

Challenge 4: VoIP (intermediate)

Submission Template

Submit your solution at <http://www.honeynet.org/challenge2010/> by 17:00 EST, Wednesday, June 30th 2010. Results will be released on Wednesday, July 21st 2010.

Name (required): Shaun Zinck	Email (required): <a href="mailto:shaun.zinck@gmail.com">shaun.zinck@gmail.com</a>
Country (optional): USA	Profession (optional): <input type="checkbox"/> Student <input type="checkbox"/> Security Professional <input checked="" type="checkbox"/> Other Software Engineer

Thanks to the authors of this challenge. It was a very interesting challenge. I learned something new each time I looked at the pcap and the log file (and thus revised my answers several times). It was also a great help to be able to look at the sample solutions and winners for previous honeynet contests.

Section 1/ Question 1. What protocol is being used? Is it TCP or UDP?	Possible Points: 1pt
Tools Used: cat	
Awarded Points:	
Answer	
\$ grep UDP logs_v3.txt ; grep TCP logs_v3.txt	
UDP	

Section 1/ Question 2. Could this log be the result a simple nmap scan being run against the honeynet? Explain	Possible Points: 1pt
Tools Used: cat	
Answer	
No. Nmap scans for open TCP or UDP ports by attempting to contact each port. The log file shows a result of SIP probes that were all done on the SIP port using a specialized piece of software that understands the SIP protocol. All of the log entries are a result of software connecting to a specific port (SIP), and issuing special instructions. The tool that did this is more specialized, while nmap is more of a general tool.	

Section 1/ Question 3a. Name the scanning tools that may have been used to by the attacker.	Possible Points: 1pt
Tools Used:google, grep, sipgrep.pl (see appendix)	
<p>Answer</p> <p>sipvicious, specifically:  svmap  svwar  svcrack</p> <p>The string “sipvicious” can be seen in the logs_v3.txt file. Also the User-Agent header of “friendly-scanner” showed up in 4248 log messages. The same string of “friendly-scanner” also shows up the sipvicious source code.</p> <pre>\$ grep sipvicious logs_v3.txt From: "sipvicious"&lt;sip:100@1.1.1.1&gt;; tag=X_removed To: "sipvicious"&lt;sip:100@1.1.1.1&gt;</pre> <pre>\$ ./sipgrep.pl friendly-scanner   grep "\-----"   wc -l 4248</pre> <pre>\$ grep friendly-scanner sipvicious/sipvicious/* sipvicious/sipvicious/helper.py:         useragent='friendly-scanner');</pre>	

Section 1/ Question 3b. What was the tool suite author's intended use of this tool suite ? Who was it designed to be used by?	Possible Points: 1pt
<p>Tools Used:</p> <p><a href="http://enablesecurity.com/">http://enablesecurity.com/</a>  <a href="http://blog.sipvicious.org/">http://blog.sipvicious.org/</a>  <a href="http://code.google.com/p/sipvicious/wiki/FrequentlyAskedQuestions">http://code.google.com/p/sipvicious/wiki/FrequentlyAskedQuestions</a></p>	
<p>Answer</p> <p>The author intended this tool to be used to be used to “audit SIP based VoIP systems.” The tool was designed to be used by administrators and security professionals, against their own systems.</p>	

Section 1/ Question 3c. One of these tools was only used against a small subset of extensions. Which were these extensions and why were only they targeted with this tool ?	Possible Points: 2pts
Tools Used: grep, sipgrep.pl	

Answer

Extensions:

100  
101  
102  
103  
111

These extensions were probably revealed by the larger *svwar* scan as valid extensions. The next step for an attacker is to try to crack the passwords for these extensions, which is why only these five were targeted.

The log events related to these extensions show a slightly different signature. The *svcrack* utility doesn't generate a *Contact* header, but the code that generates a SIP request (*helper.py*, *makeRequest*) supplies a default contact of "sip:123@1.1.1.1". This unique signature can be seen in the log files.

#### Selection from helper.py

```
def makeRequest(
    method, fromaddr, toaddr, dsthost, port, callid, srchost='',
    branchunique=None, cseq=1, auth=None, localtag=None, compact=False,
    contact='sip:123@1.1.1.1', accept='application/sdp', contentlength=None,
    localport=5060, extension=None, contenttype=None, body='',
    useragent='friendly-scanner'):
```

Notice that the contact field has a default.

#### Selection from svwar.py

```
    request = makeRequest(
        m,
        '"%s"<sip:%s@%s>' % (username, username, self.dsthost),
        '"%s"<sip:%s@%s>' % (username, username, self.dsthost),
        self.dsthost,
        self.dstport,
        cid,
        self.externalip,
        branchunique,
        cseq,
        auth,
        localtag,
        self.compact,
        contact=contact,
        localport=self.localport,
        extension=username
    )
    return request
```

Notice that a *Contact* argument is supplied in the call to *makeRequest*.

**Selection from svcrack.py**

```
register = makeRequest(  
    m,  
    "%s" < sip:%s@%s>' % (extension,extension,self.dsthost),  
    "%s" < sip:%s@%s>' % (extension,extension,self.dsthost),  
    self.dsthost,  
    self.dstport,  
    callid=cid,  
    srchost=self.externalip,  
    branchunique=branchunique,  
    cseq=cseq,  
    auth=auth,  
    localtag=localtag,  
    compact=self.compact,  
    localport=self.localport  
)  
return register
```

Notice that a *Contact* argument is not supplied in the call to *makeRequest*. This means any log event with a *User-Agent* of “friendly-scanner” and *Contact* of “sip:[123@1.1.1.1](mailto:123@1.1.1.1)” can be attributed to *svwar.py*.

```
$ ./sipgrep.pl friendly-scanner logs_v3.txt | ./sipgrep.pl sip:123@1.1.1.1 - | grep From | cut -d\ -f2 | sed 's//g' | sort |  
uniq  
100  
101  
102  
103  
111
```

Section 1/ Question 4a. How many extensions were scanned? Are they all numbered extensions, or named as well?. List them	Possible Points: 2pts
Tools Used: ./sipgrep.pl	

Answer

The following 2652 extensions were scanned. There were names, as well as numbers.

Analyzing the source code of sipvicious, it can be seen that *svwar* uses the default *User-Agent* of “friendly-scanner” and supplies a non-default *Contact*. The other tools use either a default *Contact* (*svwar*) or a different *Contact* (*svmap*).

```
$ ./sipgrep.pl friendly-scanner logs_v3.txt | ./sipgrep.pl "Contact.*@honey" - | grep From | sed 's/<.*//;s//g; s/From: //' | sort | uniq
```

```
1000
1003
1006
1009
100
1013
1016
1019
101
1022
1023
1026
1027
1029
102
1032
1034
1037
103
1041
1045
1048
104
1051
1054
1059
1063
1067
106
1072
1077
107
1081
1084
1087
108
1091
1094
1097
109
1100
1105
1109
```

110  
1110  
1114  
1118  
1119  
111  
1123  
1129  
112  
1135  
1139  
113  
1144  
1148  
114  
1154  
1159  
115  
1162  
1167  
116  
1172  
1179  
117  
1183  
1187  
118  
1192  
1195  
119  
1201  
1205  
1209  
120  
1214  
1218  
121  
1227  
122  
1230  
1233  
123  
1242  
1245  
124  
1250  
1253  
1256  
125  
1260  
1264  
1267  
126  
1270  
1274  
1277  
127  
1280

1283  
128  
1290  
1293  
1298  
129  
1300  
1303  
1305  
130  
1310  
1313  
1317  
131  
1321  
1325  
1328  
132  
1331  
1335  
1338  
133  
1341  
1345  
1348  
134  
1350  
1357  
1359  
135  
1362  
1365  
1366  
1369  
1372  
1375  
1378  
137  
1381  
1384  
1387  
1390  
1393  
1396  
1399  
1401  
1405  
1409  
1411  
1413  
1415  
1418  
1423  
1430  
1443  
1448  
1449  
1450

