Beginning analysis of the SSU attack-defense CTF packet capture corpus

Grant Fonseca and Mark Gondree

Computer Science Department, Sonoma State University

SSU Attack-Defense Corpus

- Comprised of network data recorded during Attack-Defense CTF.
- Represents 21 games, primarily the iCTF and DEFCON games.
- Presents opportunity to research CTFs as educational tools and the players

Why Attack-Defense?

Format praised for education, training, assessment.

This project: DEFCON 22 game data

- 20 teams competed in Las Vegas
- Aug 8, 2014 — Aug 10, 2014
- Contestants must qualify to compete
- Winning team gets:
  - Qualified to compete in DEFCON 23 CTF
  - free registration to all future DEFCON events

Teams	Size of pcaps	Number of Packets	Score
gallopsled	153 GB	543,807,786	921
hitcon	46 GB	234,471,087	7833
ppp	30 GB	130,868,827	11263
shellphish	22 GB	111,024,707	899
balalaikacr3w	19 GB	70,657,470	937
codered	15 GB	69,076,065	997
hackingforchimac	15 GB	55,976,008	546
kaist	15 GB	64,079,228	1334
mslc	14 GB	68,880,637	1248
raon_asrt	14 GB	65,863,338	2281
blue-lotus	13 GB	61,079,444	3233
mmbih	9.2 GB	44,507,219	2594
dragonsector	7.8 GB	35,110,744	4421
reckless	7.8 GB	38,647,458	4020
w3stormz	7.5 GB	32,668,640	987
stratum	7.1 GB	39,542,748	1529
team9447	6.5 GB	33,400,052	1519
penthackon	6.2 GB	22,420,439	979
routards	5.4 GB	28,437,005	1262
binja	3.4 GB	19,376,967	1153

Acknowledgments

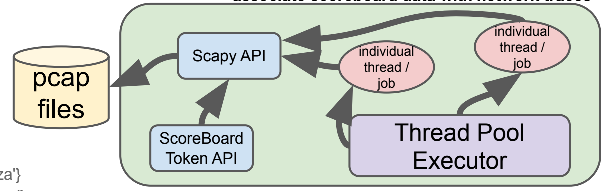
Thank you to collaborators with prior work on this project: Jonathan Soto (SSU), Gabriel Duarte, Dylan Curry (SSU).

1) Matching tokens with exploiters and targets in network traces using scoreboard data

Explored two approaches

1. Using ***ngrep***
   - Fast, mature, professional tool
   - Requires some secondary tool to "further explore" the pcap
   - Ex: extract timing information, payload data, etc.
2. Using the ***scapy*** library
   - Basically, "build your own network analysis tool"

The software architecture of our ad-hoc tool set to associate scoreboard data with network traces



First iteration of our tool

idea: extensible, multi-threaded ngrep

- pulls partial tokens from scoreboard
- removes duplicates
- uses scapy to parse pcaps
- searches for multiple tokens simultaneously

