

Progetto di Rete e Report di Implementazione e Test per THETA s.r.l.

Introduzione

Il presente report illustra la progettazione, l'implementazione e il collaudo della nuova infrastruttura di rete interna per l'azienda Theta S.r.l. L'obiettivo principale era quello di modernizzare e centralizzare l'infrastruttura esistente, migliorando l'efficienza operativa, la sicurezza e la scalabilità futura.

Nonostante la complessità dell'intervento, il progetto è stato completato con successo, includendo anche funzionalità aggiuntive come il subnetting personalizzato e strumenti software sviluppati in Python per l'analisi della rete.

1. Specifiche dell'Infrastruttura di Rete

In risposta a tale esigenza, è stato intrapreso un progetto di implementazione di una rete interna basata sulle seguenti specifiche:

- 120 postazioni di lavoro, suddivise equamente su sei piani (20 per piano).
- Uno switch dedicato per ogni piano, connesso a un router centrale.
- Router centrale che gestisce l'interconnessione tra i sei switch e funge da punto di smistamento del traffico.
- Tre IDS/IPS fisici, collocati ogni due switch, per la rilevazione e prevenzione delle intrusioni.
- Server NAS collocato al primo piano per archiviazione e condivisione centralizzata dei dati.
- Firewall perimetrale collegato al router, per la protezione da minacce esterne.
- Modem collegato al firewall per l'accesso a Internet.

Subnetting dedicato: schema IP tipo 10.0.X.0/23 con gateway 10.0.X.1 per ogni piano.

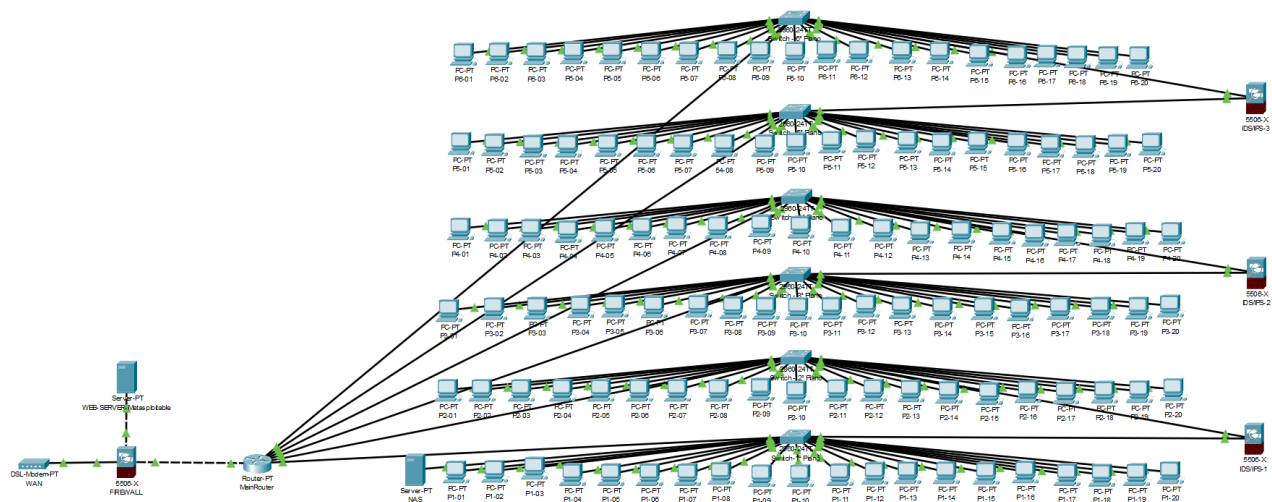
Per quanto riguarda l'analisi della sicurezza della rete esterna simulata, è stata sviluppata internamente tramite linguaggio Python una suite di strumenti. Questa include programmi per:

- Eseguire la scansione delle porte aperte sul server Metasploitable.
- Identificatore comandi per la pagina di gestione phpMyAdmin ospitata sul server Metasploitable è in grado di accettare.