1454  
1458  
1462  
1466  
1470  
1474  
1477  
1480  
1483  
1487  
1489  
1493  
1494  
1496  
1499  
1502  
1505  
1508  
1511  
1515  
1518  
1523  
1526  
1529  
152  
1533  
1537  
1540  
1544  
1547  
1551  
1555  
1558  
1559  
1561  
1565  
1569  
1574  
1577  
1580  
1583  
1586  
1592  
1596  
1599  
159  
1602  
1605  
1609  
1614  
1619  
1623  
1627  
1632  
1636  
1641  
1645  
1651

1652  
1656  
1657  
1660  
1664  
1668  
1673  
1677  
1682  
1687  
1692  
1696  
1699  
1703  
1707  
1709  
1715  
1719  
1723  
1727  
1729240413  
1730  
1733  
1737  
1740  
1745  
1751  
1753  
1758  
1759  
175  
1763  
1766  
1770  
1778  
1784  
1786  
178  
1790  
1793  
1796  
1799  
1804  
1806  
1810  
1813  
1816  
1820  
1824  
1827  
1831  
1832  
1834  
1838  
1844  
1849  
1852  
1855

1860  
1863  
1866  
1869  
1872  
1875  
1878  
1883  
1888  
1892  
1896  
189  
1900  
1905  
1909  
1913  
1916  
191  
1921  
1924  
1928  
1932  
1936  
1940  
1943  
1948  
194  
1950  
1953  
1956  
195  
1960  
1963  
196  
1970  
1976  
1979  
197  
1987  
1991  
1993  
1997  
199  
2000  
2004  
2007  
2010  
2014  
2017  
2021  
2024  
2028  
202  
2032  
2036  
2040  
2042  
2045

2049  
2053  
2056  
205  
2060  
2064  
2067  
2068  
2071  
2075  
2079  
2083  
2087  
2091  
2095  
2098  
2101  
2105  
2108  
2109  
210  
2112  
2116  
2121  
2125  
2129  
2133  
213  
2140  
2149  
2153  
2160  
2164  
2167  
216  
2171  
2178  
2182  
2186  
2190  
2192  
2195  
2202  
2203  
2205  
220  
2210  
2213  
2223  
2228  
2232  
2235  
2238  
2240  
2243  
2246  
2254  
2257

225  
2261  
2265  
2269  
226  
2273  
2277  
227  
2281  
2284  
2288  
2292  
2296  
2299  
2303  
2307  
230  
2311  
2314  
2318  
2328  
2331  
2335  
2339  
233  
2350  
2355  
2359  
2363  
2367  
2370  
2371  
2373  
2374  
2376  
237  
2380  
2381  
2384  
2389  
2393  
2396  
2397  
2409  
240  
2413  
2414  
2417  
2421  
2422  
2423  
2427  
2430  
2433  
2437  
2438  
2440  
2444

2448  
244  
2450  
2453  
2457  
2460  
2463  
2464  
2465  
2468  
2471  
2474  
2478  
247  
2482  
2486  
2489  
2493  
2496  
2499  
2501  
2505  
2509  
250  
2513  
2516  
2520  
2521  
2522  
2523  
2526  
2529  
2533  
2536  
2539  
2542  
2545  
2548  
2551  
2554  
2558  
255  
2563  
2566  
2568  
2571  
2575  
2578  
2582  
2584  
2587  
2588  
2589  
2590  
2594  
2597  
2600  
2603

2606  
260  
2610  
2614  
2617  
2621  
2624  
2628  
262  
2631  
2639  
2645  
2649  
2652  
2659  
2663  
2668  
266  
2672  
2679  
267  
2683  
2687  
2692  
2693  
2695  
2699  
269  
2704  
2707  
2710  
2715  
2719  
2725  
2729  
272  
2733  
2737  
2741  
2743  
2750  
275  
2763  
2768  
2773  
2779  
2782  
2786  
2790  
2794  
2797  
279  
2802  
2805  
2809  
2813  
2817  
2821

2825  
2828  
282  
2832  
2836  
2839  
2843  
2847  
2849  
2853  
2856  
2860  
2862  
2865  
2870  
2874  
2878  
287  
2882  
2885  
2890  
2893  
2898  
2902  
2905  
2909  
290  
2913  
2917  
2920  
2924  
2928  
2931  
2933  
2937  
2941  
2943  
2946  
2949  
294  
2952  
2955  
2958  
2959  
2962  
2964  
2966  
2968  
2971  
2975  
2981  
2982  
2983  
298  
2997  
299  
3002  
3005

3008  
3010  
3014  
3019  
301  
3021  
3025  
3028  
3032  
3035  
3038  
3042  
3045  
3048  
3051  
3054  
3057  
305  
3060  
3065  
3067  
3070  
3074  
3077  
3080  
3083  
3086  
308  
3090  
3093  
3097  
3100  
3103  
3110  
3117  
3119  
3123  
3126  
3130  
3133  
3138  
3142  
3145  
314  
3150  
3153  
3159  
3163  
3167  
3172  
3176  
3179  
3181  
3183  
3186  
318  
3190  
3193

3195  
3198  
3201  
3202  
3203  
3205  
3206  
3207  
3212  
3214  
3218  
3222  
3225  
3228  
3231  
3234  
3237  
3239  
3245  
3247  
324  
3250  
3253  
3255  
3259  
3262  
3266  
3270  
3273  
3276  
3280  
3284  
3289  
3292  
3296  
3298  
3301  
3303  
3304  
3306  
3307  
3309  
3313  
3317  
331  
3320  
3323  
3327  
3329  
3332  
3334  
3340  
3343  
3346  
3349  
3352  
3355  
3358

3362  
3364  
3366  
3369  
3372  
3375  
3379  
3382  
3384  
3387  
338  
3390  
3399  
3402  
3405  
3408  
3410  
3413  
3416  
3419  
3422  
3424  
3427  
3428948518  
3428  
3430  
3432  
3434  
3436  
343  
3440  
3441  
3447  
3449  
3454  
3457  
3459  
3462  
3463  
3465  
3468  
3470  
3472  
3474  
3476  
3479  
3481  
3483  
3488  
3490  
3492  
3494  
3496  
3498  
349  
3501  
3503  
3504

3505  
3506  
3509  
3512  
3514  
3516  
3519  
3522  
3524  
3527  
3529  
3532  
3535  
3538  
3540  
3543  
3546  
3549  
3551  
3552  
3553  
3557  
3559  
355  
3561  
3563  
3566  
3568  
3570  
3572  
3574  
3577  
3580  
3583  
3586  
3588  
3591  
3594  
3597  
3601  
3605  
360  
3610  
3625  
3629  
3632  
3635  
3638  
3641  
3646  
3651  
3654  
3658  
3660  
3663  
3667  
3669  
366

3673  
3676  
3680  
3683  
3686  
3689  
3693  
3695  
3699  
3702  
3704  
3706  
3709  
3712  
3715  
3718  
3722  
3724  
3727  
3729  
3732  
3735  
3739  
373  
3742  
3746  
3750  
3751  
3754  
3758  
3760  
3764  
3767  
3771  
3774  
3778  
3781  
3783  
3786  
3790  
3794  
3798  
3802  
3805  
3808  
380  
3810  
3814  
3818  
3819  
3820  
3823  
3826  
3829  
3830  
3834  
3838  
3841

3845  
3850  
3852  
3853  
3857  
385  
3861  
3864  
3867  
3871  
3875  
3878  
3881  
3884  
3888  
3891  
3894  
3897  
3901  
3905  
3910  
3914  
3918  
3921  
3925  
392  
3930  
3934  
3938  
3943  
3948  
3951  
3955  
3958  
3962  
3965  
3969  
3975  
3977  
3982  
3986  
398  
3990  
3993  
3997  
4002  
4005  
4009  
4013  
4016  
4020  
4023  
4027  
4030  
4033  
4036  
4039  
403

4043  
4049  
4055  
4059  
4062  
4066  
4068  
4071  
4073  
4076  
4080  
4082  
4085  
4086  
4088  
408  
4091  
4095  
4097  
4101  
4104  
4108  
4115  
4117  
4121  
4123  
4126  
4128  
4131  
4134  
4136  
4138  
413  
4140  
4142  
4144  
4146  
4149  
4151  
4154  
4156  
4158  
4161  
4164  
4167  
4168  
4171  
4174  
4176  
4180  
4186  
4189  
418  
4192  
4195  
4197  
4199  
4201