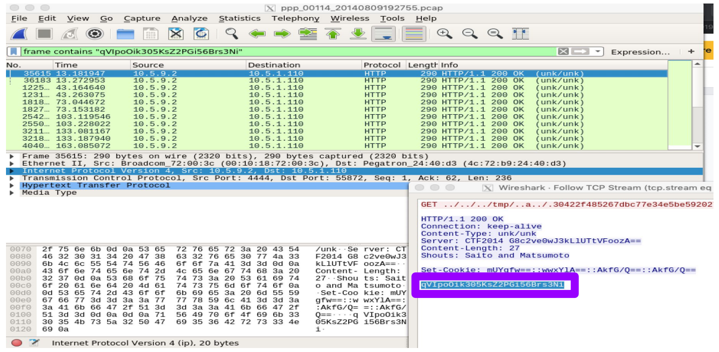
Example: Scoreboard data of tokens recovered in rounds 175--176

```
{'round': 175, 'token': '4emlfzRyzUb3n', 'owner': 'Gallopsled', 'exploiter': 'Routards', 'service': 'eliza'}
{'round': 175, 'token': '4emlfzRyzUb3n', 'owner': 'Gallopsled', 'exploiter': 'blue-lotus', 'service': 'eliza'}
{'round': 175, 'token': '4emlfzRyzUb3n', 'owner': 'Gallopsled', 'exploiter': 'Reckless Abandon', 'service': 'eliza'}
{'round': 175, 'token': 'p12kT5jKo9Zky', 'owner': 'Gallopsled', 'exploiter': 'blue-lotus', 'service': 'wdub'}
{'round': 176, 'token': 'oYPCWUjTHaUft', 'owner': 'raon_ASRT', 'exploiter': 'More Smoked Leet Chicken', 'service': 'justify'}
{'round': 176, 'token': 'oYPCWUjTHaUft', 'owner': 'raon_ASRT', 'exploiter': 'Plaid Parliament of Pwning', 'service': 'justify'}
{'round': 176, 'token': '4Ys27GiHsD9lo', 'owner': '9447', 'exploiter': 'More Smoked Leet Chicken', 'service': 'justify'}
{'round': 176, 'token': '[illegible]', 'owner': 'raon_ASRT', 'exploiter': 'Reckless Abandon', 'service': 'eliza'}
{'round': 176, 'token': 'LzaGQ3k5viLBQ', 'owner': 'Plaid Parliament of Pwning', 'exploiter': 'HITCON', 'service': 'eliza'}
{'round': 176, 'token': 'qloi35s2G5BsN', 'owner': 'Routards', 'exploiter': 'HITCON', 'service': 'eliza'}
```

2) Searching for attack payloads manually

Partial token from Scoreboard database: qloi35s2G5BsN

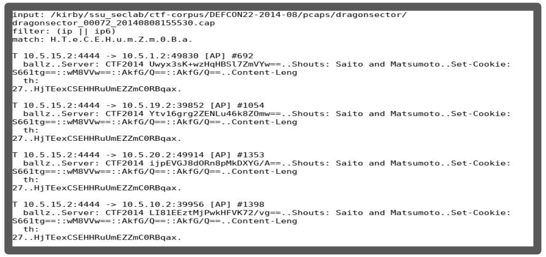
Regular Expression of Token: q.l.o.i.3.5.s.2.G.5.B.s.N.


