THIERRY MEYER
SÉCURITÉ INFORMATIQUE

INTRODUCTION A LA SÉCURITÉ DES PROTOCOLES RÉSEAUX
Travaux pratiques : lab n°2 – 4 heures

Manipulation des protocoles réseaux à l'aide d'outils de sécurité
Écriture d'un scanner de ports rudimentaire avec hping3 et TCL

---

1 Aperçu du lab :

A travers ce TP vous allez approfondir vos connaissances sur le scan de ports TCP en développant votre propre scanner de ports. Pour parvenir à cela vous devrez d'abord prendre en main l'outil hping3[1] et les rudiments de la syntaxe du langage Tcl[2]. Vous suivrez donc les quelques manipulations décrites sur le site officiel de hping3.

Pour réaliser ce TP vous aurez besoin de deux poste. Celui sur lequel vous développerez votre outil devra fonctionner sous Linux.

Vous travaillerez en binôme de façon totalement autonome, vous devrez donc consulter toute la documentation officielle à votre disposition pour comprendre les options que vous utiliserez et les décrire. Pour pouvoir travailler correctement vous pourrez avoir besoin d'un support vous décrivant les en-têtes des paquets de la plupart des protocoles qui vous sera fourni et d'un outil pour capturer le trafic réseau.

2 Objectifs du lab :

Ce TP a été créé avec en tête plusieurs objectifs :

- tout d'abord il est une bonne illustration des acquis théoriques vue en cours sur le scan de ports, et
- il complète parfaitement un exercice sur la manipulation de nmap ;
- ensuite il vous fait découvrir un outil, hping3 très utilisé en sécurité informatique, et qui pourra vous rendre de nombreux services sur des prestations offensives ou dans le cadre de la protection de votre système d'information.

1 *Cf http://www.hping.org/*
2 *Cf https://wiki.tcl-lang.org/*

3 Les consignes :

3.1 Manipulation du trafic réseau avec Hping3 et Tcl :

3.1.1 Présentation : (en cours)

3.1.2 Rappels théoriques sur TCP/IP :

- Expliquez en détail la technique de manipulation et d'analyse des flux réseaux couramment employée pour effectuer des scans de ports TCP.

3.1.3 Utilisation de hping3[3]:

Hping est un utilitaire de diagnostic et de sécurité réseau interfacé avec le langage de programmation Tcl[4]. Il est aussi présent sous la forme d'un outil en ligne de commande. Vous pouvez consulter la documentation et différents tutoriels sur le site officiel.

1. Découverte de l'outil :
   - Que permet de faire hping exactement ? A quelles fins est-il possible de l'utiliser ?
   - Lisez la page de documentation[5] puis suivez le mini tutoriel officiel intitulé « Getting started with hping3 »[6] pour prendre en main l'outil[7] :
     - Lisez également la rubrique concernant la syntaxe APD[8] pour comprendre comment sont représentés les paquets dans hping3 et Tcl.
     - Effectuez toutes les manipulations présentées, puis forgez quelques paquets, capturez les trames et observez le résultat. Décrivez vos manipulations.
2. Utilisation de l'outil pour la création d'un utilitaire de scan de ports TCP :
   - Vous allez maintenant approfondir vos connaissances sur Hping et Tcl en développant à l'aide de ces deux technologies un utilitaire basique de scan de ports TCP. Votre nouvel outil devra disposer des caractéristiques suivantes :
     - Il sera exécuté en ligne de commande et prendra en argument les paramètres suivants :
       - la **liste des cibles** à analyser. Il pourra s'agir d'une adresse IP, d'une liste d'adresses IP ou d'un range d'adresses IP ;
       - la **liste des ports** TCP à analyser. De la même façon que pour les adresses IP, Il pourra s'agir d'un port spécifique, d'une liste de ports ou d'un range. Si aucun port n'est spécifié, il scannera alors les 1000 ports TCP les plus couramment utilisés, dont vous trouverez la liste en annexe ;
       - Une **option -v** qui permettra de basculer en mode verbeux. Dans ce mode la commande ressortira les résultats pour l'ensemble des ports scannés. Par défaut ce mode n'est pas activé et la commande n'affiche les résultats que pour les ports ouverts ;
     - La sortie de la commande fera apparaître les informations suivantes :
       - un rappel des paramètres du scan effectué, et des cibles visées ;