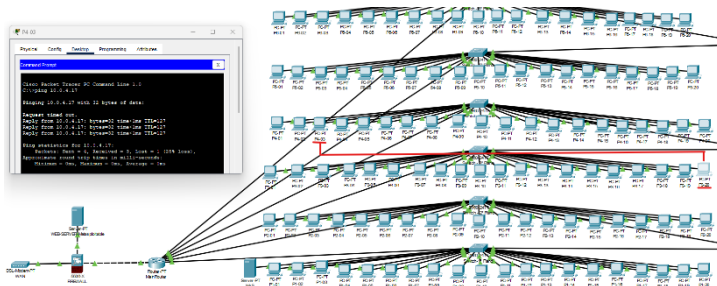
I dettagli tecnici di questi strumenti e i risultati delle analisi saranno presentati in una sezione dedicata del presente report.

2. Architettura della Rete Implementata

Rete Interna (Topologia a Stella Estesa) Firewall perimetrale → Router centrale → Switch di piano → Postazioni di lavoro



Per simulare una DMZ (Demilitarized Zone), è stata implementata una rete esterna contenente un server web (IP: 192.168.20.10) basato su Metasploitable. Questo server simula un servizio pubblico accessibile tramite Internet ed è protetto da un firewall esterno dedicato. Il firewall esterno controlla il traffico in entrata e in uscita verso il



server web, applicando policy di sicurezza specifiche per i servizi esposti. Questa separazione architetturale garantisce che la rete esterna simulata (e il server web) siano logicamente distinti e isolati dalla rete interna del cliente, prevenendo potenziali impatti sulla rete aziendale durante le attività di test e analisi di sicurezza.

(Test di ping tra un pc del 4° piano con uno del 3° – immagine a sinistra)

La rete interna del cliente è stata progettata con una topologia centralizzata a stella estesa, dove un router centrale funge da fulcro per l'interconnessione dei vari segmenti di rete.

La comunicazione con il mondo esterno è gestita attraverso una connessione WAN protetta da un firewall perimetrale. Il flusso del traffico dati, dall'esterno verso l'interno, segue il seguente percorso logico:

Rete WAN: La connessione a Internet è stabilita tramite una rete WAN (Wide Area Network) fornita da un provider di servizi.

Firewall Perimetrale: Il traffico proveniente dalla rete WAN transita attraverso un firewall perimetrale dedicato. Questo dispositivo analizza il traffico in base a policy di sicurezza configurate per proteggere la rete interna da accessi non autorizzati e minacce esterne. Il firewall è direttamente connesso al router centrale – e filtra tutti i pacchetti in entrata di uscita.

Router Centrale: Il router centrale riceve il traffico dal firewall e lo instrada verso le diverse sottoreti interne. Agisce anche come punto di interconnessione per i sei switch di piano. A livello di infrastruttura, ogni porta **GigabitEthernet** del router è stata configurata con un indirizzo IP statico appartenente alla relativa Subnet e collegata direttamente allo switch di piano. Questa configurazione consente la separazione fisica e logica del traffico di rete tra i diversi piani o reparti.

Lo abbiamo configurato tramite il CLI come si può evincere da screenshot a destra, tramite i comandi:

```
Router(config)#interface GigabitEthernet6/0
Router(config-if)#ip address 10.0.10.1 255.255.254.0
Router(config-if)#ip helper-address 10.0.0.2
Router(config-if)#no shutdown
```



```
Router(config)#interface Gi
Router(config)#interface GigabitEthernet4/0
Router(config-if)#ip address 10.0.6.1 255.255.254.0
Router(config-if)#ip helper-address 10.0.0.2
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Gi
Router(config)#interface GigabitEthernet5/0
Router(config-if)#ip address 10.0.8.1 255.255.254.0
Router(config-if)#ip helper-address 10.0.0.2
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Gi
Router(config)#interface GigabitEthernet6/0
Router(config-if)#ip address 10.0.10.1 255.255.254.0
Router(config-if)#ip helper-address 10.0.0.2
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface GigabitEthernet4/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet4/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet5/0
Router(config-if)#
```

IP Configuration	
IPv4 Address	10.0.2.1
Subnet Mask	255.255.254.0

Switch per piano: Un totale di sei switch di rete, uno per ciascun piano dell'edificio, sono collegati al router centrale tramite connessioni cablate.

