# IDS Rules

@Cody Welu 2023

# IDS

- IDS = Intrusion Detection System
- We're looking deeper into the packets than a firewall would
  - Looking at source/destination/protocol
  - Looking at the contents of the packets (data) too
- Use signatures for known bad
- Anomaly detection
  - Something looks different than normal?
    - Maybe it's bad…

@Cody Weiu 2023

# IDS Software

- Snort
  - Open source IDS/IPS
  - Created in 1998
  - Currently developed by Cisco
- Suricata
  - Open source IDS/IPS
  - First standard release in 2010
  - Develooped by the Open Information Security Foundation (OISF)

@Lody Welu 2023

# Snort vs. Suricata

- Price: Well, they're both open source, so… Free!
- Snort has been the de-facto standard IDS
- Suricata is multi-threaded
  - Not everyone agrees this is better
- Suricata includes lots of protocol extractors
  - Example: Rule can look at just the HTTP Request type rather than the whole packet
- Suricata can (mostly) use Snort rules

@Cody_Wells_2023

# IDS Rules

- Many rules come with Snort and Suricata
- You can write your own rules, but you can't write them for everything
  - All the vulnerabilities
  - All the exploits
  - All the policy violations
- Free rulesets
- Paid rulesets

```
# This Ruleset is EmergingThreats Open optimized for suricata-2.0-enhanced.

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Adob
flow:to_client,established; content:"PDF-"; depth:300; content:"this.media.newP
reference:url,www.metasploit.com/redmine/projects/framework/repository/revision
reference:url,vrt-sourcefire.blogspot.com/2009/12/adobe-reader-medianewplayer-a
user; sid:2010495; rev:13; metadata:affected_product Web_Browsers, affected_pro
Web_Client_Attacks, signature_severity Major, created_at 2010_07_30, updated_at

alert http $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET WEB_CLIENT Possi
flow:established,to_client; content:"|0d 0a|%FDF-"; depth:600; content:"/F(Java
reference:cve,2009-3956; reference:url,doc.emergingthreats.net/2010664; referen
001_Stratsec_Acrobat_Script_Injection_Security_Advisory_v1.0.pdf; classtype:att
affected_product Web_Browser_Plugins, attack_target Client_Endpoint, deployment
2010_07_30, updated_at 2016_07_01;)

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET WEB_CLIENT Possible Foxi
flow:to_client,established; content:"PDF-"; depth:300; content:"Launch"; distan
reference:url,www.kb.cert.org/vuls/id/570177; reference:url,www.h-online.com/se
979286.html; reference:url,www.sudosecure.net/archives/673; reference:url,www.h
vulnerability-971932.html; reference:url,blog.didierstevens.com/2010/03/31/esca
Used-to-Install-Zeus.trace.1301-.asp; reference:url,doc.emergingthreats.net/201
```

@Lodu Wolu 2023

# Rulesets

- ET = Emerging Threats
- ET Open
  - Primarily Suricata
  - Free
- ET Pro (Proofpoint)
  - Primarily Suricata
  - License fee per sensor
- Snort Community
  - Primarily Snort
  - Free
  - Community-contributed
- Snort Subscriber (Talos)
  - Snort only
  - License fee per sensor
- Snort Registered
  - Snort only
  - Same as Snort Subscriber, but 30 days delayed

@Lody Web 2023

# IDS Rules

- There's a bunch
- Typically broken up into categories
  - DNS rules
  - Trojan rules
  - Worm rules
  - Games rules
- http://rules.emergingthreats.net/open/suricata/rules/

@Cody Welu 2023

# What's in a rule?

- Syntax can vary from platform to platform
- All will have similar components, though
- IDS rules are similar to firewall rules to start
- Let's look at Suricata specifically

@Cody Wahl 2023

# Here's a rule

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- Detects bad telnet logins
- Let's break it down