3 *Cf http://www.hping.org/*
4 *Cf https://wiki.tcl-lang.org/*
5 *Cf http://www.hping.org/documentation.php*
6 *Cf http://wiki.hping.org/94*
7 *Cf https://scapy.readthedocs.io/en/latest/usage.html#interactive-tutorial*
8 *Cf http://wiki.hping.org/26*

- la liste des ports ouverts ;
- si le mode verbeux est activé (option -v), pour chaque port scanné devrons figurer les informations suivantes :
  - numéro du port,
  - état du port (ouvert, fermé ou filtré) et,
  - la raison pour laquelle le port a été qualifié de cette façon. (Par exemple : filtré parce que aucune réponse n'a été retournée par la cible.)

4 Les livrables :

A l'issue de ce TP, vous devrez me présenter vos résultats. Votre présentation devra contenir également les réponses aux éventuelles questions théoriques posées. Toutes les manipulations que vous allez faire devront être testées et vous devrez prouver leur bon fonctionnement.

La note tiendra compte de vos résultats, l'implication sur le lab, ainsi que la clarté de vos explications.

5 Annexes :

Liste des 1000 ports TCP les plus couramment utilisés :

1,3,4,6,7,9,13,17,19,20,21,22,23,24,25,26,30,32,33,37,42,43,49,53,70,79,80,81,82,83,84,85,88,89,90,99,10
0,106,109,110,111,113,119,125,135,139,143,144,146,161,163,179,199,211,212,222,254,255,256,259,264,2
80,301,306,311,340,366,389,406,407,416,417,425,427,443,444,445,458,464,465,481,497,500,512,513,514,
515,524,541,543,544,545,548,554,555,563,587,593,616,617,625,631,636,646,648,666,667,668,683,687,69
1,700,705,711,714,720,722,726,749,765,777,783,787,800,801,808,843,873,880,888,898,900,901,902,903,9
11,912,981,987,990,992,993,995,999,1000,1001,1002,1007,1009,1010,1011,1021,1022,1023,1024,1025,10
26,1027,1028,1029,1030,1031,1032,1033,1034,1035,1036,1037,1038,1039,1040,1041,1042,1043,1044,104
5,1046,1047,1048,1049,1050,1051,1052,1053,1054,1055,1056,1057,1058,1059,1060,1061,1062,1063,1064
,1065,1066,1067,1068,1069,1070,1071,1072,1073,1074,1075,1076,1077,1078,1079,1080,1081,1082,1083,
1084,1085,1086,1087,1088,1089,1090,1091,1092,1093,1094,1095,1096,1097,1098,1099,1100,1102,1104,1
105,1106,1107,1108,1110,1111,1112,1113,1114,1117,1119,1121,1122,1123,1124,1126,1130,1131,1132,11
37,1138,1141,1145,1147,1148,1149,1151,1152,1154,1163,1164,1165,1166,1169,1174,1175,1183,1185,118
6,1187,1192,1198,1199,1201,1213,1216,1217,1218,1233,1234,1236,1244,1247,1248,1259,1271,1272,1277
,1287,1296,1300,1301,1309,1310,1311,1322,1328,1334,1352,1417,1433,1434,1443,1455,1461,1494,1500,
1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687,1688,1700,1717,1718,1719,1
720,1721,1723,1755,1761,1782,1783,1801,1805,1812,1839,1840,1862,1863,1864,1875,1900,1914,1935,19
47,1971,1972,1974,1984,1998,1999,2000,2001,2002,2003,2004,2005,2006,2007,2008,2009,2010,2013,202
0,2021,2022,2030,2033,2034,2035,2038,2040,2041,2042,2043,2045,2046,2047,2048,2049,2065,2068,2099
,2100,2103,2105,2106,2107,2111,2119,2121,2126,2135,2144,2160,2161,2170,2179,2190,2191,2196,2200,
2222,2251,2260,2288,2301,2323,2366,2381,2382,2383,2393,2394,2399,2401,2492,2500,2522,2525,2557,2