Ogni switch gestisce la connettività locale di 20 postazioni di lavoro presenti sul rispettivo piano.

Subnetting: Le 120 postazioni di lavoro sono distribuite uniformemente sui sei piani (20 per piano). Ogni PC è configurato con un indirizzo IP DHCP appartenente alla sottorete specificata nel Server del primo piano. Lo schema di indirizzamento IP segue il pattern 10.0.X.Y/23, dove X identifica il piano (X=0-2-4-6-8-10). La segmentazione logica è ottenuta tramite l'implementazione di una subnetting dedicata per ciascun piano. Per la rete 10.0.0.0/23 è stato assegnato il gateway 10.0.0.1, primo indirizzo disponibile della Subnet, secondo le convenzioni standard di rete, inoltre questo IP permette un'espansione futura all'azienda di un massimo di 510 host.

IDS/IPS: Tre sistemi fisici, uno per ogni due switch, di Intrusion Detection and Prevention sono strategicamente posizionati nella rete interna per monitorare e, potenzialmente, prevenire attività sospette o dannose. Agisce in modalità **inline**, intercettando il traffico prima che raggiunga la destinazione.

I vantaggi di questa implementazione sono:

- Prestazioni **elevate** grazie a risorse dedicate.
- **Minore latenza** rispetto a soluzioni virtuali o software-based.
- **Affidabilità e robustezza**, adatte ad ambienti enterprise.
- **Facilità di integrazione** in architetture di rete complesse

Server NAS: Un server Network Attached Storage è situato al primo piano ed è connesso allo switch del primo piano. La segmentazione logica della rete è stata realizzata attraverso l'implementazione di Subnet dedicate per ciascun piano dell'edificio. Ogni Subnet è stata progettata per garantire isolamento, sicurezza e gestione efficiente del traffico, utilizzando uno schema di indirizzamento IP strutturato (es. 10.0.X.0/23). Il server NAS è configurato per essere accessibile in lettura e scrittura da tutte le postazioni di lavoro autorizzate presenti nei diversi piani, tramite il Routing gestito dal router centrale. Il server aziendale, connesso alla rete centrale, è stato configurato per svolgere il ruolo di **DHCP Server**. Questo consente l'assegnazione automatica degli indirizzi IP a tutti i dispositivi presenti su ciascuna Subnet, garantendo coerenza nell'indirizzamento, riduzione degli errori manuali e facilità di gestione centralizzata.

In questo modo, la rete risulta **scalabile, ordinata e sicura**, permettendo un'espansione agevole e un controllo preciso delle risorse distribuite nei diversi segmenti, anche per espansioni future.

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 10.0.0.1

DNS Server: 0.0.0.0

Start IP Address: 10 0 0 10

Subnet Mask: 255 255 254 0

Maximum Number of Users: 502

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool6	10.0.10.1	0.0.0.0	10.0.10.10	255.255....	502	0.0.0.0	0.0.0.0
serverPool5	10.0.8.1	0.0.0.0	10.0.8.10	255.255....	502	0.0.0.0	0.0.0.0
serverPool4	10.0.6.1	0.0.0.0	10.0.6.10	255.255....	502	0.0.0.0	0.0.0.0
serverPool3	10.0.4.1	0.0.0.0	10.0.4.10	255.255....	502	0.0.0.0	0.0.0.0
ServerPool2	10.0.2.1	0.0.0.0	10.0.2.10	255.255....	502	0.0.0.0	0.0.0.0
serverPool	10.0.0.1	0.0.0.0	10.0.0.10	255.255....	502	0.0.0.0	0.0.0.0

3. Strumenti Software Sviluppati

In questa sezione, vengono presentati il funzionamento e le finalità degli strumenti software sviluppati internamente in Python per l'analisi di sicurezza del server web Metasploitable (IP: 192.168.20.10), situato nella rete esterna simulata.

