questo comportamento è tipico di nmap, che cerca di bilanciare velocità ed evasione dai sistemi di difesa. Inoltre, l'assenza di richieste (Get) per ottenere informazioni sui protocolli (come accadrebbe con il comando -sV) conferma che si tratta di una semplice scansione delle porte note (0-1023) senza ulteriori dettagli sui servizi

60 36.776905004	192.168.200.150	192.168.200.100	TCP	60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36.776905043	192.168.200.150	192.168.200.100	TCP	74 25 + 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1
62 36.776905082	192.168.200.150	192.168.200.100	TCP	60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36.776905123	192.168.200.150	192.168.200.100	TCP	74 53 + 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1
64 36.776905162	192.168.200.150	192.168.200.100	TCP	60 500 → 54898 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
65 36.776914772	192.168.200.100	192.168.200.150	TCP	66 33042 + 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810
66 36.776941020	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810
67 36.776962320	192.168.200.100	192.168.200.150	TCP	66 60632 + 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810
68 36.776983878	192.168.200.100	192.168.200.150	TCP	66 37282 + 53 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=810
69 36.777118481	192.168.200.150	192.168.200.100	TCP	60 487 → 51534 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
70 36.777143014	192.168.200.100	192.168.200.150	TCP	74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
71 36.777186821	192.168.200.100	192.168.200.150	TCP	74 35638 - 436 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK
72 36.777302991	192.168.200.100	192.168.200.150	TCP	74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK PR
73 36.777337934	192.168.200.100	192.168.200.150	TCP	74 49780 + 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK P
74 36.777430632	192.168.200.150	192.168.200.100	TCP	60 707 → 56990 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
75 36.777430741	192.168.200.150	192.168.200.100	TCP	60 436 → 35638 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
76 36.777473018	192.168.200.100	192.168.200.150	TCP	74 36138 → 580 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK
77 36.777522494	192.168.200.100	192.168.200.150	TCP	74 52428 + 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
78 36.777623082	192.168.200.150	192.168.200.100	TCP	60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149	192.168.200.150	192.168.200.100	TCP	60 78 → 49780 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
80 36.777645027	192.168.200.100	192.168.200.150	TCP	74 41874 → 764 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 SACK
81 36.777680898	192.168.200.100	192.168.200.150	TCP	74 51506 + 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK I
82 36.777758636	192.168.200.150	192.168.200.100	TCP	60 580 → 36138 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
83 36.777758696	192.168.200.150	192.168.200.100	TCP	60 962 + 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36.777871245	192.168.200.150	192.168.200.100	TCP	60 764 → 41874 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
85 36.777871293	192.168.200.150	192.168.200.100	TCP	60 435 → 51506 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
86 36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 + 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSV
87 36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 → 139 [RST, ACK] Seg=1 Ack=1 Win=64256 Len=0 TSV
88 36.777986759	192.168.200.100	192.168.200.150	TCP	66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
89 36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 + 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
90 36.778179978				
	192.168.200.100	192.168.200.150	TCP	74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_I
	192.168.200.100 192.168.200.100	192.168.200.150 192.168.200.150	TCP TCP	74 51450 + 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 48448 + 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161				_
91 36.778200161 92 36.778307830	192.168.200.100	192.168.200.150	TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 <b>93 36.778385846</b>	192.168.200.100 192.168.200.100	192.168.200.150 192.168.200.150	TCP TCP	74 48448 + 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948	192.168.200.100 192.168.200.100 192.168.200.150	192.168.200.150 192.168.200.150 <b>192.168.200.100</b>	TCP TCP TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494	192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100	TCP TCP TCP TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494 96 36.778482791	192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100	TCP TCP TCP TCP TCP	74 48448 + 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494 96 36.778482791 97 36.778591226	192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100	TCP TCP TCP TCP TCP TCP	74 48448 + 886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 886 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494 96 36.778482791 97 36.778591226 98 36.778614095	192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150	TCP TCP TCP TCP TCP TCP TCP TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.77849494 96 36.778492791 97 36.778591226 98 36.778614095 99 36.778663064	192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150	TCP TCP TCP TCP TCP TCP TCP TCP TCP	74 48448 + 886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 886 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 93 36.778385948 94 36.778345948 95 36.778449494 96 36.77861299 97 36.778614095 99 36.778663064 100 36.778721080	192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494 96 36.77842791 97 36.778591226 98 36.778614095 99 36.778621080 101 36.778759636	192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP	74 48448 + 886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 + 1807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 1007 + 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 206 + 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 40318 + 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494 96 36.778492791 97 36.778591226 98 36.778614095 99 36.778614095 100 36.778759636 102 36.778759636	192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP TCP TCP TCP TCP TCP TCP TCP TCP	74 48448 + 886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 + 1807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 286 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 1007 + 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 206 + 36466 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 40318 + 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 93 36.778385846 94 36.778385948 95 36.778449494 96 36.77851226 99 36.77861296 99 36.77861206 101 36.778721880 101 36.77879636 102 36.778781327	192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP	74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 886 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 131 → 54202 [RST, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
91 36.778200161 92 36.778307830 93 36.778385948 94 36.778385948 95 36.778449994 96 36.77861995 98 36.778614995 99 36.778663064 100 36.778721080 101 36.77879636 102 36.778781327 103 36.778826294	192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP	74 48448 + 886 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0 74 42420 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 1007 + 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 206 + 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 40318 + 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 51276 + 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
91 36.778200161 92 36.778307830 93 36.778385948 95 36.778489494 96 36.778482791 97 36.778591226 98 36.778614095 99 36.778663064 100 36.778759636 101 36.778759636 102 36.778781327 103 36.778826394 104 36.77886493 105 36.7788939327	192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	192.168.200.150 192.168.200.150 192.168.200.100 192.168.200.100 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150 192.168.200.150	TCP	74 48448 + 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54566 + 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 148 + 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 806 + 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 221 + 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 42420 + 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 34646 + 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 74 54202 + 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 1007 + 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 60 206 + 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 40318 + 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 75 1276 + 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 131 + 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 74 39566 + 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_ 60 131 + 54202 [RST, ACK] Seq=0 Win=64240 Len=0 MSS=1460 SACK_