4203  
4205  
4209  
4212  
4214  
4220  
4222  
4224  
4227  
4230  
4232  
4235  
4237  
4239  
4241  
4244  
4247  
4249  
4251  
4253  
4255  
4257  
4259  
425  
4262  
4265  
4267  
4270  
4271  
4275  
4282  
4289  
4293  
4296  
4300  
4303  
4307  
4309  
4312  
4315  
4318  
431  
4321  
4323  
4326  
4330  
4332  
4335  
4337  
4340  
4342  
4345  
4346  
4348  
4350  
4352  
4354  
4356

4358  
4360  
4363  
4367  
4369  
4372  
4374  
4377  
4379  
4381  
4383  
4384  
4387  
4389  
438  
4392  
4397  
4399  
4401  
4403  
4405  
4410  
4412  
4414  
4416  
4418  
4421  
4424  
4426  
4429  
4432  
4434  
4437  
4439  
4440  
4441  
4443  
4446  
4449  
444  
4452  
4455  
4458  
4461  
4464  
4467  
4469  
4472  
4475  
4478  
4479  
4482  
4485  
4487  
4490  
4493  
4496  
4499

4502  
4504  
4507  
450  
4510  
4513  
4517  
4520  
4523  
4526  
4530  
4535  
4539  
4543  
4547  
454  
4551  
4554  
4555  
4558  
4561  
4564  
4568  
4569  
4573  
4576  
4579  
4584  
4588  
4589  
4591  
4596  
4601  
4606  
460  
4612  
4618  
4625  
4630  
4635  
4641  
4645  
4650  
4654  
465  
4670  
4678  
4684  
4689  
4695  
4707  
4715  
4722  
4727  
472  
4733  
4737  
4743

4747  
4752  
4758  
4761  
4765  
4769  
4773  
4777  
4780  
4784  
4786  
4791  
4794  
4798  
4803  
480  
4812  
4817  
4822  
4827  
4833  
4836  
4840  
4846  
4850  
4853  
4858  
485  
4861  
4864  
4868  
4871  
4876  
4879  
4883  
4887  
4891  
4894  
4899  
4903  
4906  
490  
4911  
4915  
4919  
4922  
4927  
4931  
4935  
4940  
494  
4953  
4957  
4962  
4968  
4972  
4977  
4983

4986  
4990  
4994  
4999  
5005  
500  
5010  
5015  
5020  
5029  
5035  
5041  
5046  
504  
5053  
5058  
5062  
5068  
5091  
509  
5101  
5115  
5119  
5123  
5124  
5129  
5133  
5138  
513  
5143  
5148  
5152  
5157  
5161  
5165  
5170  
5176  
5180  
5183  
5188  
518  
5193  
5197  
5200  
5205  
5209  
5213  
5218  
5224  
5231  
5235  
5239  
523  
5243  
5248  
5253  
5258  
5264

5268  
5271  
5272  
5275  
5279  
527  
5284  
5288  
5291  
5295  
5299  
5303  
5307  
5310  
5315  
5318  
5322  
5326  
5330  
5334  
5338  
5341  
5345  
5348  
534  
5353  
5356  
5360  
5361  
5364  
5367  
5368  
5371  
5374  
5377  
5380  
5384  
5386  
5390  
5393  
5395  
5399  
539  
5400  
5403  
5406  
5409  
5412  
5415  
5417  
5420  
5423  
5426  
5429  
5433  
5436  
543  
5440

5444  
5448  
5452  
5455  
5457  
5460  
5463  
5466  
5469  
5472  
5478  
5482  
5484  
5487  
5489  
5494  
5496  
5498  
5499  
549  
5502  
5506  
5508  
5511  
5514  
5517  
5519  
5522  
5524  
5528  
5530  
5532  
5535  
5538  
5541  
5552  
5558  
5561  
5568  
5571  
5574  
5577  
5580  
5583  
5587  
558  
5590  
5594  
5598  
5601  
5605  
5609  
5612  
5615  
5617  
5625  
5628  
5632

5634  
563  
5640  
5643  
5646  
5648  
5651  
5656  
5659  
5662  
5666  
5669  
566  
5673  
5678  
5682  
5683  
5685  
5689  
5693  
5697  
5703  
5706  
570  
5710  
5714  
5719  
5723  
5729  
5733  
5739  
5745  
5748  
574  
5752  
5756  
5760  
5764  
5767  
5772  
5776  
5779  
577  
5783  
5788  
5792  
5796  
5797  
5799  
5803  
5807  
5811  
5816  
581  
5821  
5824  
5829  
5832

5836  
5842  
5847  
5853  
5858  
5862  
5867  
5868  
586  
5871  
5878  
5888  
5897  
589  
5903  
5916  
5923  
5929  
5936  
593  
5941  
5946  
5950  
5956  
5961  
5965  
596  
5970  
5976  
5981  
5986  
5992  
5999  
599  
6003  
6004  
6009  
6015  
6021  
6027  
602  
6032  
6038  
6041  
6045  
6051  
6056  
6062  
6067  
606  
6072  
6078  
6083  
6088  
6092  
6096  
6101  
6105

610  
6110  
6115  
6120  
6124  
6129  
612  
6133  
6138  
6144  
6149  
6154  
6159  
6163  
6168  
616  
6173  
6179  
6184  
6188  
6193  
6198  
619  
6204  
6208  
6212  
6216  
6220  
6224  
6225  
6229  
622  
6233  
6237  
6242  
6248  
6251  
6255  
6258  
625  
6262  
6267  
6270  
6274  
6279  
6284  
6288  
628  
6294  
6300  
6304  
6308  
6310  
6316  
631  
6320  
6325  
6330

6335  
6340  
6345  
634  
6351  
6356  
6360  
6364  
6368  
6371  
6377  
6381  
6385  
6389  
6394  
6398  
6402  
6405  
6409  
640  
6414  
6417  
6421  
6425  
6429  
6433  
6436  
643  
6440  
6445  
6449  
6455  
6458  
6462  
6467  
646  
6472  
6476  
6480  
6485  
6498  
649  
6506  
6520  
6525  
6529  
652  
6533  
6538  
6542  
6545  
6548  
654  
6552  
6557  
6564  
6569  
656

6572  
6578  
6589  
659  
6611  
6617  
6626  
662  
6632  
6638  
6644  
6648  
6654  
6658  
665  
6664  
6668  
6673  
6675  
667  
6681  
6687  
6693  
6697  
669  
6703  
6707  
6712  
6717  
6724  
6729  
672  
6734  
6738  
6744  
6749  
6756  
6762  
6767  
6773  
6779  
6785  
678  
6791  
6797  
6802  
6808  
6813  
6819  
6824  
6828  
6832  
6833  
6835  
683  
6840  
6843  
6850

6854  
6858  
6861  
6869  
6870  
6873  
6876  
6879  
6882  
6883  
6886  
6887  
6888  
6890  
6891  
6892  
6898  
689  
6903  
6907  
6917  
6920  
6923  
6927  
6930  
6935  
6939  
6943  
6947  
6950  
6953  
6956  
6960  
6964  
6967  
6970  
6974  
6978  
6981  
6984  
6989  
698  
6992  
6995  
6998  
7001  
7002  
7006  
7009  
7011  
7013  
7016  
7018  
701  
7021  
7024  
7029  
7036

7038  
7041  
7044  
7046  
7047  
7049  
704  
7052  
7055  
7060  
7061  
7063  
7066  
7069  
7073  
7076  
707  
7080  
7084  
7088  
7091  
7095  
7096  
7098  
709  
7101  
7104  
7108  
7112  
7115  
7116  
7119  
7123  
7126  
7129  
712  
7133  
7135  
7139  
7141  
7144  
7148  
7151  
7154  
7157  
715  
7160  
7164  
7168  
7172  
7175  
717  
7180  
7183  
7188  
7192  
7199  
7203

7208  
7212  
7216  
721  
7220  
7225  
7230  
7233  
7235  
7240  
7243  
7247  
724  
7251  
7255  
7260  
7265  
7269  
7272  
7276  
727  
7280  
7285  
7288  
7293  
7297  
729  
7301  
7305  
7309  
7312  
7316  
7321  
7325  
7329  
732  
7333  
7336  
7340  
7344  
7348  
7351  
7356  
735  
7367  
7372  
7374  
7386  
738  
7391  
7395  
7399  
7403  
7408  
7412  
7416  
741  
7424