Software della scansione delle aperte

Script "myPortScanner.py" - Lo script esegue una scansione TCP delle porte su un host specificato. Richiede come input l'IP del target, la porta iniziale e finale del range da scansionare. Per ogni porta nel range valido (1-65535), tenta una connessione utilizzando `socket.connect_ex()`. Se la connessione ha successo (status 0), la porta è considerata aperta e viene aggiunta alla lista `open_port_list`.

Al termine della scansione, viene stampata la lista delle porte aperte.

- Funzione `port_valid(port):`
Verifica se una porta è compresa tra 1 e 65535.
- Variabili principali:
`ip_target`, `low_port`, `high_port`, `open_port_list`, `status`.

Resultati del test → (vedi screenshot)

```

1 myPortScanner.py
2 import socket
3 # controlla se la porta inserita sono valide
4 def port_valid(port):
5     if not(0 <= port <= 65535):
6         return False
7     return True
8
9 ip_target = input("Inserisci ip target: ")
10
11 while True:
12     try:
13         low_port = int(input("Inserisci porta di partenza: "))
14         if not port_valid(low_port): # se l'input e' invalido ripeti il ciclo
15             print("porta invalida, riprovare")
16             continue
17         high_port = int(input("Inserisci porta finale: "))
18         if not port_valid(high_port):
19             print("porta invalida, riprovare")
20             continue
21         # se l'input e' valido l'esecuzione arriva qui e stoppa il ciclo
22         break
23     except ValueError:
24         print("Inserire solo numeri interi\n")
25
26 open_port_list = []
27
28 print("Inizieremo la scansione di ", ip_target, " da porta ", low_port, " a porta ", high_port)
29
30 for port in range(low_port, high_port + 1):
31     sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
32     status = sock.connect_ex((ip_target, port))
33
34     if status == 0:
35         print("porta (port) = APERTA")
36         open_port_list.append(port)
37     else:
38         print("porta (port) = CHIUSA")
39
40 sock.close()
41
42 print("\nRIEPILOGO DELLE PORTE APERTE")
43 for port in open_port_list:
44     print(port)
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245

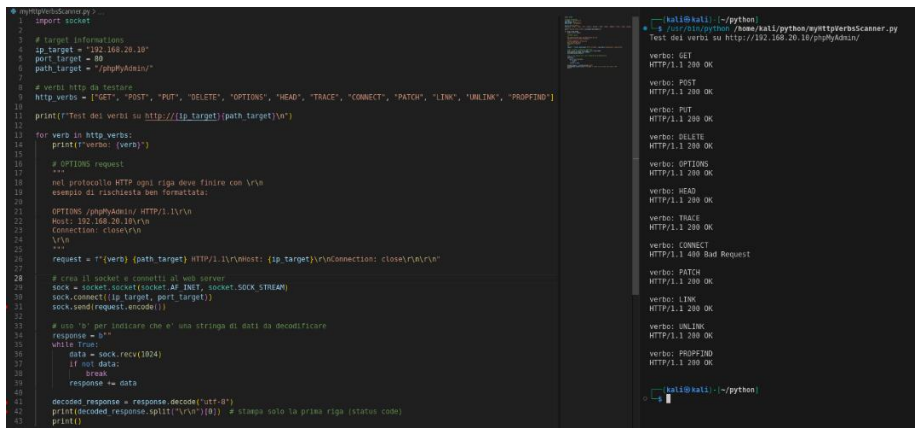
```

Software dei Verbi http (GET, POST, PUT, DELETE) - "myHttpVerbsScanner.py"

Lo script in questione testa diversi metodi HTTP su un web server specificato. Prende in input l'IP del target, la porta (default 80) e il percorso della risorsa. Per ogni verbo nella lista http_verbs, costruisce e invia una richiesta HTTP tramite un socket TCP. Riceve la risposta del server e ne stampa la prima riga (lo status code HTTP), indicando se il metodo è supportato, bloccato, ecc.

