Network Security Monitoring

Network Startup Resource Center
www.nsrc.org

Where is the “security” button?

- Securing a computer or a network of computers is hard!
- Vendors will gladly say, “buy my widget and your data will be secure”
- There is no single solution that will ensure that your systems don’t “get hacked”

Need proof?

- **… $6.7m in South African cyber bank robbery**
  https://nakedsecurity.sophos.com/2012/01/20/hackers-snatch-6-7m-in-south-african-cyber-bank-robbery/
- **… SONY GOT HACKED HARD...**
  http://www.wired.com/2014/12/sony-hack-what-we-know/
- **...Cyberspy Attack Hacked Southeast Asian Targets...**
  http://www.bloomberg.com/news/articles/2015-04-12/decade-long-cyber-spying-campaign-hacked-southeast-asia-targets

What to do?

- Accept that being compromised is inevitable
- Understand which resources you want to protect
  - Database servers?
  - Students?
  - End-users in accounting department?
  - All of the above?
- Monitor resources very closely!

Network traffic is interesting for security because...

- **Its ubiquitous** – most devices connect to it, one can monitor network connected light switches, Windows servers and Mac workstations using the same methodologies
- **It tells the truth** – if you're monitoring the link of a compromised host, the traffic leaving the host will appear in your network logs, even if the traffic is obscured
- **It has really useful data –** Malware families and attackers often reuse their attack infrastructure (domain names, IP addresses, SSL certificates, etc.) If you know that certain domains are bad, you can match against them in network traffic and find other affected hosts

What is Network Security Monitoring?

- NSM is a fresh name for practices that have been around for a long time:
  - Network flow analysis
  - Network intrusion detection

- A tool that calls itself a “network security monitor” generally has two functions:
  - Regex packet matching against threat intelligence
  - Protocol parsing, network metadata logging

Sensor inputs and outputs

- INPUT – Traffic captured from your network
  - SPAN Port
  - Physical tap
- OUTPUT – Log files
  - Alert logs for matches against threat intelligence
  - Network metadata logs

Terminology: Threat Intelligence

- **Threat intelligence** is a collection of information about an adversary's infrastructure or tactics that can be used to detect the presence of the adversary

- Threat intelligence can be curated by your organization, bought, or acquired for free on the Internet from groups like Emerging Threats (http://www.emergingthreats.net/open-source/etopen-ruleset)

Threat Intelligence: (Suricata)

- `alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Fake Antivirus Download ws.exe"; flow:established,to_server; content:"GET"; http_method; content:"/install/ws.exe"; http_uri; nocase; reference:url,doc.emergingthreats.net/2010051; classtype:trojan-activity; sid:2010051; rev:4;`

Network Protocol Metadata

- Data pertaining to the information contained in a network flow, including but not limited to:
  - End-points addresses – source address, destination address, source port, destination port
  - Statistics – byte counts, connection durations, …
  - Protocol information – DNS queries, SSL certificate DN's, user-agent strings

Using Network Protocol Metadata

- **Detecting unknown threats**
  - Blacklists can only alert you to threats that you (or your community) knows about.
  - Large security organizations often have “hunt” teams to sift through and analyze this data and look for anomalies
- **Incident response**
  - In the case that your organization discovers a breach, its very helpful to have forensic data to understand the scope and timeline of the intrusion

Example Metadata


```
{"timestamp":"2015-06-
23T18:27:40.634114","event_type":"dns","src_ip":"
10.10.0.241","src_port":53,"dest_ip":"10.10.2.5",
"dest_port":54948,"proto":"UDP","dns":
{"type":"answer","id":10275,"rrname":"wikipedia.o
rg","rrtype":"NS","ttl":20864}}
```

Placing an NSM Sensor

First deploy NSM sensors at the Internet edge, then expand to the inside of the network

- The internet is where most the attackers arrive from
- The internet is the easiest data exfiltration channel to use (if its available)

Network data acquisition

Deciding where to tap in your network:

- How much traffic does the tap see?
- Does the tap see both ingress and egress traffic?
- Is there NAT in your network? Will your tap see traffic pre or post NAT?
- How will you acquire data? Taps? SPAN?

Network Data Acquisition: Taps

- A network tap is a hardware device which provides a way to access the data flowing across a computer network.

  http://en.wikipedia.org/wiki/Network_tap

- Taps are the preferred method for acquiring network data, especially in cases when physical networks are the data source.

Taps: Pros / Cons

- Pros
  - Taps are passive, they do not alter the contents of the network traffic that you are delivering
  - Taps do not drop packets. When acquiring data from a tap you can be confident of the integrity of the captured data.
- Cons
  - Expensive
  - Require physical infrastructure (Fiber, network interfaces, tap aggregators)

Network Data Acquisition: SPAN

The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer from a network switch

SPAN: Pros / Cons

- Pros
  - Low cost - Often it can be configured on hardware you already have in your network
  - Easy to deploy - Takes no network downtime (TAPs require network links to flow through them)
- Cons
  - Utilize switch resources, prone to reducing performance on your network infrastructure
  - Prone to modification of network traffic

NSM Sensor: Suricata

- Open source NSM / IDS / IPS tool
- Created by the founder of Emerging Threats
- Compatible with Snort rules
- Multi-threaded
- Parses SSL, HTTP, DNS metadata
- Capable of IPS (inline, blocking “bad” flows)
- Multi-threaded, scales to 10GB and beyond

Suricata: Output

- Logs located at /var/log/suricata:
  - fast.log (ASCII alert log)
  - unified2.alert.* (ASCII alert and packet dump from offending traffic)
  - dns.log (optional – log of all DNS queries captured)
  - http.log (optional – log of all HTTP sessions captured)
  - tls.log (optional – log of all TLS sessions captured)

Suricata: Configuration

- YAML file at '/etc/suricata/suricata.yml'
- Used to configure:
  - Rule sets (emerging-malware.rules, ...)
  - Monitored interfaces (eth0, eth1, ...)
  - Monitored networks (HOME_NET, DNS_SERVERS ...)
  - Capture modes (PF_RING, AF_PACKET, ...)

Installing & Configuring Suricata