7431  
7446  
7449  
744  
7454  
7458  
7464  
7468  
7472  
7478  
747  
7481  
7484  
7487  
7491  
7494  
7497  
7500  
7503  
7506  
750  
7510  
7514  
7517  
7521  
7524  
7527  
7530  
7534  
7539  
753  
7541  
7544  
7547  
7551  
7554  
7558  
7560  
7563  
7566  
756  
7571  
7575  
7578  
757  
7582  
7586  
7591  
7597  
759  
7601  
7602  
7606  
7610  
7614  
7618  
7623  
7627

762  
7632  
7635  
7638  
7643  
7646  
7647  
7650  
7651  
7655  
7656  
7658  
7661  
7662  
7665  
7666  
766  
7670  
7674  
7680  
7681  
7694  
7697  
769  
7701  
7705  
7709  
7711  
7715  
7719  
7722  
7726  
7728  
772  
7733  
7736  
7739  
7744  
7748  
7752  
7755  
775  
7760  
7763  
7768  
7772  
7777  
7781  
7788  
778  
7792  
7793  
7795  
7799  
7803  
7808  
7813  
7816

7820  
7827  
782  
7831  
7834  
7837  
7842  
7847  
7852  
7857  
785  
7861  
7866  
7872  
7877  
7883  
7887  
7892  
7896  
7897  
7902  
7907  
790  
7912  
7917  
7922  
7931  
7936  
7942  
7946  
7952  
7958  
795  
7964  
7976  
7986  
7991  
7997  
799  
8004  
8010  
8017  
8024  
8031  
8038  
803  
8044  
8052  
8061  
8069  
8078  
8086  
808  
8093  
8101  
8110  
8120  
8121

8128  
8137  
8143  
8149  
8156  
8161  
8168  
8169  
8175  
8180  
8188  
8189  
818  
8192  
8198  
8204  
8210  
8216  
821  
8222  
8238  
8245  
8249  
8255  
8260  
8264  
8268  
8276  
827  
8280  
8284  
8292  
8296  
8301  
8306  
8309  
8310  
8312  
8316  
831  
8320  
8324  
8327  
8332  
8336  
8338  
8341  
8344  
8347  
8350  
8353  
8357  
8359  
8363  
8366  
836  
8370  
8374

8377  
8380  
8384  
8386  
8390  
8397  
8399  
839  
8402  
8404  
8408  
8412  
8414  
8417  
8420  
8422  
8425  
8429  
842  
8431  
8434  
8438  
8442  
8445  
8448  
8451  
8453  
8456  
8459  
845  
8463  
8467  
846  
8470  
8474  
8478  
8481  
8484  
8487  
8488  
8491  
8495  
8499  
849  
8504  
8508  
8513  
8517  
8522  
8527  
8528  
852  
8532  
8536  
8541  
8546  
8550  
8554

8559  
8564  
8568  
856  
8572  
8577  
8582  
8586  
8592  
8596  
8597  
859  
8601  
8607  
8612  
8618  
8624  
8629  
8630  
8634  
8639  
8643  
8647  
864  
8651  
8654  
8659  
8663  
8667  
8671  
8674  
8677  
8681  
8684  
868  
8690  
8693  
8698  
8700  
8703  
8706  
8709  
8713  
8716  
8719  
871  
8722  
8726  
8728  
8731  
8734  
8738  
8742  
8745  
8748  
8751  
8755  
8758

875  
8762  
8766  
8769  
8772  
8775  
8777  
8779  
8782  
8784  
8787  
8790  
8793  
8795  
8797  
8801  
8804  
8807  
8812  
8814  
8817  
8819  
881  
8822  
8825  
8831  
8834  
8837  
8840  
8843  
8847  
8850  
8853  
8856  
8859  
8864  
8866  
886  
8870  
8873  
8876  
887  
8881  
8886  
8889  
8893  
8897  
8902  
8905  
8909  
8912  
8916  
891  
8921  
8925  
8929  
8934  
8938

8943  
8946  
8950  
8955  
895  
8960  
8964  
896  
8970  
8975  
8979  
8983  
8988  
898  
8992  
8995  
8999  
9003  
900  
9010  
9013  
9015  
9018  
9021  
9022  
9025  
9028  
9032  
9033  
9036  
9040  
9044  
9048  
9051  
9056  
9057  
9059  
905  
9065  
9069  
9074  
9077  
9081  
9085  
9091  
9095  
9098  
9102  
9105  
9108  
9112  
9113  
9116  
9120  
9123  
9128  
912  
9132

9136  
9141  
9146  
9150  
9154  
9159  
9163  
9171  
9179  
917  
9182  
9191  
9196  
9201  
9207  
920  
9211  
9215  
9219  
9224  
9229  
9233  
923  
9240  
9245  
9250  
9251  
9254  
9258  
9262  
9265  
9268  
9272  
9275  
9279  
927  
9282  
9288  
9294  
9296  
9299  
9302  
9306  
9310  
9314  
9318  
931  
9321  
9325  
9328  
9332  
9335  
9339  
9343  
9347  
9350  
9353  
9356

9360  
9363  
9367  
936  
9371  
9376  
9380  
9385  
9390  
9395  
9400  
9406  
940  
9410  
9412  
9416  
9419  
9420  
9424  
9427  
9428  
9430  
9435  
9438  
943  
9442  
9446  
9449  
9452  
9457  
9460  
9463  
9467  
946  
9470  
9473  
9476  
9479  
9483  
9488  
9490  
9493  
949  
9500  
9503  
9505  
9518  
951  
9523  
9526  
9530  
9532  
9535  
9539  
9543  
9547  
9548  
954

9551  
9554  
9558  
9562  
9565  
9569  
956  
9573  
9577  
9580  
9582  
9586  
9590  
9593  
9598  
9602  
9605  
9609  
960  
9612  
9616  
9620  
9624  
9625  
9629  
9632  
9636  
9639  
963  
9642  
9646  
9649  
9652  
9654  
9658  
9663  
9666  
9670  
9672  
9676  
9679  
9683  
9686  
9689  
968  
9693  
9697  
9702  
9706  
9710  
9715  
9718  
9722  
9725  
9726  
972  
9731  
9735

9738  
9741  
9745  
9748  
9751  
9756  
9760  
9765  
9769  
976  
9772  
9775  
9779  
9784  
9788  
9791  
9795  
9799  
979  
9803  
9807  
9811  
9815  
9818  
9823  
9827  
982  
9830  
9835  
9837  
9841  
9845  
9849  
9851  
9855  
9858  
985  
9861  
9865  
9867  
9871  
9874  
9890  
9896  
989  
9901  
9906  
9911  
9915  
9922  
9928  
9930  
9933  
9934  
9939  
993  
9943  
9948

9950  
9954  
9957  
9961  
9965  
996  
9970  
9975  
9976  
997  
9983  
9991  
9994  
aaron  
abigail  
admin  
andrew  
asterisk  
christopher  
client  
cpanel  
data  
fax  
freddy  
heaven  
help  
info  
jane  
jobs  
joshua  
manager  
market  
marketing  
mike  
news  
norman  
operator  
oracle  
orders  
owner  
postfix  
postmaster  
richard  
sales  
samantha  
sarah  
sebastian  
service  
shop  
spam  
steve  
steven  
support  
temp  
test  
trixbox  
user

