

# Visual Threat Hunting

By Ryan Nolette  
Security Technologist

# What am I trying to accomplish?

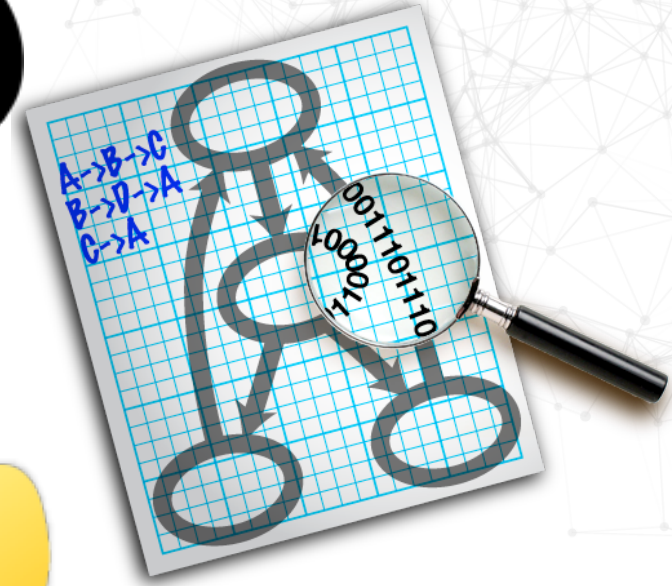


- ◆ Perform a Threat Hunt
  - ◆ Find internal hosts beaconing out
- ◆ Explain what I found to my management
- ◆ Justify my time to Hunt

# Tools used in this talk



- Bro sensor - <https://www.bro.org/>
  - Configured to output logs to json
- Graphviz - <http://www.graphviz.org/>
  - To create visuals of the data bro is producing
- Python - <https://www.python.org/>
  - To convert bro data to graphviz formatting
  - <https://github.com/sonofagl1tch/visualization/tree/master/VisualThreatHunting>
- Centos 7 minimal server to run bro
  - Because the GUI makes you weak