ppp_00114_20140809192755.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
Wireshark · Follow TCP Stream (tcp.stream eq

```
frame contains "qVIpoOik305KsZ2PGi56Brs3Ni"

No.      Time        Source      Destination   Protocol Length Info
  35615  13.181947   10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  36183  13.272953   10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  1225…  43.164640   10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  1231…  43.263075   10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  1818…  73.044672   10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  1827…  73.153182   10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  2542…  103.119546  10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  2550…  103.228022  10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  3211…  133.081167  10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  3218…  133.187940  10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)
  4040…  163.085072  10.5.9.2    10.5.1.110    HTTP     290 HTTP/1.1 200 OK  (unk/unk)

▸ Frame 35615: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits)
▸ Ethernet II, Src: Broadcom_72:00:3c (00:10:18:72:00:3c), Dst: Pegatron_24:40:d3 (4c:72:b9:24:40:d3)
▸ Internet Protocol Version 4, Src: 10.5.9.2, Dst: 10.5.1.110
▸ Transmission Control Protocol, Src Port: 4444, Dst Port: 55872, Seq: 1, Ack: 62, Len: 236
▸ Hypertext Transfer Protocol
▸ Media Type

0070  2f 75 6e 6b 0d 0a 53 65  72 76 65 72 3a 20 43 54   /unk··Se rver: CT
0080  46 32 30 31 34 20 47 38  63 32 76 65 30 77 4a 33   F2014 G8 c2ve0wJ3
0090  6b 4c 6c 55 54 74 56 46  6f 6f 7a 41 3d 3d 0d 0a   kLlUTtVF oozA==··
00a0  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length: 
00b0  32 37 0d 0a 53 68 6f 75  74 73 3a 20 53 61 69 74   27··Shou ts: Sait
00c0  6f 20 61 6e 64 20 4d 61  74 73 75 6d 6f 74 6f 0a   o and Ma tsumoto·
00d0  0d 53 65 74 2d 43 6f 6f  6b 69 65 3a 20 6d 55 59   ·Set-Coo kie: mUY
00e0  67 66 77 3d 3d 3a 3a 77  77 78 59 6c 41 3d 3d 3a   gfw==::w wxYlA==:
00f0  3a 41 6b 66 47 2f 51 3d  3d 3a 3a 41 6b 66 47 2f   :AkfG/Q= =::AkfG/
0100  51 3d 3d 0d 0a 0d 0a 71  56 49 70 6f 4f 69 6b 33   Q==····q VIpoOik3
0110  30 35 4b 73 5a 32 50 47  69 35 36 42 72 73 33 4e   05KsZ2PG i56Brs3N
0120  69 0a                                              i·

Internet Protocol Version 4 (ip), 20 bytes

GET ../../../tmp/..a../.30422f485267dbc77e34e5be59202

HTTP/1.1 200 OK
Connection: keep-alive
Content-Type: unk/unk
Server: CTF2014 G8c2ve0wJ3kLlUTtVFoozA==
Content-Length: 27
Shouts: Saito and Matsumoto

Set-Cookie: mUYgfw==::wwxYlA==::AkfG/Q==::AkfG/Q==
qVIpoOik305KsZ2PGi56Brs3Ni
```

3) Searching for attack payloads with software tools

Example output of ngrep matching a particular regular expression



```
input: /kirby/ssu_seclab/ctf-corpus/DEFCON22-2014-08/pcaps/dragonsector/
dragonsector_00072_20140808155530.cap
filter: (ip || ip6)
match: H.T.e.C.E.H.u.m.Z.m.0.B.a.

T 10.5.15.2:4444 -> 10.5.1.2:49830 [AP] #692
  ballz..Server: CTF2014 Uwyx3sK+wzHqHBSl7ZmVYw==..Shouts: Saito and Matsumoto..Set-Cookie:
S661tg==::wM8VVw==::AkfG/Q==::AkfG/Q==..Content-Leng
  th:
27..HjTEexCSEHHRuUmEZZmC0RBqax.

T 10.5.15.2:4444 -> 10.5.19.2:39852 [AP] #1054
  ballz..Server: CTF2014 Ytv16grg2ZENLu46k8ZOmw==..Shouts: Saito and Matsumoto..Set-Cookie:
S661tg==::wM8VVw==::AkfG/Q==::AkfG/Q==..Content-Leng
  th:
27..HjTEexCSEHHRuUmEZZmC0RBqax.

T 10.5.15.2:4444 -> 10.5.20.2:49914 [AP] #1353
  ballz..Server: CTF2014 ijpEVGJ8dORn8pMkDXYG/A==..Shouts: Saito and Matsumoto..Set-Cookie:
S661tg==::wM8VVw==::AkfG/Q==::AkfG/Q==..Content-Leng
  th:
27..HjTEexCSEHHRuUmEZZmC0RBqax.

T 10.5.15.2:4444 -> 10.5.10.2:39956 [AP] #1398
  ballz..Server: CTF2014 LI81EEztMjPwkHFVK72/vg==..Shouts: Saito and Matsumoto..Set-Cookie:
S661tg==::wM8VVw==::AkfG/Q==::AkfG/Q==..Content-Leng
  th:
27..HjTEexCSEHHRuUmEZZmC0RBqax.
```

Finds all occurances of a particular regular expression

Limitations motivate building a custom tool

- one regular expression at a time, one file at a time
- output difficult to parse (need to refer to pcap for more info)