<p>Section 1/ Question 4b. Categorize these extensions into the following groups, and explain to method you used:</p> <ul style="list-style-type: none"> <li>• Those that exist on the honeypot, AND require authentication</li> <li>• Those that exist on the honeypot, and do NOT require authentication</li> <li>• Those that do not exist on the honeypot</li> </ul>	<p>Possible Points: 6pts</p>
<p>Tools Used: perl, grep, less</p>	
<p>Answer</p> <p><b>Those that exist, AND require authentication</b></p> <pre>\$ ./sipgrep.pl friendly-scanner logs_v3.txt   ./sipgrep.pl sip:123@1.1.1.1 -   grep Auth   perl -n -e '/username="(.*?)"/;print \$1, "\n"   sort   uniq</pre> <p>101 102 103 111</p> <p>These have repeated authentication attempts using the <i>Authentication:</i> header in the second (cracking) portion of the log, indicative of password cracking.</p> <p><b>Those that exist on the honeypot, and do NOT require authentication</b></p> <p>100</p> <p>This has a single REGISTER message in the second (cracking) portion of the log, indicating that a password cracking session was started. The absence of <i>Authentication:</i> headers suggests that the REGISTER was successful without a password being attempted. The attacker was also able to REGISTER, SUBSCRIBE, and INVITE using extension 100, again without showing any <i>Authentication:</i> headers.</p> <p><b>Those that do not exist on the honeypot</b></p> <p>There are 2647 nonexisting extensions (The listed 2652 extensions that were scanned, minus the five that were identified (100, 101, 102, 103, 111)).</p> <p>These are extensions that show scan probes in the first portion of the log file, but do not show password cracking attempts in the second portion of the log file. It can be assumed that these extensions do not exist.</p>	

<p>Section 1/ Question 5. Was a real SIP client used at any point ? If it was, what time was it used, and why ?</p>	<p>Possible Points: 1pt</p>
<p>Tools Used: less</p>	
<p>Answer</p> <pre>\$ ./sipgrep.pl 'User-Agent: (?!friendly-scanner)' logs_v3.txt   less</pre> <p>Yes. It was used on 2010-05-05 at 10:00AM, 3 days after the password cracking attempt. The usage lasted just a few minutes. The attacker was probably verifying the results of the password cracking session, and also trying to determine if outside phone numbers could be dialed using this system.</p>	

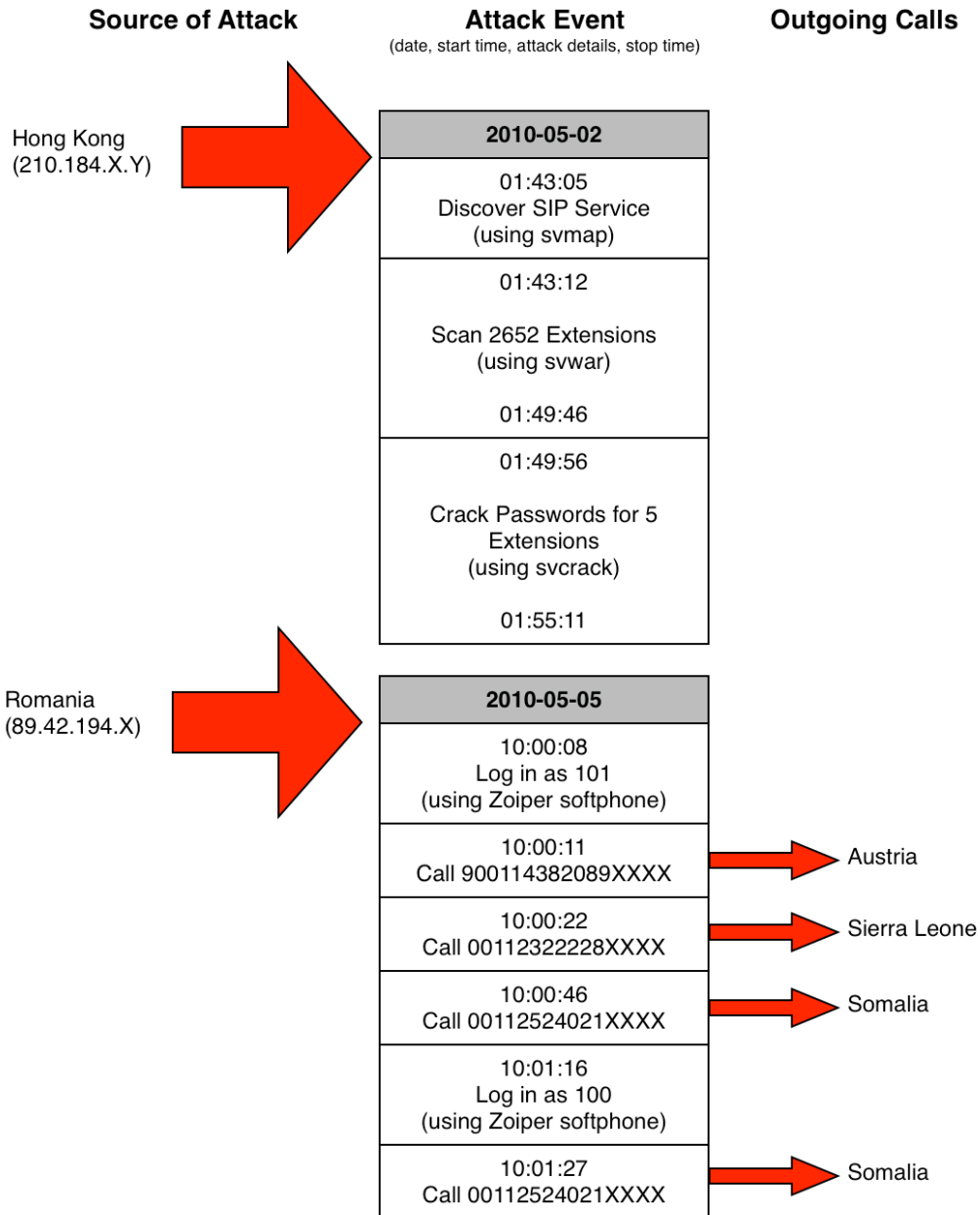
Section 1/ Question 6. List the following, include geo-location information. - Source IP addresses involved - The real world phone numbers that were attempted to be dialled	Possible Points: 3pts
Tools Used: <a href="http://en.wikipedia.org/wiki/List_of_country_calling_codes">http://en.wikipedia.org/wiki/List_of_country_calling_codes</a> <a href="http://www.geoptool.com/">http://www.geoptool.com/</a> <a href="http://www.countrycallingcodes.com/Reverse-Lookup.php">http://www.countrycallingcodes.com/Reverse-Lookup.php</a> whois	
Answer	
<b>Source IP addresses:</b> 210.184.X.Y - the IP address of the machine that initiated scanning and password cracking 89.42.194.X - the IP address of the machine running the SIP client used to make calls, after a valid password was found	
<b>Geo Location:</b>  210.184.X.Y: Hong Kong, Hong Kong (Asia) 89.42.194.X: Constanta, Romania (Europe)	
<b>Real world phone numbers:</b>  \$ ./sipgrep.pl '\nINVITE' logs_v3.txt   less  900114382089XXXX: Austria 00112322228XXXX: Sierra Leone 00112524021XXXX (from 101): Somalia 00112524021XXXX (from 100): Somalia	

Section 1/ Question 7. Draw a simple static or animated timeline of events, describing when and where certain phases occurred from, and what the purpose of each phase was

Possible Points: 5pts

Tools Used: Pages '09

### SIP Service Attack Incident



Section 1/ Question 8a. Assuming this were a real incident, write 2 paragraphs of an Executive summary of this incident. Assume the reader does not have IT Security or VOIP experience. a) First Paragraph: Write, in the minimum detail necessary a description the nature and timings, and possible motives of the attack phases. (3 points)	Possible Points: 3pts
Tools Used:	
Answer  The phone system was attacked and compromised on May 2, 2010. Around 1:43 AM the phone system was discovered by an attacking system from Hong Kong. The attacker was probably scanning random IP ranges on the internet to find vulnerable phone systems. After discovering the system, the attacker used tools to determine which extensions were valid extensions, and another tool that attempts to guess passwords for the valid extensions. This scanning and password guessing lasted approximately 12 minutes, and passwords were discovered for five accounts. Three days later, around 10 AM, an attacker from Romania used a real VOIP telephone to log in to the system as the previously discovered users, and dialed international numbers in Austria, Sierra Leone, and Somalia. These calls may have been made to determine if the phone system allowed making international calls. Hackers will often sell phone system credentials to third parties.	