- Variabili principali:
ip_target, port_target,
path_target,
http_verbs, request,
response,
decoded_response.

Resultati dei test →
(vedi screenshot)



```
1 import socket
2
3 # Target information
4 ip_target = "192.168.20.10"
5 port_target = 80
6 path_target = "/"
7
8 # Verbi http da testare
9 http_verbs = ["GET", "POST", "PUT", "DELETE", "OPTIONS", "HEAD", "TRACE", "CONNECT", "PATCH", "LINK", "UNLINK", "PROPFIND"]
10
11 print(f"Test dei verbi su http://{ip_target}:{port_target}/{path_target}")
12
13 for verbo in http_verbs:
14     print(f"Verbo: {verbo}")
15
16     # OPTIONS request
17     """
18     nel protocollo HTTP ogni riga deve finire con \r\n
19     esempio di richiesta non formattata:
20     OPTIONS /phpmyAdmin/ HTTP/1.1\r\n
21     Host: 192.168.20.10\r\n
22     Connection: close\r\n
23     \r\n
24     """
25     request = f"({verbo}) {path_target} HTTP/1.1\r\nHost: {ip_target}\r\nConnection: close\r\n\r\n"
26
27     # crea il socket e connetti al web server
28     sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
29     sock.connect((ip_target, port_target))
30     sock.send(request.encode())
31
32     # att "b" per indicare che e' una stringa di dati da decodificare
33     response = b""
34     while True:
35         data = sock.recv(1024)
36         if not data:
37             break
38         response += data
39
40     decoded_response = response.decode('utf-8')
41     print(decoded_response.split("\r\n")[0]) # stampa solo la prima riga (status code)
42     print()
```

Script per catturare Socket di Rete - "myPacketSniffer.py".

Questo script Python è un semplice sniffer di pacchetti IP. Utilizzando un socket RAW, cattura il traffico Ethernet e analizza l'intestazione IP per visualizzare gli indirizzi di origine e destinazione di ogni pacchetto in transito sulla rete. Il programma continua a monitorare il traffico in tempo reale fino all'interruzione manuale.

Funzioni Chiave:

parse_ip_header(packet): Estrae gli IP di origine e destinazione dall'header IP.

start_sniffer(): Avvia la cattura e l'analisi dei pacchetti, gestendo anche eventuali errori.

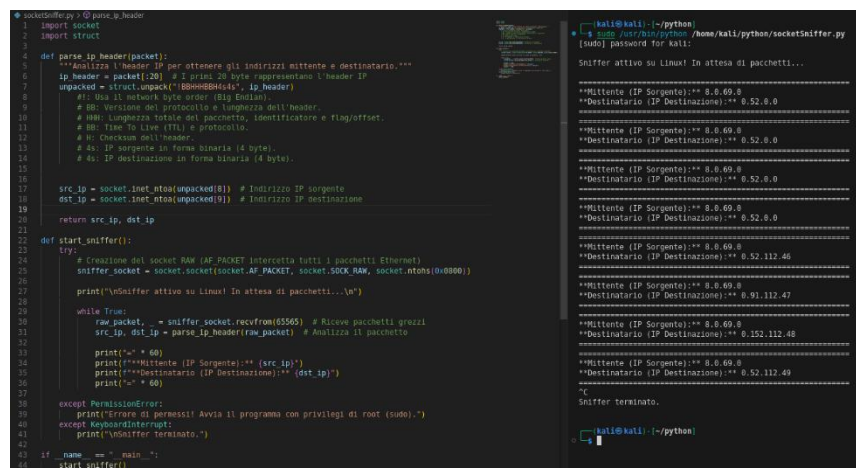
Variabili Fondamentali:

sniffer_socket: Il socket RAW per la cattura.

src_ip: IP di origine.

dst_ip: IP di destinazione.