CentOS



# Log Crawling

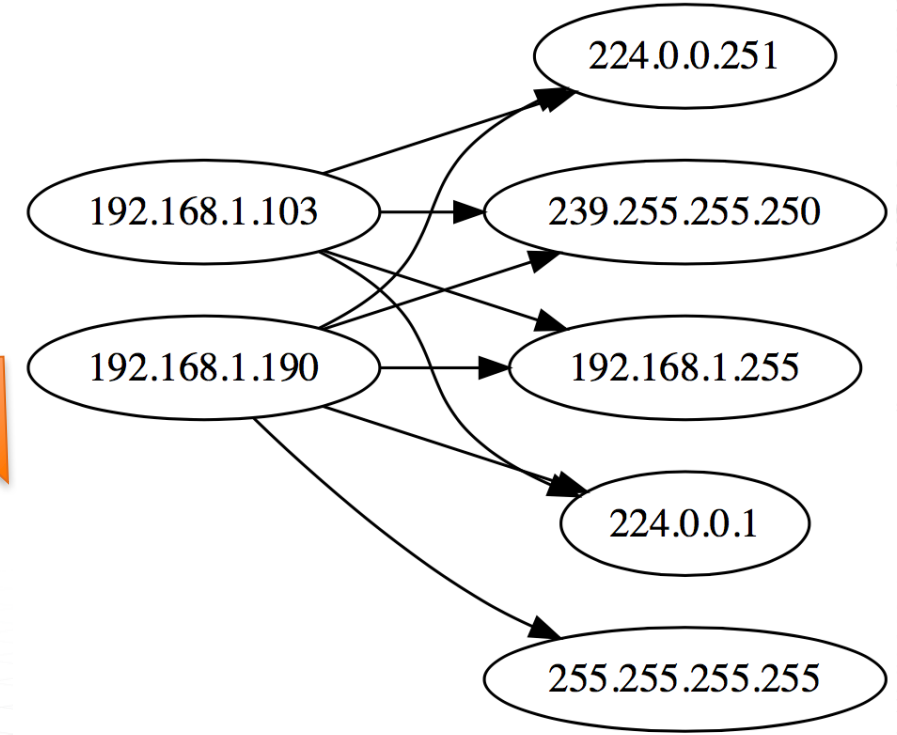
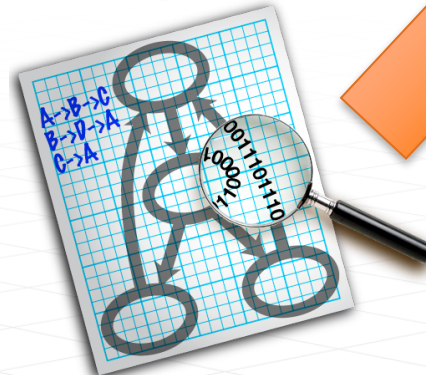
- What systems if any are beaconing out?
- Where did it beacon out?
- How do I know it was beaconing and not legitimate traffic?

```
{ "ts": "2017-05-02T08:58:57.049184Z", "uid": "CkEcDYCQ080oILf2", "id.orig_h": "192.168.1.143", "id.orig_p": 49204, "id.resp_h": "239.255.255.250", "id.resp_p": 1900, "proto": "udp", "duration": 2.96896, "orig_bytes": 700, "resp_bytes": 0, "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 4, "orig_ip_bytes": 812, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:01.861092Z", "uid": "CTMvnq1IvK0oM5H8Cb", "id.orig_h": "fe80::a22b:b8ff:fe60:965d", "id.orig_p": 546, "id.resp_h": "ff02::1:2", "id.resp_p": 547, "proto": "udp", "conn_state": "S0", "local_orig": false, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 146, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:02.168225Z", "uid": "CQ5hON2ftGeiU1dJ0c", "id.orig_h": "fe80::10f2:85f6:ef79:c762", "id.orig_p": 143, "id.resp_h": "ff02::16", "id.resp_p": 0, "proto": "icmp", "conn_state": "OTH", "local_orig": false, "local_resp": false, "missed_bytes": 0, "orig_pkts": 1, "orig_ip_bytes": 116, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:02.373484Z", "uid": "C4Wfwf4gy8vDeHgXqk", "id.orig_h": "192.168.1.99", "id.orig_p": 68, "id.resp_h": "192.168.1.1", "id.resp_p": 67, "proto": "udp", "service": "dhcp", "conn_state": "S0", "local_orig": true, "local_resp": true, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 336, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:58:59.608627Z", "uid": "C1B6K61MUA0U6AV15", "id.orig_h": "192.168.1.103", "id.orig_p": 50498, "id.resp_h": "239.255.255.250", "id.resp_p": 1900, "proto": "udp", "duration": 2.96972, "orig_bytes": 700, "resp_bytes": 0, "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 4, "orig_ip_bytes": 812, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:02.782701Z", "uid": "CDdYP827cVsEEtj3l", "id.orig_h": "192.168.1.190", "id.orig_p": 50837, "id.resp_h": "192.168.1.255", "id.resp_p": 8612, "proto": "udp", "conn_state": "S0", "local_orig": true, "local_resp": true, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 44, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:02.782717Z", "uid": "C0yMD426ckvdQPYG88", "id.orig_h": "192.168.1.190", "id.orig_p": 62326, "id.resp_h": "224.0.0.1", "id.resp_p": 