Le risposte RST (reset) frequenti e ravvicinate sono messe in evidenza in rosso da Wireshark, segnalando potenzialmente un comportamento sospetto. Tuttavia, il fatto che le connessioni vengano chiuse in modo regolare e in successione veloce si capisce che non è un attacco "diretto" (specifico ad una porta, altrimenti vedrei sempre tentativi sulla stessa).

Come rimedio, è consigliabile bloccare il traffico verso le porte che non sono strettamente necessarie per il funzionamento del server e applicare filtri firewall per limitare l'accesso alle sole macchine autorizzate. È inoltre utile configurare un sistema di monitoraggio che rilevi tentativi di scansione o attività anomale, oltre a implementare meccanismi di rate-limiting per prevenire eventuali abusi. Infine, è sempre buona pratica monitorare e pulire periodicamente la cache ARP per evitare problemi legati alle informazioni residue lasciate da scansioni simili.

Inoltre Se abbiamo preso i MAC "Address" di ogni pc aziendale, sappiamo a chi appartiene e possiamo andare direttamente da lui e capire se è stato infettato (o e lui) ed isolarlo\* (Prevention, sapremo già se l'attacante sta usando un computer aziendale e anche di chi è) altrimenti possiamo anche staccare il wi-fi ( per comprendere se l'attacco è sulla rete fissa aziendale o dall'esterno tramite rete wireless aziendale, ovviamente in congruenza con il Business Continuity.) Quando possibile.

## CONCLUSIONE

Il traffico analizzato non evidenzia un attacco DoS o DDoS, Mitm(arp poisoning), Backdoor(Reverse tcp o altre minaccie). Possiamo appurare che l'attacante ha effettuato uno scan da un computer sulla nostra rete locale con un tool come nmap o l'equivalente di questo comando <nmap -sT -Pn -p 0,1023> facendo uno scan sulle porte note in modo veloce. è un'attività di ricognizione tramite scansione delle porte note e sebbene non rappresenti una minaccia diretta, questo tipo di comportamento deve essere monitorato e bloccato per prevenire escalation o attacchi futuri.

# Recap

#### Scan di nmap con:

- -sT 100% perchè negli altri modi tipo sS non completerebbe l'handshake
- (-sT syn,syn/ack,ack-rst/ack o syn) Completa (-sS syn,syn/ack-rst/ack non completando l'handshake "half open")
- -sV non è possibile perchè non sono presenti richieste di GET per le versioni dei protocolli (Non potrà sfruttare vulnerabilità dovute a versioni non aggiornate, che comunque non dovrebbe accadere in primis e bisogna sempre tenere tutto aggiornato)
- -Pn 100% perchè non ci sono richieste icmp per verificare l'host se è attivo <host discovery> (icmp echo request also known as "Ping")
- e -p 0,1023 100% (più specifico) perchè l'attacante fa uno scan solamente delle porte note mirato.
- --top-ports 1023 o anche -p- non possono essere: --top-ports 1023 scansionerebbe le 1023 porte più comuni in base al database interno di Nmap (nmap-services), che ordina le porte in base alla loro frequenza di utilizzo. Questo potrebbe includere porte sparse su tutto il range (0-65535), non limitandosi solo alle prime 1023.
- -p- non avrebbe riguardo, farebbe una ricerca completa (0-65535)