Resultati del test → (vedi screenshot)



```
1 import socket
2 import struct
3
4 def parse_ip_header(packet):
5     """Analizza l'header IP per ottenere gli indirizzi mittente e destinatario."""
6     ip_header = packet[0:20] # I primi 20 byte rappresentano l'header IP
7     unpacked = struct.unpack("BBBBB", ip_header)
8     # Usa il network byte order (Big Endian).
9     # 0: versione del protocollo e lunghezza dell'header.
10     # 16: lunghezza totale del pacchetto, identificatore e flag/offset.
11     # 20: Time To Live (TTL) e protocollo.
12     # 24: checksum dell'header.
13     # 28: IP sorgente in forma binaria (4 byte).
14     # 32: IP destinazione in forma binaria (4 byte).
15
16     src_ip = socket.inet_ntoa(unpacked[8:12]) # Indirizzo IP sorgente
17     dst_ip = socket.inet_ntoa(unpacked[12:16]) # Indirizzo IP destinazione
18
19     return src_ip, dst_ip
20
21 def start_sniffer():
22     try:
23         # Creazione del socket RAW (AF_PACKET intercetta tutti i pacchetti Ethernet)
24         sniffer_socket = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.ntohs(0x0000))
25
26         print("\nSniffer attivo su Linux! In attesa di pacchetti...\n")
27
28         while True:
29             raw_packet, _ = sniffer_socket.recvfrom(65535) # Riceve pacchetti grezzi
30             src_ip, dst_ip = parse_ip_header(raw_packet) # Analizza il pacchetto
31
32             print(f"=====")
33             print(f"IP Sorgente: {src_ip}")
34             print(f"IP Destinazione: {dst_ip}")
35             print(f"=====")
36
37     except PermissionError:
38         print("Errore di permessi! Avvia il programma con privilegi di root (sudo).")
39     except KeyboardInterrupt:
40         print("\nSniffer terminato.")
41
42 if __name__ == "__main__":
43     start_sniffer()
```

4. Implementazioni Future

Per ottimizzare ulteriormente l'infrastruttura di rete di Theta e rafforzarne la sicurezza, si raccomandano le seguenti implementazioni future:

- Configurazione di VLAN: Fornire una segmentazione di rete più granulare per migliorare la sicurezza e l'organizzazione del traffico.
- Policy di Firewall Interne: Implementare regole di firewall più specifiche tra le sottoreti dei piani per limitare la comunicazione laterale non necessaria.
- Monitoraggio e Logging Centralizzato: Adottare un sistema per la raccolta e l'analisi centralizzata dei log di rete e di sicurezza.
- Hardening del Server Web (Metasploitable): Disabilitare i servizi non necessari (come FTP e Telnet), limitare i metodi HTTP supportati su interfacce sensibili come phpMyAdmin e applicare patch di sicurezza.
- Valutazione e Configurazione Ottimale degli IDS/IPS: Analizzare il traffico rilevato dagli IDS/IPS e affinare le regole per una rilevazione più efficace delle minacce.
- Test di Penetrazione Approfonditi: Eseguire penetration test sia sulla rete interna che sulla DMZ simulata per identificare ulteriori vulnerabilità.

Formazione sulla Sicurezza: Sensibilizzare il personale sui rischi e sulle corrette pratiche di sicurezza Informatica.