8612, "proto": "udp", "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 44, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:00.532818Z", "uid": "CjBg0C1GQZalFbNIA8", "id.orig_h": "192.168.1.139", "id.orig_p": 61809, "id.resp_h": "239.255.255.250", "id.resp_p": 1900, "proto": "udp", "duration": 3.069253, "orig_bytes": 696, "resp_bytes": 0, "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 4, "orig_ip_bytes": 808, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:05.137956Z", "uid": "Ca6wuQDuWDrNaatv3", "id.orig_h": "192.168.1.98", "id.orig_p": 55679, "id.resp_h": "192.168.1.255", "id.resp_p": 8612, "proto": "udp", "conn_state": "S0", "local_orig": true, "local_resp": true, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 44, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:05.138017Z", "uid": "C0fyhN2rPMsVxKaak5", "id.orig_h": "192.168.1.98", "id.orig_p": 53943, "id.resp_h": "224.0.0.1", "id.resp_p": 8612, "proto": "udp", "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 44, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:05.445329Z", "uid": "CwhfDf4hDN8jhiMeg5", "id.orig_h": "192.168.1.103", "id.orig_p": 65507, "id.resp_h": "192.168.1.255", "id.resp_p": 8612, "proto": "udp", "conn_state": "S0", "local_orig": true, "local_resp": true, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 44, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:05.445340Z", "uid": "CrUzb2X89R06epvsi", "id.orig_h": "192.168.1.103", "id.orig_p": 57063, "id.resp_h": "224.0.0.1", "id.resp_p": 8612, "proto": "udp", "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 44, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:59:56.237795Z", "uid": "CyqgAw3Z1b2jXI6Kri", "id.orig_h": "192.168.1.73", "id.orig_p": 5353, "id.resp_h": "224.0.0.251", "id.resp_p": 5353, "proto": "udp", "service": "dns", "conn_state": "S0", "local_orig": true, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 143, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
{ "ts": "2017-05-02T08:58:59.199071Z", "uid": "CKEdXM13bhgvwjqi5", "id.orig_h": "fe80::10f2:85f6:ef79:c762", "id.orig_p": 133, "id.resp_h": "ff02::2", "id.resp_p": 134, "proto": "icmp", "duration": 8.703862, "orig_bytes": 16, "resp_bytes": 0, "conn_state": "OTH", "local_orig": false, "local_resp": false, "missed_bytes": 0, "history": "D", "orig_pkts": 1, "orig_ip_bytes": 16, "resp_pkts": 0, "resp_ip_bytes": 0, "tunnel_parents": [] }
```