Section 1/ Question 8b. Assuming this were a real incident, write 2 paragraphs of an Executive summary of this incident. Assume the reader does not have IT Security or VOIP experience. b) Second Paragraph: What actions would you recommend should occur following this particular incident, include any priority/urgency. Also describe any good practices that should be employed to mitigate future attacks.	Possible Points: 3pts
Tools Used: <a href="http://www.cert.org/tech_tips/win-UNIX-system_compromise.html">http://www.cert.org/tech_tips/win-UNIX-system_compromise.html</a>	
Answer  The first step is to disable access for the attacker by disconnecting the phone system from the network. This should be done immediately. Management should decide if prosecution will be pursued. If so, law enforcement should be contacted. The phone company should be notified too. A backup image of the drive (for evidence/forensics) should be made, dated, and stored in a safe location. The system should be inspected to ensure that no other vulnerabilities have been exploited. In this case, it appears only that unauthorized phone calls had been made. Passwords should be changed for all users of this system, and required for accounts that previously didn't have passwords. Finally, the system can be brought back online.  To prevent future attacks, the following recommendations should be considered. 1. The PBX should not acknowledge the presence of certain users: that is, it should give the same message if someone attempts to log in as an existing user or a nonexisting user. 2. Passwords should be required for every extension. 3. Extensions that do not need external access should have external access disabled, and only use internal access. 4. Passwords should be more complex. A password was guessed after merely six minutes. 5. An intrusion detection system should be configured to detect these types of attacks.	

Section 2/ Question 1. Which 4 protocols are involved in the PCAP (VOIP protocols and otherwise) ? Give a brief explanation as to their purpose.	Possible Points: 4pts
Tools Used:wireshark	
Answer	
Wireshark: Statistics -> Protocol Hierarchy	
<b>SIP</b> Session Initiation Protocol - used to set up VOIP call	
<b>HTTP</b> Hypertext Transport Protocol - used for web interface of PBX control panel	
<b>RTP</b> Real Time Transport Protocol - used to transfer audio of the call (voice and DTMF tones)	
<b>RTCP</b> Real Time Transport Control Protocol - provides control, mostly used to gather statistics on the quality of the RTP stream	
There are also a couple of ICMP messages.	

Section 2/ Question 2a. Which codec does the RTP stream use?	Possible Points: 1pt
Tools Used: Wireshark RTP analysis	
Answer	
(Wireshark: Telephony -> RTP -> Show All Streams: Payload)	
ITU-T G.711 PCMU	

Section 2/ Question 2b. How long is the sampling time (in milliseconds)?	Possible Points: 1pt
Tools Used: <a href="http://en.wikipedia.org/wiki/G.711">http://en.wikipedia.org/wiki/G.711</a>	
Answer	
125 ms (1000000 ms /sec / 8000 samples/sec)	

Section 2/ Question 3. How did the attacker gain access to the server? List ways this could have been prevented.	Possible Points: 2pts
Tools Used: Wireshark, google	
Answer	
<p>After finding the server, the attacker used the web interface of the SIP control panel to gain further access. The attacker logged in using a well known default username and password for the maintenance account (of 'maint' and 'password'). The attacker then viewed the 'sip_custom.conf' configuration file and obtained a SIP username and secret (password). The attacker used these credentials to authenticate as the user 555 to the SIP service.</p>	
<p>To prevent this from happening, the maintenance account's password could have been changed from the well-known default. Also, port 80 could have been blocked to prevent remote administration of the SIP service. Also, HTTP Basic authentication is used. Though it would not have prevented this attack, if Basic Authentication is used, the web server should run HTTPS to prevent the credentials from being transmitted unencrypted.</p>	
Details	
<ol style="list-style-type: none"> <li>1. In packet 1, sipvicious was used to check that a SIP server exists. sipvicious uses the OPTIONS by default to scan for SIP servers.</li> <li>2. Packets 3-12 show the attacker requesting the /maint URI and receiving a 401 Authorization Required response. (This is interesting in that a <i>Referer</i> header is given, along with a PHPSESSID cookie, suggesting that the user had already been browsing the trixbox server before this pcap was started. The large number of “304 Not Modified” responses for requested images also corroborate this. Since the trixbox interface uses AJAX, it could be possible the contest authors had left a browser window open and /maint was inadvertently requested. I don't think this is material for this investigation.)</li> <li>3. Packets 13-46 show the attacker requesting the / URI and navigating the interface, which identifies itself as “trixbox”.</li> <li>4. In packets 13-22, the default / URI is requested. This redirects to /user/, which is requested in packets 23-46. This is the default trixbox page.</li> <li>5. In packets 47-69, the /maint URI is requested and credentials of “maint:password” are supplied. These are the default credentials for trixbox (See <a href="http://trixbox.org/wiki/trixbox-quick-install-guide">http://trixbox.org/wiki/trixbox-quick-install-guide</a>).</li> <li>6. The remaining HTTP packets show the attacker accessing the trixbox web interface. I'll highlight the relevant ones.</li> <li>7. In packets 1276-1293, the file “sip_custom.conf” was viewed. This file contained login credentials for two users.</li> <li>8. Packets 1294-1296 shows the attacker using an X-Lite softphone to REGISTER as user 555 using an <i>Authorization</i> header, probably using the secret discovered in sip_custom.conf.</li> <li>9. Packet 1305 shows an INVITE to extension 1000. From the audio this seems to be a conference number.</li> <li>10. Packets of type 'rtpevent' show several attempted conference PINs: 2255#, 4125#, and finally the successful attempt of 4321#.</li> </ol>	

Section 2/ Question 4. What information was gained by the attacker ?	Possible Points: 2pts
Tools Used:wireshark, chaosreader, whois	

Answer

In packets 1276-1293, the contents of the file sip\_custom.conf were viewed. Below is that file:

**sip\_custom.conf**

```
[555]
type=friend
username=555
secret=1234
host=dynamic
extension=from-trunk
context=from-trunk
```

```
[556]
type=friend
username=555
secret=1234
host=dynamic
extension=from-trunk
context=from-trunk
```

Aside from this file containing usernames/passwords, other pertinent details about the system were discovered.

**\$ chaosreader -v Forensic\_challenge\_4.pcap** shows:

**Chaosreader report item number 6:**

Apache/2.2.3 (CenOS)

**Chaosreader report item number 7:**

System Status Version: 2.6.2.3

trixbox version: v279 2.8.0.3

Chaosreader report item number 44:

7555

<p><b>Server Status</b></p> <p>Asterisk <span style="background-color: green; color: white; padding: 2px;">Running</span></p> <p>web server <span style="background-color: green; color: white; padding: 2px;">Running</span></p> <p>cron server <span style="background-color: green; color: white; padding: 2px;">Running</span></p> <p>SSH server <span style="background-color: green; color: white; padding: 2px;">Running</span></p> <p>Mysql <span style="background-color: green; color: white; padding: 2px;">Running</span></p> <p>HUD Server <span style="background-color: orange; color: white; padding: 2px;">N/A</span></p>	<p><b>Announcements</b></p> <p>trixbox CE current release is 2.8.0</p> <p><b>Network Usage</b></p> <table border="0"> <thead> <tr> <th>Device</th> <th>Received</th> <th>Sent</th> <th>Err/Drop</th> </tr> </thead> <tbody> <tr> <td>lo</td> <td>504.88 KB</td> <td>504.88 KB</td> <td>0/0</td> </tr> <tr> <td>eth0</td> <td>3.29 MB</td> <td>4.79 MB</td> <td>0/0</td> </tr> <tr> <td>sit0</td> <td>0.00 KB</td> <td>0.00 KB</td> <td>0/0</td> </tr> </tbody> </table> <p><b>Memory Usage</b></p> <table border="0"> <thead> <tr> <th>Type</th> <th>Percent Capacity</th> <th>Free</th> <th>Used</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>- Kernel + applications</td> <td><div style="width: 27%; border: 1px solid gray; display: inline-block;"></div> 27%</td> <td>135.57 MB</td> <td></td> <td></td> </tr> <tr> <td>- Buffers</td> <td><div style="width: 4%; border: 1px solid gray; display: inline-block;"></div> 4%</td> <td>22.38 MB</td> <td></td> <td></td> </tr> <tr> <td>- Cached</td> <td><div style="width: 34%; border: 1px solid gray; display: inline-block;"></div> 34%</td> <td>171.39 MB</td> <td></td> <td></td> </tr> <tr> <td>Disk Swap</td> <td><div style="width: 0%; border: 1px solid gray; display: inline-block;"></div> 0%</td> <td>760.88 MB</td> <td>0.00 KB</td> <td>760.88 MB</td> </tr> </tbody> </table> <p><b>Mounted Filesystems</b></p> <table border="0"> <thead> <tr> <th>Mount</th> <th>Type</th> <th>Partition</th> <th>Percent Capacity</th> <th>Free</th> <th>Used</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>/</td> <td>ext3</td> <td>/dev/sda2</td> <td><div style="width: 46%; border: 1px solid gray; display: inline-block;"></div> 46% (8%)</td> <td>1.51 GB</td> <td>1.39 GB</td> <td>3.06 GB</td> </tr> <tr> <td>/boot</td> <td>ext3</td> <td>/dev/sda1</td> <td><div style="width: 18%; border: 1px solid gray; display: inline-block;"></div> 18% (1%)</td> <td>75.86 MB</td> <td>17.76 MB</td> <td>98.72 MB</td> </tr> <tr> <td>/dev/shm</td> <td>tmpfs</td> <td>tmpfs</td> <td><div style="width: 0%; border: 1px solid gray; display: inline-block;"></div> 0% (1%)</td> <td>251.68 MB</td> <td>0.00 KB</td> <td>251.68 MB</td> </tr> <tr> <td colspan="3"><b>Totals :</b></td> <td><div style="width: 42%; border: 1px solid gray; display: inline-block;"></div> 42%</td> <td>1.83 GB</td> <td>1.41 GB</td> <td>3.40 GB</td> </tr> </tbody> </table> <p><b>System Uptime</b></p> <p>Server Uptime: 0 hours, 34 minutes                  Asterisk Uptime: 32 minutes, 56 seconds                  Last Reload Time: 32 minutes, 56 seconds</p>	Device	Received	Sent	Err/Drop	lo	504.88 KB	504.88 KB	0/0	eth0	3.29 MB	4.79 MB	0/0	sit0	0.00 KB	0.00 KB	0/0	Type	Percent Capacity	Free	Used	Size	- Kernel + applications	<div style="width: 27%; border: 1px solid gray; display: inline-block;"></div> 27%	135.57 MB			- Buffers	<div style="width: 4%; border: 1px solid gray; display: inline-block;"></div> 4%	22.38 MB			- Cached	<div style="width: 34%; border: 1px solid gray; display: inline-block;"></div> 34%	171.39 MB			Disk Swap	<div style="width: 0%; border: 1px solid gray; display: inline-block;"></div> 0%	760.88 MB	0.00 KB	760.88 MB	Mount	Type	Partition	Percent Capacity	Free	Used	Size	/	ext3	/dev/sda2	<div style="width: 46%; border: 1px solid gray; display: inline-block;"></div> 46% (8%)	1.51 GB	1.39 GB	3.06 GB	/boot	ext3	/dev/sda1	<div style="width: 18%; border: 1px solid gray; display: inline-block;"></div> 18% (1%)	75.86 MB	17.76 MB	98.72 MB	/dev/shm	tmpfs	tmpfs	<div style="width: 0%; border: 1px solid gray; display: inline-block;"></div> 0% (1%)	251.68 MB	0.00 KB	251.68 MB	<b>Totals :</b>			<div style="width: 42%; border: 1px solid gray; display: inline-block;"></div> 42%	1.83 GB	1.41 GB	3.40 GB	<p><b>trixbox Status</b></p> <p>Hostname: trixbox1.localdomain</p> <p>Local IP: 172.25.105.40</p> <p>Public IP: 132.248.255.82</p> <p>Active Channels SIP: 0 IAX: 0</p> <p>Current Registrations SIP: 1 IAX: 1</p> <p>SIP Peers Online: 0 Offline: 0 Unmonitored: 0</p> <p>IAX2 Peers Online: 0 Offline: 0 Unmonitored: 0</p> <p>Extensions DND</p>
Device	Received	Sent	Err/Drop																																																																											
lo	504.88 KB	504.88 KB	0/0																																																																											
eth0	3.29 MB	4.79 MB	0/0																																																																											
sit0	0.00 KB	0.00 KB	0/0																																																																											
Type	Percent Capacity	Free	Used	Size																																																																										
- Kernel + applications	<div style="width: 27%; border: 1px solid gray; display: inline-block;"></div> 27%	135.57 MB																																																																												
- Buffers	<div style="width: 4%; border: 1px solid gray; display: inline-block;"></div> 4%	22.38 MB																																																																												
- Cached	<div style="width: 34%; border: 1px solid gray; display: inline-block;"></div> 34%	171.39 MB																																																																												
Disk Swap	<div style="width: 0%; border: 1px solid gray; display: inline-block;"></div> 0%	760.88 MB	0.00 KB	760.88 MB																																																																										
Mount	Type	Partition	Percent Capacity	Free	Used	Size																																																																								
/	ext3	/dev/sda2	<div style="width: 46%; border: 1px solid gray; display: inline-block;"></div> 46% (8%)	1.51 GB	1.39 GB	3.06 GB																																																																								
/boot	ext3	/dev/sda1	<div style="width: 18%; border: 1px solid gray; display: inline-block;"></div> 18% (1%)	75.86 MB	17.76 MB	98.72 MB																																																																								
/dev/shm	tmpfs	tmpfs	<div style="width: 0%; border: 1px solid gray; display: inline-block;"></div> 0% (1%)	251.68 MB	0.00 KB	251.68 MB																																																																								
<b>Totals :</b>			<div style="width: 42%; border: 1px solid gray; display: inline-block;"></div> 42%	1.83 GB	1.41 GB	3.40 GB																																																																								

**Helpful Links**

[Forum](#)  
[Recent Posts](#)  
[HUD Lite](#)  
[Video Tutorials](#)  
[Documentation](#)  
[FrOCC](#)  
[Buy Support](#)

This contains server uptime, mounted filesystems, network interfaces, and other services running.

It's also very interesting that a public IP is listed: 132.248.255.82. This system is located in Mexico, apparently belonging to UNAM. (That makes sense since a honeynet event has been hosted at UNAM before.)

\$ whois 132.248.255.82

... abbreviated

```
owner: Universidad Nacional Autonoma de Mexico
ownerid: MX-UNAM1-LACNIC
responsible: DGSCA - NICUNAM
address: Ciudad Universitaria, circuito exterior, s/n,
address: 04510 - Mexico - DF
country: MX
phone: +52 55 56228884 []
owner-c: CIR
tech-c: CIR
abuse-c: CIR
inetrev: 132.248/16
... abbreviated
```

Chaosreader report item number 52:

The registration page shows this as trixbox CE (not SE or EE).

**Chaosreqader report item number 70:**

The /admin/config.php URI shows the following:

Modules available for upgrade:

announcement 2.5.1.9 (current: 2.5.1.8)  
fw\_fop 2.5.0.2 (current: 2.5.0.1)  
framework 2.5.2.3 (current: 2.5.1.5)  
ivr 2.5.20.8 (current: 2.5.20.6)  
weakpasswords 2.5.0.4 (current: 2.5.0.3)  
core 5.5.2.4 (current: 5.5.1.7)  
cidlookup 2.5.0.7 (current: 2.5.0.6)

Statistics

Total active calls: 0  
Internal calls: 0  
External calls: 0  
Total active channels: 0

Connections

IP Phones Online: 1

Other information also available in Chaosreader report item number 44.

**Chaosreader report item number 76:**

Index of /admin/images. A file listing is returned. Listing files, and directory traversal can provide additional attackable surfaces.

**Chaosreader report item number 90:**

A listing of other config files available on the server.