- **Campagne di sensibilizzazione ricorrenti** su phishing, social engineering, sicurezza delle password e uso consapevole delle risorse aziendali.
- **Workshop pratici** e interattivi con scenari realistici per stimolare il riconoscimento delle minacce.
- **Newsletter mensili sulla sicurezza informatica**, con consigli pratici, aggiornamenti sulle minacce e quiz per mantenere alta l'attenzione.
- **Portale interno con microlearning**: pillole formative fruibili on-demand per rafforzare le competenze.
- **Coinvolgimento attivo** dei dipendenti nella segnalazione di anomalie (es. email sospette), creando una *cybersecurity culture* distribuita.

Queste implementazioni future mirano a rendere la rete di Theta più sicura, gestibile ed efficiente nel lungo termine.

Conclusioni

L'implementazione della nuova infrastruttura di rete interna per l'azienda cliente ha raggiunto gli obiettivi prefissati, fornendo una connettività affidabile e una segmentazione logica tramite subnetting per le postazioni di lavoro suddivise su sei piani.

L'architettura a stella estesa, con un router centrale che interconnette gli switch di piano, facilita la gestione e la scalabilità della rete. La presenza di un firewall perimetrale costituisce una prima linea di difesa essenziale per la protezione della rete interna.

L'analisi preliminare della sicurezza della rete esterna simulata (DMZ) tramite gli strumenti software sviluppati internamente, ed ha fornito insights iniziali sullo stato del server web:

- **myHttpVerbsScanner.py:** Il test dei metodi HTTP sulla risorsa /phpMyAdmin/ ha indicato che, oltre ai metodi standard GET e POST, sono supportati anche i metodi HEAD, OPTIONS, PUT e DELETE. L'abilitazione di metodi come PUT e DELETE su un'interfaccia di gestione web sensibile come phpMyAdmin potrebbe comportare rischi significativi se non adeguatamente protetta.
- **myPortScanner.py:** L'esecuzione dello script ha rivelato che sul server target sono attive le porte TCP 21 (FTP), 22 (SSH), 23 (Telnet), 80 (HTTP) e 443 (HTTPS). La presenza di servizi potenzialmente non necessari come FTP e Telnet rappresenta una potenziale superficie di attacco da valutare.
- **myPacketSniffer.py:** L'analisi del traffico di rete ha permesso di osservare i pattern di comunicazione con il server Metasploitable durante i test. In particolare, sono state rilevate richieste e risposte associate ai tentativi di connessione sulle porte aperte e alle richieste HTTP con i diversi verbi.

Questi risultati iniziali evidenziano la necessità di un'analisi di sicurezza più approfondita del server web esposto e l'implementazione di misure di hardening specifiche per mitigare i rischi identificati.

In sintesi, sebbene l'infrastruttura di rete sia solida e ben configurata, le problematiche emerse a livello di sicurezza del server web necessitano di ulteriori interventi per garantire una protezione completa e ridurre le superfici di attacco.

Con l'adozione delle giuste contromisure, sarà possibile rafforzare ulteriormente la sicurezza complessiva dell'ambiente, aggiungere impostazioni mirate come la VLAN, ampliare i software di monitoraggio.



Il Team LockNet ha curato l'implementazione e il collaudo della nuova infrastruttura di rete interna per Theta Company, assicurando una connettività affidabile e sicura in linea con i nostri elevati standard di qualità e sicurezza.

Inoltre, sono stati condotti con successo vari test di funzionamento software per assicurare l'efficienza e la sicurezza del sistema.

Ringraziamo Theta Company per aver scelto **LockNet** come partner di fiducia nella protezione della loro infrastruttura IT, confermando così l'impegno della nostra azienda nell'offrire soluzioni di cybersecurity all'avanguardia e di alta qualità.

Il presente report è stato redatto dal Team LockNet, composto dai seguenti membri:

Gugliotta Stefano

Technical writer

Pasetto Matteo

Software Developer

Fabriani Anais

Project Supervisor & Presenter

Mihai Andrei

Software Developer

Rubeo Roberto

Project Coordinator & Editor