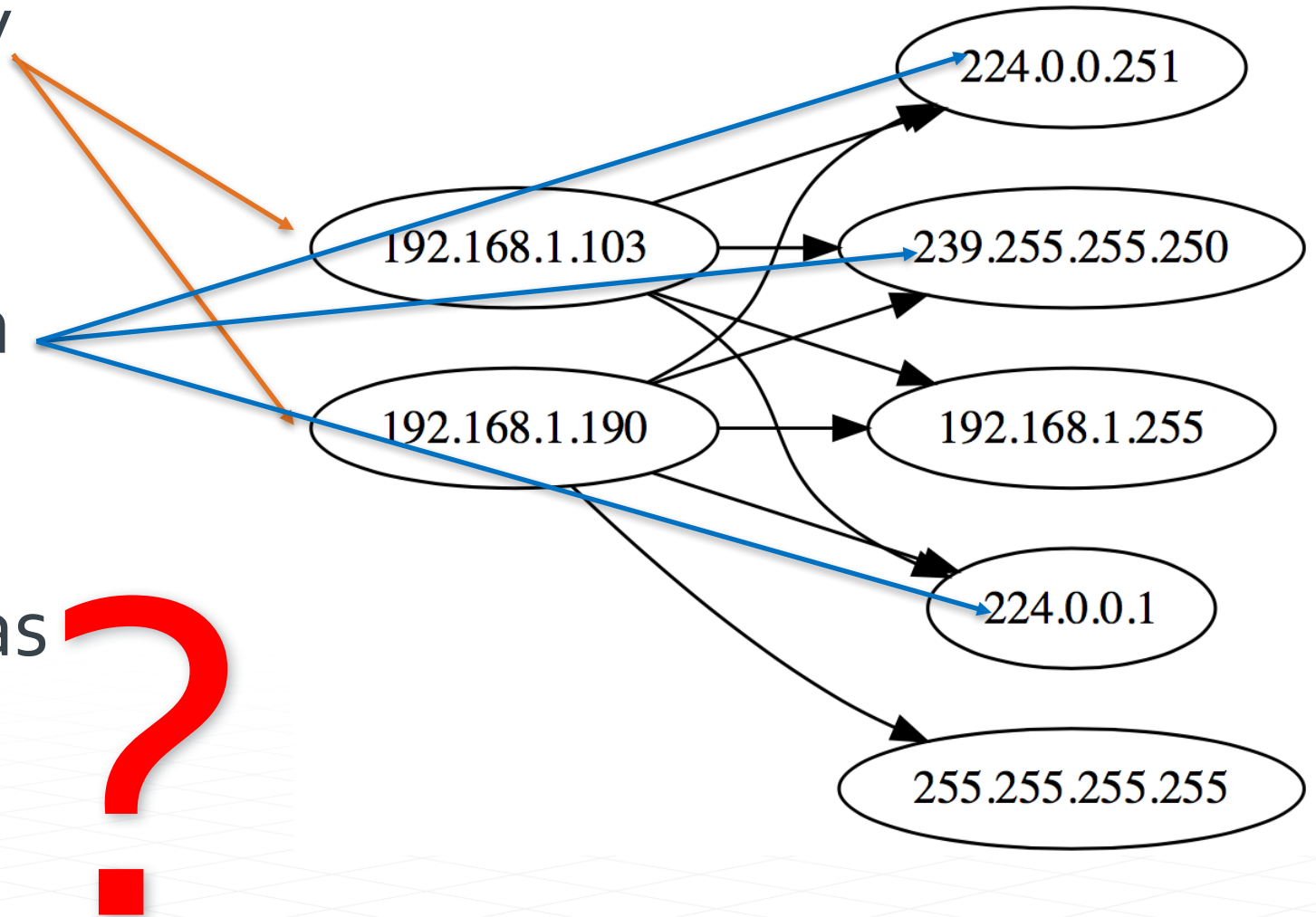
# Process: High Level

```
{
  "ts": "2017-05-02T08:58:57.049184Z",
  "uid": "CkEcDTYCQO80oIlF2",
  "id.orig_h": "192.168.1.143",
  "id.orig_p": 49204,
  "id.resp_h": "239.255.255.250",
  "id.resp_p": 1900,
  "proto": "udp",
  "duration": 2.96896,
  "orig_bytes": 700,
  "resp_bytes": 0,
  "conn_state": "S0",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 4,
  "orig_ip_bytes": 812,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
}
```