[adsis.conf](#)

[adtranvoivr.conf](#)

[agents.conf](#)

[alarmreceiver.conf](#)

[alsa.conf](#)

[amd.conf](#)

[asterisk.conf](#)

[cbmysql.conf](#)

[cdr\\_custom.conf](#)

[cdr\\_manager.conf](#)

[cdr\\_mysql.conf](#)

[cdr\\_pgsq.conf](#)

[cdr\\_tds.conf](#)

chan\_dahdi.conf  
chan\_dahdi\_additional.conf  
cli.conf  
codecs.conf  
console.conf  
dahdi-channels.conf  
dnsmgr.conf  
dundi.conf  
enum.conf  
extconfig.conf  
extensions-away-status.conf  
extensions.conf  
extensions\_additional.conf  
extensions\_custom.conf  
extensions\_hud.conf  
extensions\_minivm.conf  
extensions\_override\_freepbx.conf  
features.conf  
features\_applicationmap\_additional.conf  
features\_applicationmap\_custom.conf  
features\_featuremap\_additional.conf  
features\_featuremap\_custom.conf  
features\_general\_additional.conf  
features\_general\_custom.conf  
festival.conf  
flite.conf  
followme.conf  
freepbx\_featurecodes.conf  
freepbx\_module\_admin.conf  
func\_odbc.conf  
globals\_custom.conf  
gtalk.conf  
h323.conf  
http.conf

iax.conf  
iax\_additional.conf  
iax\_custom.conf  
iax\_custom\_post.conf  
iax\_general\_additional.conf  
iax\_general\_custom.conf  
iax\_registrations.conf  
iax\_registrations\_custom.conf  
iaxprov.conf  
indications.conf  
jabber.conf  
jingle.conf  
logger.conf  
manager.conf  
manager\_additional.conf  
manager\_custom.conf  
meetme.conf  
meetme\_additional.conf  
mgcp.conf  
minivm.conf  
misdn.conf  
mobile.conf  
modem.conf  
modules.conf  
musiconhold.conf  
musiconhold\_additional.conf  
musiconhold\_custom.conf  
muted.conf  
mysql.conf  
ooh323.conf  
osp.conf  
oss.conf  
phone.conf  
phoneprov.conf

phpagi.conf  
privacy.conf  
queuerules.conf  
queues.conf  
queues\_additional.conf  
queues\_custom.conf  
queues\_custom\_general.conf  
queues\_general\_additional.conf  
queues\_post\_custom.conf  
res\_ldap.conf  
res\_mysql.conf  
res\_odbc.conf  
res\_pgsqll.conf  
res\_snmp.conf  
rpt.conf  
rtp.conf  
say.conf  
sip.conf  
sip\_additional.conf  
sip\_custom.conf  
sip\_custom\_post.conf  
sip\_general\_additional.conf  
sip\_general\_custom.conf  
sip\_nat.conf  
sip\_notify.conf  
sip\_registrations.conf  
sip\_registrations\_custom.conf  
skinny.conf  
sla.conf  
smdi.conf  
udptl.conf  
unistim.conf  
usbradio.conf  
users.conf

vm\_email.inc  
 vm\_general.inc  
 voicemail.conf  
 vpb.conf  
 zapata\_additional.conf

Section 2/ Question 5a. The PCAP includes a (not so) hidden bonus! [hint1: You can't read it in the pcap, hint2: It's a city with an active honeynet chapter]	Possible Points: 10pts
a) Describe it, and explain how you found it.	
Tools Used: Wireshark, mplayer	
Answer	
MEXICO	
"Congratulations, you're listening to an unencrypted VOIP call. The secret password is MEXICO, so write it down and submit your challenge."	
The audio is a call from an attacker repeatedly attempting to enter a PIN to enter a conference room on the PBX server. I used Wireshark's Telephony -> VoIP Calls tool play back the audio of the call.	

Section 2/ Question 5b. If VOIP packets between the two calling parties traverse an untrusted network (eg the wireless/internet) and a similar PCAP was captured by a malicious party, would you think this a security problem? why?	Possible Points: 3pts
Tools Used: Wireshark	
Answer	
Yes, this is definitely a security problem. If SIP data is contained in the capture, it could contain authentication information. While the secret is not sent in plaintext, the username is. An attacker could attempt an offline dictionary or brute force scan to discover the secret.	
Even more damaging is the fact that RTP packets can easily be reassembled and converted to audio. This means that potentially any call could be monitored without the knowledge of the victims. These calls could contain DTMF tones representing passwords or credit card numbers. If this were a VOIP setup for a company with distributed offices, confidential information could easily be discovered that could be disastrous for the company.	

Section 2/ Question 5c. Wireshark has an option "Use RTP timestamp". What is the function of this option?	Possible Points: 2pts
Tools Used: wireshark	
Answer	
The option causes RTP traffic to be reordered according to its timestamp. UDP packets may not arrive in the same order they were sent, which could cause issues with real-time data (VOIP) arriving in a different order than intended. To solve the problem, UDP packets can be rearranged in the correct order (of increasing RTP timestamp).	
In fact, turning this option on makes the VoIP call in question a little bit easier to understand and removes some of the jitter.	

Section 2/ Question 6. What technologies or protocols can be used to protect confidentiality of RTP traffic as it traverses untrusted networks.	Possible Points: 3pts
Tools Used: <a href="http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol">http://en.wikipedia.org/wiki/Secure_Real-time_Transport_Protocol</a>	
Answer	
<p>SRTP can encrypt traffic between two RTP endpoints.</p> <p>A VPN technology such as IPSec could be used between two networks if the RTP devices do not support encryption.</p>	

Section 3/ Question 1. What is "RTP injection" and describe how it functions. What conditions are required to allow this?	Possible Points: 2pts
Tools Used: google <a href="https://www.blackhat.com/presentations/bh-usa-07/Lackey_and_Garbutt/Presentation/bh-usa-07-lackey_and_garbutt.pdf">https://www.blackhat.com/presentations/bh-usa-07/Lackey_and_Garbutt/Presentation/bh-usa-07-lackey_and_garbutt.pdf</a>	
Answer	
<p>RTP injection is when an attacker sends RTP packets to an endpoint of an established RTP session between hosts A and B. It allows an attacker to send audio, which could include DTMF keytones, to the attacked party (B) as though they came from the legitimate party (A).</p> <p>To perform RTP injection, an RTP packet from the source (A) needs to be discovered. If this RTP packet is not encrypted, the attacker can capture this packet and use it as a template. The attacker will alter the sequence number and timestamp, and replace the payload with the attacker's own audio payload, and send it to the victim. The victim (B) will accept the payload as though it came from A.</p> <p>For this to work, the RTP stream between two clients needs to be unencrypted, or the key needs to be known. The RTP stream must also pass through a host that the attacker can use to intercept the traffic.</p>	

Section 3/ Question 2. Explain how a SIP password digest could be intercepted or stolen. Is this a security issue? why or why not.	Possible Points: 2pts
Tools Used: <a href="http://www.net-security.org/secworld.php?id=7263">http://www.net-security.org/secworld.php?id=7263</a>	
Answer	
<p>There are several methods to obtain SIP password digests. A SIP password digest could be intercepted in transit by an attacker monitoring any connection between the SIP user and the SIP server. There is also an exploitable vulnerability in which a SIP phone can be coerced to reveal its password digest by asking it to authenticate against a rogue SIP server. SIP log files also show password digests, so the log files could be stolen either by physical or remote access.</p> <p>This is a security issue. An offline password cracking attempt can be performed on the intercepted key, using one or many computers. This is a much more efficient cracking method than guessing passwords on a live system (like svcrack does).</p>	

Section 3/ Question 3. Is DDoS a threat to VOIP systems? Are there any general functional requirements of telephony systems that would be impaired by a DDoS?	Possible Points: 2pts
Tools Used:	
Answer	
<p>Yes, DDoS is a threat to VOIP systems. It is a general requirement that VOIP systems support Quality of Service. If enough traffic was generated to consistently delay RTP packets, a VOIP call could be jittery, unintelligible, or not work at all.</p>	

## Appendix

### sipgrep.pl

```
#!/usr/bin/perl

# This tool applies a regexp to an entire log event, and prints the event if
# that regexp matches.  Log events are separated by "-----".
#
# usage: ./sipgrep.pl <regexp> <filename>

use strict;
my ($REGEX, $LOGFILE) = @ARGV;

open(IN,"<$LOGFILE");

my $event="";
while (<IN>) {
    $event .= $_;

    if (/^---/) {
        print $event if $event =~ /$REGEX/;
        $event = "";
    }
}
```