601,2602,2604,2605,2607,2608,2638,2701,2702,2710,2717,2718,2725,2800,2809,2811,2869,2875,2909,29
10,2920,2967,2968,2998,3000,3001,3003,3005,3006,3007,3011,3013,3017,3030,3031,3052,3071,3077,312
8,3168,3211,3221,3260,3261,3268,3269,3283,3300,3301,3306,3322,3323,3324,3325,3333,3351,3367,3369
,3370,3371,3372,3389,3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689,3690,3703,3737,3766,
3784,3800,3801,3809,3814,3826,3827,3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3
971,3986,3995,3998,4000,4001,4002,4003,4004,4005,4006,4045,4111,4125,4126,4129,4224,4242,4279,43
21,4343,4443,4444,4445,4446,4449,4550,4567,4662,4848,4899,4900,4998,5000,5001,5002,5003,5004,500
9,5030,5033,5050,5051,5054,5060,5061,5080,5087,5100,5101,5102,5120,5190,5200,5214,5221,5222,5225
,5226,5269,5280,5298,5357,5405,5414,5431,5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,
5666,5678,5679,5718,5730,5800,5801,5802,5810,5811,5815,5822,5825,5850,5859,5862,5877,5900,5901,5
902,5903,5904,5906,5907,5910,5911,5915,5922,5925,5950,5952,5959,5960,5961,5962,5963,5987,5988,59
89,5998,5999,6000,6001,6002,6003,6004,6005,6006,6007,6009,6025,6059,6100,6101,6106,6112,6123,612
9,6156,6346,6389,6502,6510,6543,6547,6565,6566,6567,6580,6646,6666,6667,6668,6669,6689,6692,6699
,6779,6788,6789,6792,6839,6881,6901,6969,7000,7001,7002,7004,7007,7019,7025,7070,7100,7103,7106,
7200,7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777,7778,7800,7911,7920,7921,7937,7938,7
999,8000,8001,8002,8007,8008,8009,8010,8011,8021,8022,8031,8042,8045,8080,8081,8082,8083,8084,80
85,8086,8087,8088,8089,8090,8093,8099,8100,8180,8181,8192,8193,8194,8200,8222,8254,8290,8291,829
2,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651,8652,8654,8701,8800,8873,8888,8899,8994,9000
,9001,9002,9003,9009,9010,9011,9040,9050,9071,9080,9081,9090,9091,9099,9100,9101,9102,9103,9110,
9111,9200,9207,9220,9290,9415,9418,9485,9500,9502,9503,9535,9575,9593,9594,9595,9618,9666,9876,9
877,9878,9898,9900,9917,9929,9943,9944,9968,9998,9999,10000,10001,10002,10003,10004,10009,10010
,10012,10024,10025,10082,10180,10215,10243,10566,10616,10617,10621,10626,10628,10629,10778,111
10,11111,11967,12000,12174,12265,12345,13456,13722,13782,13783,14000,14238,14441,14442,15000,1
5002,15003,15004,15660,15742,16000,16001,16012,16016,16018,16080,16113,16992,16993,17877,17988
,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221,20222,208
28,21571,22939,23502,24444,24800,25734,25735,26214,27000,27352,27353,27355,27356,27715,28201,3
0000,30718,30951,31038,31337,32768,32769,32770,32771,32772,32773,32774,32775,32776,32777,32778
,32779,32780,32781,32782,32783,32784,32785,33354,33899,34571,34572,34573,35500,38292,40193,409
11,41511,42510,44176,44442,44443,44501,45100,48080,49152,49153,49154,49155,49156,49157,49158,4
9159,49160,49161,49163,49165,49167,49175,49176,49400,49999,50000,50001,50002,50003,50006,50300

,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055,55056,55555,55600,56737,56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389