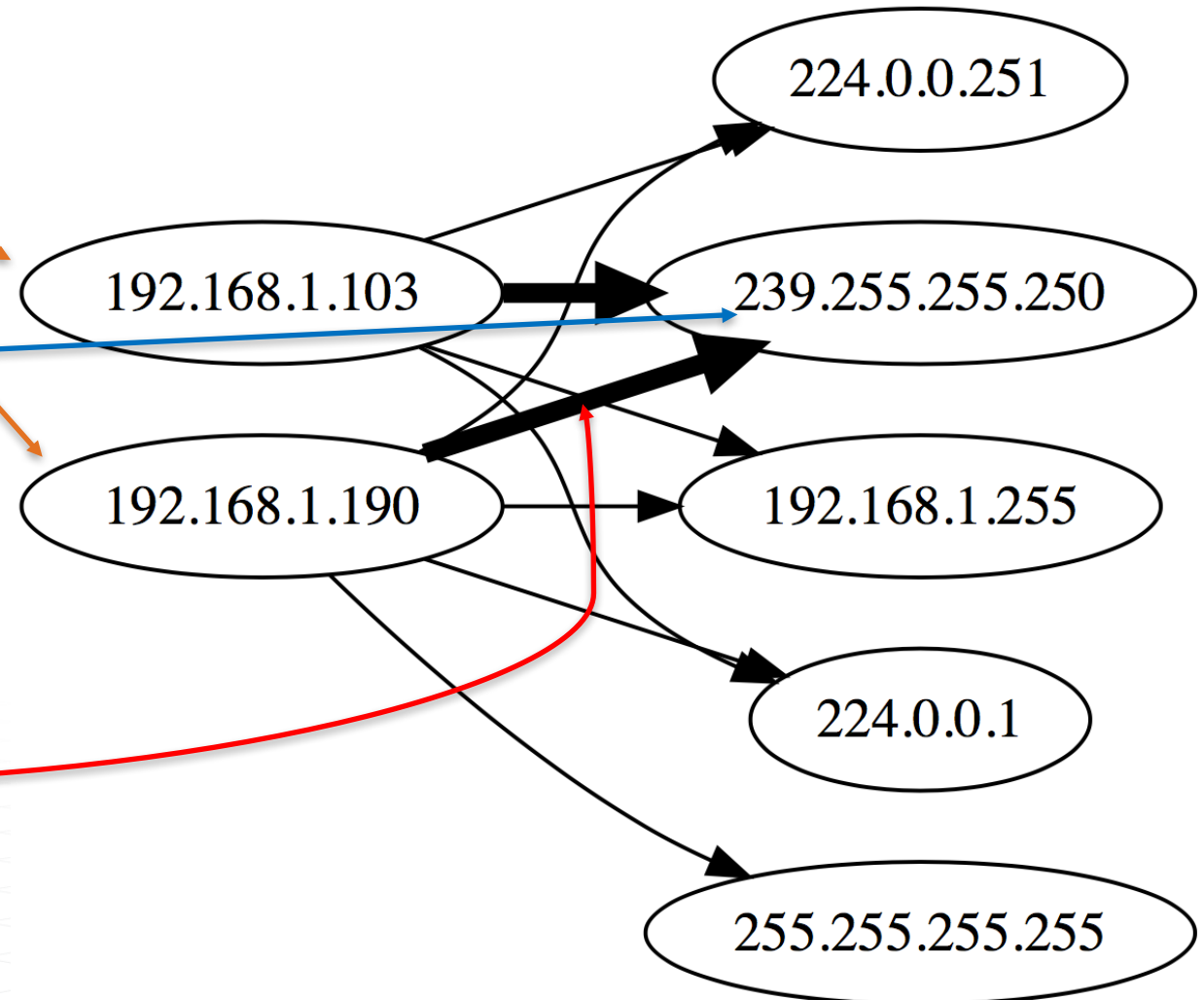
# relationships

- What systems if any are beaconing out?
- Where did it beacon out?
- How do I know it was beaconing and not legitimate traffic?



# Explain what I found to my management

- What systems if any are beaconing out?
- Where did it beacon out?
- How do I know it was beaconing and not legitimate traffic?



# Justify my time to Hunt



## Log Crawling

- Cost of hunt
- 8 hours
- \$50/hr
- \$400/day

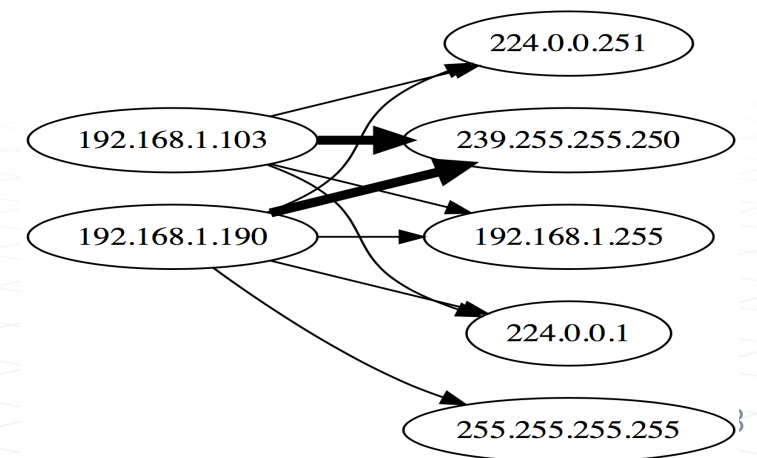
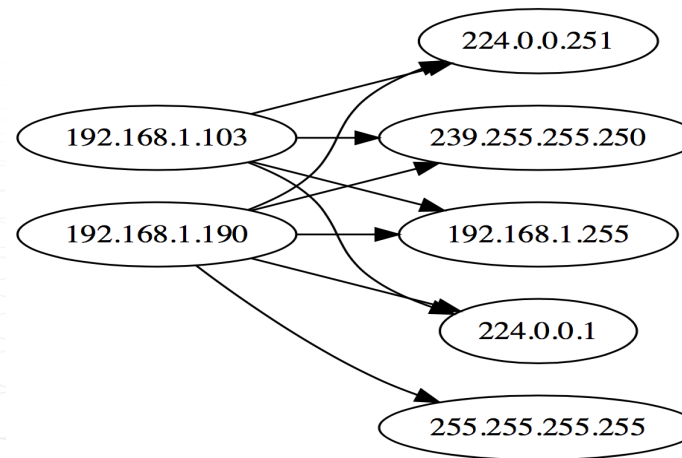
## Explain what I found to my management