@Lady Ada 2023

# Action

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"GPL
TELNET Bad Login"; flow:from_server,established;
content:"Login incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at 2010_09_23;)
```

- If the rule matches, what should we do?
  - Alert
    - Log the traffic, and let it through
  - Pass
    - Just let it through
  - Drop
    - Stop the packet, do not inform the receiver or sender (IPS mode)
  - Reject
    - Stop the packet, inform the receiver and sender (IPS mode)

@Cody Web 2023



# Protocol

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- What protocol to match on?
  - TCP, UDP, ICMP
  - IP
    - Essentially "any"
  - Suricata specific
    - HTTP, FTP, TLS, SMB, DNS

@Lody Way 2023



# Source and Destination IPs

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- IPv4, IPv6 addresses
- Can also negate addresses
- $HOME_NET and $EXTERNAL_NET
  - Defined in the IDS's configuration
  - $HOME_NET defaults to private addresses
  - $EXTERNAL_NET is basically !$HOME_NET



# Source and Destination Ports

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- Can do ranges, negations
  - 80, 82 — Ports 80 and 82
  - 80:82 — Ports 80 through 82, inclusive
  - 1024: — Ports 1024 and higher (until 65535)
  - !80 — Any port but port 80
  - Any — All the ports

# Direction

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- Which way the signature has to match
- Packets must flow in that direction
- Most are an arrow to the right
  - ->
- Can also do bi-directional
  - <>

@Cody Wass 2023



# Try It 1

- Example…
  - alert proto $HOME_NET any -> $EXTERNAL_NET any
- Example_1.pcap
  - Packet 26
- Example_2.pcap
  - Packet 2
- Example_3.pcap
  - Packet 10

https://files.dakotastate.net/ids_pcaps.zip

@Cody Welu 2023

# Try It 1 - Answers

- Example…
  - alert proto $HOME_NET any -> $EXTERNAL_NET any
- Example_1.pcap
  - Packet 26
  - alert tcp $HOME_NET any -> $EXTERNAL_NET 80
- Example_2.pcap
  - Packet 2
- Example_3.pcap
  - Packet 10

@Lody Welu 2023



# Message

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- Descriptive Message
- Type of malware
  - Trojan, Ransomware, DDoS, etc.
- Action of the malware
  - Checking, Activity, Exfil…

@Lady Ugly 2023

# Different Types of Rules

- ET Rulesets include (but not limited to…)
  - Activex.rules
  - Attack_response.rules
  - Botcc.rules
  - Chat.rules
  - Dns.rules
  - Dos.rules
  - Drop.rules
  - Files.rules
  - ftp.rules
  - Icmp.rules
  - Misc.rules
  - Netbios.rules
  - scan.rules
  - Shellcode.rules
  - Smtp.rules
  - Snmp.rules
  - telnet.rules
  - Tor.rules
  - Trojan.rules
  - Policy.rules
  - User_agents.rules
  - Worm.rules
- Some note of this will go in the rule message

@Cody Wo 2023

# Message Examples

- ET TELNET External Telnet Login Prompt from Cisco Device

- Rule Creator
  - ET == Emerging Threats
- Ruleset/Category
  - TELNET
  - MALWARE
- Description
  - External Telnet Login Prompt from Cisco Device
  - Malware Type: Ransomware, DDoS, Adware, etc…

- Be consistent and descriptive
- This is SUPER important for logging and analysis!

@Cody Welu 2023



# Good or Bad?

- DSU TROJAN Mirage User Agent
- DSU INFO IP Lookup
- DSU POLICY Zeus Variant Checkin

@Lody Welu 2023

# Good or Bad?

- DSU TROJAN Mirage User Agent
  - Good!
- DSU INFO IP Lookup
- DSU POLICY Zeus Variant Checkin

@Lody Welu 2023



# Good or Bad?

- DSU TROJAN Mirage User Agent
  - Good!
- DSU INFO IP Lookup
  - No – not descriptive at all
- DSU POLICY Zeus Variant Checkin

@Lodg Welu 2023



# Good or Bad?

- DSU TROJAN Mirage User Agent
  - Good!
- DSU INFO IP Lookup
  - No – not descriptive at all
- DSU POLICY Zeus Variant Checkin
  - No – Zeus checking in isn't a policy violation

@Cody Welu 2023

# Flow

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"GPL
TELNET Bad Login"; flow:from_server,established;
content:"Login incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at 2010_09_23;)
```

- More than source and dest ip
- Client is the originator of the connection
- Server is the responder
- to_server == from_client
- from_server == to_client
- Most TCP rules will also contain “established”
  - UDP rules will just state the direction

@Lady Web 2023



# Try It 2

- msg:"DSU *Category Description*";flow: *flow_direction*;

- You are writing a signature for a WannaCry DNS Lookup
  - _____
- You are writing a signature for an executable payload from the Neutrino Exploit Kit as it enters the network
  - _____

@Cooly Wolf 2023

# Rule Headers

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
(msg:"GPL TELNET Bad Login";
flow:from_server,established; content:"Login
incorrect"; nocase; fast_pattern:only;
classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at
2010_09_23;)
```

- Do not affect how the rule matches packets
- Message to describe the rule
- Aid the analyst



# Rule Headers

- Classtype
  - Provide some classification to the rules
  - Priority levels assigned in the classification.config file (/etc/suricata/classification.config on our VM)
  - Some examples…
    - Not-suspicious
    - Unknown
    - Successful-dos
    - Successful-admin
    - Suspicious-login
    - Policy-violation
  - Optional field
- SID – Signature Identifier
  - Some allocated ranges
    - 1000000-1999999 are for your local custom use
    - Ranges above are reserved for ET Open, ET Pro, Original Snort GPL, Dynamically updated rules, etc.
  - Required field

@Cooly Welu 2023

# Rule Headers

- Rev
  - Revision
  - Increments as changes are made to the signature over time
  - Optional field
- Metadata
  - Really any key/value pair that you want
  - Optional field
  - Some examples…
    - Date created
    - Tags
    - Performance impact
    - Attack target

@Cody Weiu 2023

# Contents

```
alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"GPL TELNET Bad
Login"; flow:from_server,established; content:"Login incorrect";
nocase; fast_pattern:only; classtype:bad-unknown; sid:2101251; rev:9;
metadata:created_at 2010_09_23, updated_at 2010_09_23;)
```

- Unique packet contents
- Can have multiple content sections
- Many options
  - Nocase
  - Distance
  - Dsize
  - Isdataat
  - …and more…
- Excellent guide: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Payload_keywords

@Lody Web 2023



# Contents

- Contents can be string based
- content:”test”;

- Contents can be hex based
- content:”|00 2a 26 4a|”;

- Or both!
- content:”This | 20 | is | 20 | fun”;

@Lady Welu 2023



# Content Modifiers

- ```
  alert tcp $HOME_NET 23 -> $EXTERNAL_NET any
  (msg:"GPL TELNET Bad Login";
  flow:from_server,established; content:"Login
  incorrect"; nocase; fast_pattern:only;
  classtype:bad-unknown; sid:2101251; rev:9;
  metadata:created_at 2010_09_23, updated_at
  2010_09_23;)
  ```

- There are many, but we're going to start with just one.
  - Nocase;
  - The previous content match is not case sensitive.

@Lady Ada 2023




  ```

# Try It 3

- Write the full rule so far (as much as we have learned) with content for the following:
- Example_1.pcap
  - Packet 26
- Example_3.pcap
  - Packet 10
- Example_4.pcap
  - Packet 10

@Cody Welu 2023