Analyzing Honeypot Traffic

Chumming shark infested waters

Tom Peterson
CloudShark

What we'll be talking about

- What a honeypot is
- Different types of honeypots
- A running example
  - Accepts and listens to TCP connections
- Look at some captures
  - Wireshark, Suricata, Zeek

Who

- Tom
- I 💙 packets
- Live in New Hampshire
- Got my start at the IOL@UNH
- Work at QA Cafe
- Presented last year!
- Excited to be at SharkFest!
- tom@cloudshark.io

Why did I do this

- I 💙 packets
- Internet is like shark infested waters
- What happens when you listen to everything
- Practice using packet analysis tools
  - Wireshark profiles
  - Zeek is new to me
  - What Suricata detects
- So I can talk to all of you!

History

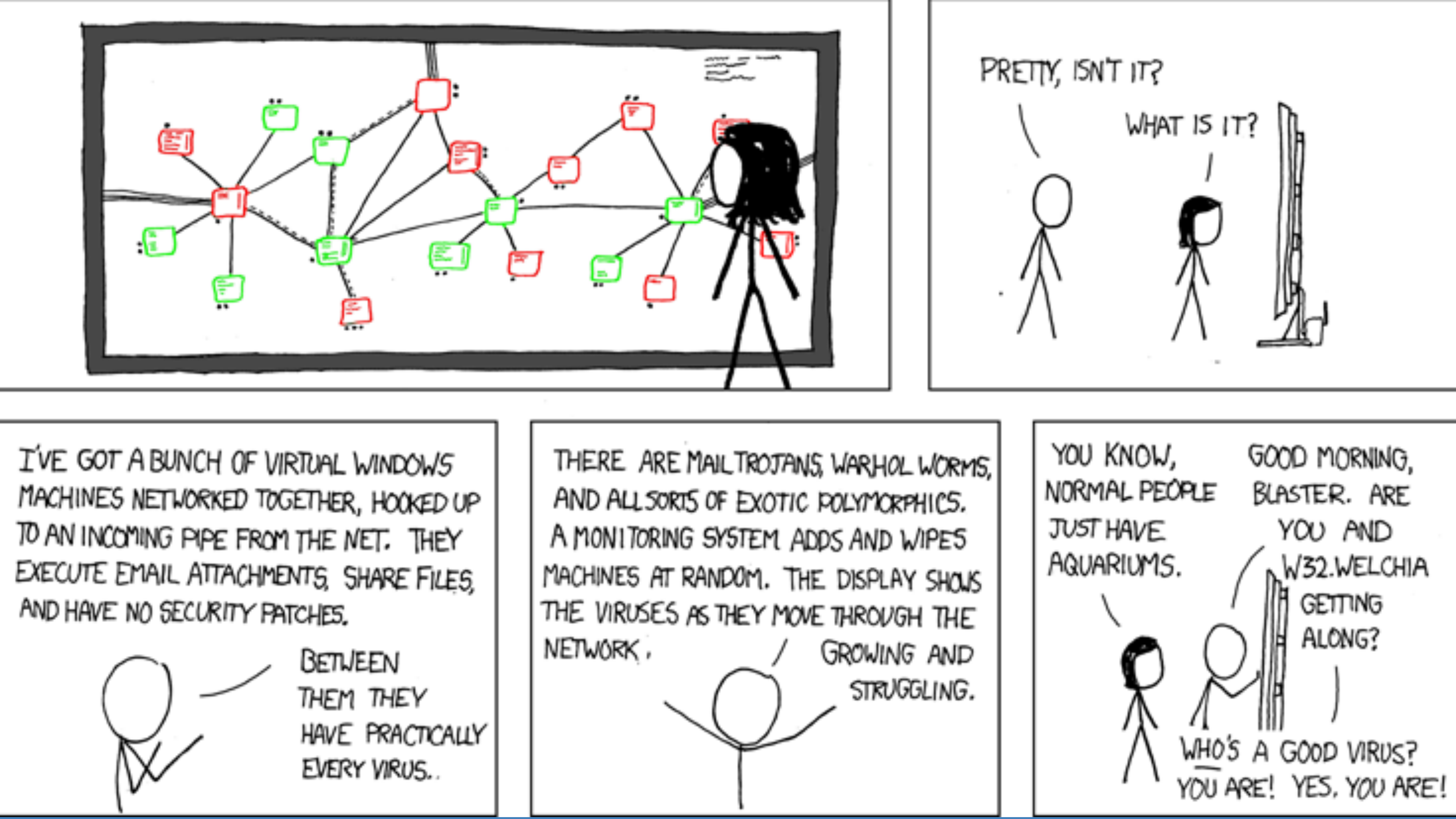
- Cuckoo's Egg - Clifford Stoll (1989)
- First example of honey pot
- Alert when attacker connected
- Monitored everything typed
- Fake documents to entice hacker
- Keynote at SharkFest 2012

How to define

- Look like a valid network resource
- No valid user should access it
- Monitored
  - We want PCAPs!
- Alert on actions
  - IDS rule
  - E-mail

What can they do

- Detect attackers
  - Inside firewall
- Waste their resources
- Threat hunting
- Curiosity and fun!


PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.
THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK,
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

General Classifications

- Production/Research
- Level of interactivity
  - Low - Listen on port and alert on connection
  - High - Fake/emulated service
  - Pure - A real device
- Honey nets
  - A whole collection emulating a network
- There are different types

Detection Honeypot

- Really interesting idea
- My home router has one
  - Listens on common ports
  - Alerts on any connection to that port
- Chris Sanders new book all about this

Tarpit

- First instance was LaBrea
- Used to exhaust attackers resources
- TCP fake SYN/ACK in 3-way handshake
  - Other side keeps sending ACK
- Endless SSH
- HTTP drag out response as long as possible
- So many bots out there though!

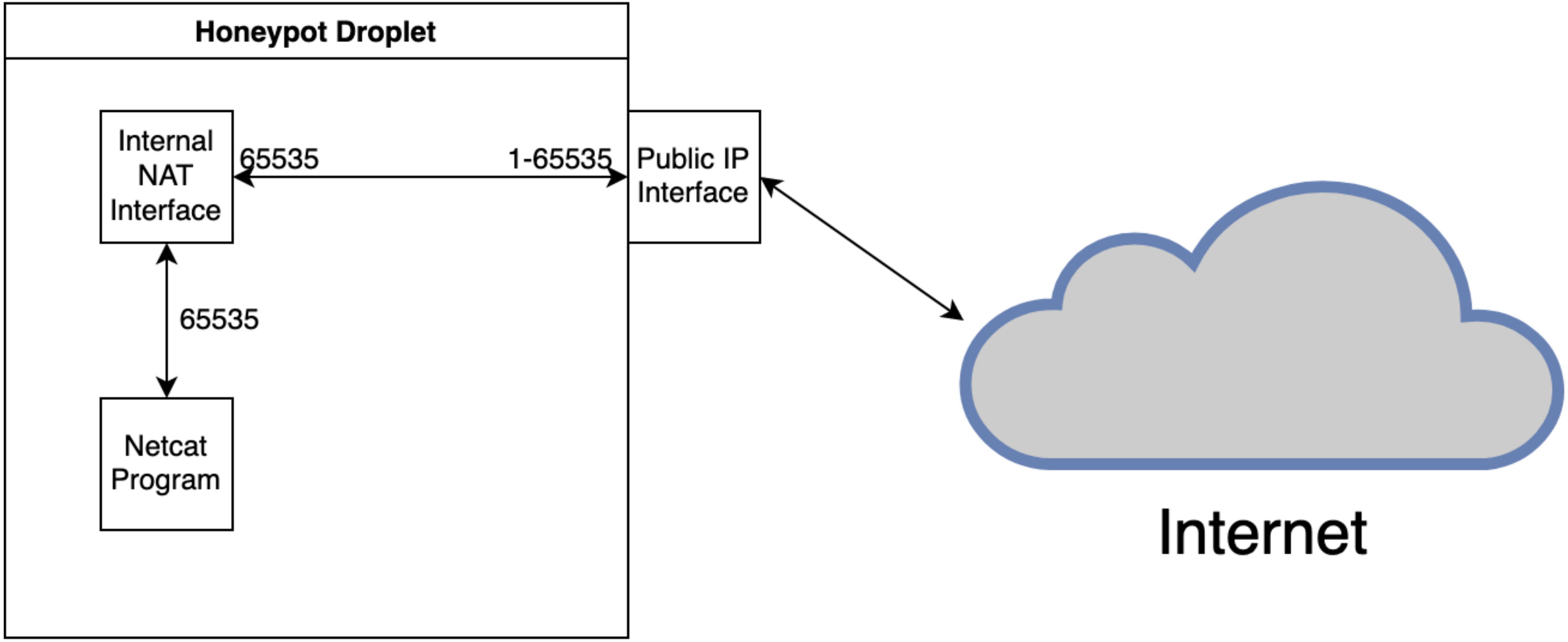
My honeypot

- Curious what happens on the internet
- Digital Ocean
- Accepts any TCP connection
- Just listens, never sends data
- Captures the packets!

How does it work

- Digital Ocean
- CentOS 7 droplet
- Added NAT interface
- Forward all ports to single port on NAT interface
- Netcat listens on NAT interface
- Ringbuffer for capturing

Diagram



github.com/thomasp11/sf20

What happened

- Statistics
- Interesting finds
- How I analyze the pcap data
  - Suricata
  - Zeek
  - Wireshark

Stats

- In 1 day
  - 456731 packets
  - 4678 Endpoints
  - 621 from China
  - 120 High severity alerts
  - 8947 RDP Attempts
  - 1560 SSH Attempts

Tools

- Wireshark
- Suricata
- Zeek
- CloudShark

Wireshark

- Looking directly at packets
- All the data
- All of it
- Profiles
- Filters
- Analysis Tools

Suricata

- Signature based
- Needs to be something previously seen
- Stream data
- Create filter for pcap

Zeek

- Behavior based
- Generates log files
- Custom Zeek scripts
- Plugins
- Display info from pcap data
- Can create filter for pcap too

CloudShark

- Web interface
- These are the tools under the hood
- I’ll make it clear which tools are generating the data we’re seeing

PCAP Time

Interesting finds

- Way more RDP traffic than expected
  - Very common way to get in
- Not so friendly sip scanner
- Looks like machine was a CnC server
  - Could we take those bitcoins?
  - Infected machine sending a password!?!

Wrap-up

- All tools have advantages/disadvantages
- Number of connections/packets makes pcap analysis tricky
- Zeek is an interesting tool.
- Lots of data when you listen for it

Resources

- github.com/thomasp11/sf20
- Cuckoo’s Egg - Cliff Stoll
- Honeynet
- SANS ISC
- Intrusion Detection Honeypots: Detection Through Deception - Chris Sanders