- Cost of hunt
- 4 hours
- \$50/hr
- \$200/day

## Actionable Hunting

- Cost of hunt
- 2 hours
- \$50/hr
- \$100/day

```
{
  "ts": "2017-05-02T08:59:51.041042",
  "user": "CCKdYlC0886117",
  "id.orig_h": "192.168.1.143",
  "id.orig_p": 49284,
  "id.resp_h": "239.255.255.250",
  "id.resp_p": 1980,
  "proto": "udp",
  "duration": 2.68886,
  "orig_bytes": 180,
  "resp_bytes": 0,
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 4,
  "orig_ip_bytes": 812,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:51.0618922",
  "user": "CTWvq11V80H9HCB",
  "id.orig_h": "fe80::a22b:b8ff:fe8b:9e58",
  "id.orig_p": 1546,
  "id.resp_h": "ff02::1:2",
  "id.resp_p": 147,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": false,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 146,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:52.1482252",
  "user": "CQ3H02fG6u1u3d3d",
  "id.orig_h": "fe80::18f2:85f6:ef79:c762",
  "id.orig_p": 143,
  "id.resp_h": "ff02::1:2",
  "id.resp_p": 187,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": false,
  "local_resp": false,
  "missed_bytes": 0,
  "orig_pkts": 1,
  "orig_ip_bytes": 116,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:52.3734842",
  "user": "C4Wf4dybVb0h9kq",
  "id.orig_h": "192.168.1.99",
  "id.orig_p": 68,
  "id.resp_h": "192.168.1.1",
  "id.resp_p": 67,
  "proto": "udp",
  "service": "DHCP",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": true,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 339,
  "resp_pkts": 18,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.686272",
  "user": "C186K61M0V8U6AV15",
  "id.orig_h": "192.168.1.183",
  "id.orig_p": 50498,
  "id.resp_h": "239.255.255.250",
  "id.resp_p": 1980,
  "proto": "udp",
  "duration": 2.95972,
  "orig_bytes": 1789,
  "resp_bytes": 0,
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 4,
  "orig_ip_bytes": 822,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:52.762703",
  "user": "C0dP927v5EEt31",
  "id.orig_h": "192.168.1.190",
  "id.orig_p": 150837,
  "id.resp_h": "192.168.1.255",
  "id.resp_p": 18612,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": true,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 144,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:52.7627172",
  "user": "C0YMD426kvdDPG88",
  "id.orig_h": "192.168.1.190",
  "id.orig_p": 62326,
  "id.resp_h": "224.0.0.1",
  "id.resp_p": 8612,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 44,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:58.533818",
  "user": "C186K61M0V8U6AV15",
  "id.orig_h": "192.168.1.139",
  "id.orig_p": 61889,
  "id.resp_h": "239.255.255.250",
  "id.resp_p": 1980,
  "proto": "udp",
  "duration": 3.00253,
  "orig_bytes": 690,
  "resp_bytes": 0,
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 4,
  "orig_ip_bytes": 188,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.337952",
  "user": "C0dP927v5EEt31",
  "id.orig_h": "192.168.1.99",
  "id.orig_p": 155679,
  "id.resp_h": "192.168.1.255",
  "id.resp_p": 18612,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": true,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 144,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.338112",
  "user": "C0YMD426kvdDPG88",
  "id.orig_h": "192.168.1.90",
  "id.orig_p": 153943,
  "id.resp_h": "224.0.0.1",
  "id.resp_p": 8612,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 144,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.4453202",
  "user": "C0YMD426kvdDPG88",
  "id.orig_h": "192.168.1.183",
  "id.orig_p": 65587,
  "id.resp_h": "192.168.1.255",
  "id.resp_p": 18612,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": true,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 144,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.4453462",
  "user": "C0YMD426kvdDPG88",
  "id.orig_h": "192.168.1.183",
  "id.orig_p": 157083,
  "id.resp_h": "224.0.0.1",
  "id.resp_p": 8612,
  "proto": "udp",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": true,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 144,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.237792",
  "user": "C0YMD426kvdDPG88",
  "id.orig_h": "192.168.1.73",
  "id.orig_p": 15353,
  "id.resp_h": "224.0.0.1",
  "id.resp_p": 8612,
  "proto": "udp",
  "service": "DHCP",
  "conn_state": "SR",
  "local_orig": true,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 144,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
},
{
  "ts": "2017-05-02T08:59:59.1598712",
  "user": "C0YMD426kvdDPG88",
  "id.orig_h": "fe80::18f2:85f6:ef79:c762",
  "id.orig_p": 133,
  "id.resp_h": "ff02::1:2",
  "id.resp_p": 133,
  "proto": "udp",
  "duration": 0.78893,
  "orig_bytes": 10,
  "resp_bytes": 0,
  "conn_state": "SR",
  "local_orig": false,
  "local_resp": false,
  "missed_bytes": 0,
  "history": "D",
  "orig_pkts": 1,
  "orig_ip_bytes": 10,
  "resp_pkts": 0,
  "resp_ip_bytes": 0,
  "tunnel_parents": []
}
```





# Questions?

"I use Sqrri to find those dark places in my environment, poke it with a stick, and see what crawls out."  
-Ryan Nolette

