Intrusion Detection for Home Networks

GREG KING

CUUG PRESENTATION

MAY 22, 2018

Agenda

- Personal background
- Intrusion detection overview
- Honeypots
- HoneyPi
- DEMO
- Other resources
- Q&A

Greg King

- Started IT career in early 1970s after receiving BSc in Computer Science at UNB
- Provided technical support for UNIVAC mainframes for NB Government and Oil & Gas companies in Calgary
- Managed operations support teams for datacentres at Dome and Amoco
- Provided presales technical support for HP Openview in western Canada
- Provided consulting services around systems and network monitoring using HP Openview and various open source tools like Nagios until retirement in 2016.

Intrusion detection overview

From Wikipedia, the free encyclopedia

"An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms."

Intrusion Detection Overview

- IDS encompasses a large variety software and fall into 2 large classes:
- 1. Host based
  - Antivirus (Windows defender, ClamAV, etc)
  - Configuration monitoring (Tripwire, etc)
  - **Honeypots**
- 2. Network based
  - Network monitors (Availability, utilization, performance)
  - Traffic analyzers (packet / protocol analysis – inline, tap)
  - Firewalls (keep malicious traffic out of your internal network)
- More capable IDS' can become an Intrusion Prevention System (IPS)

Intrusion Detection Overview

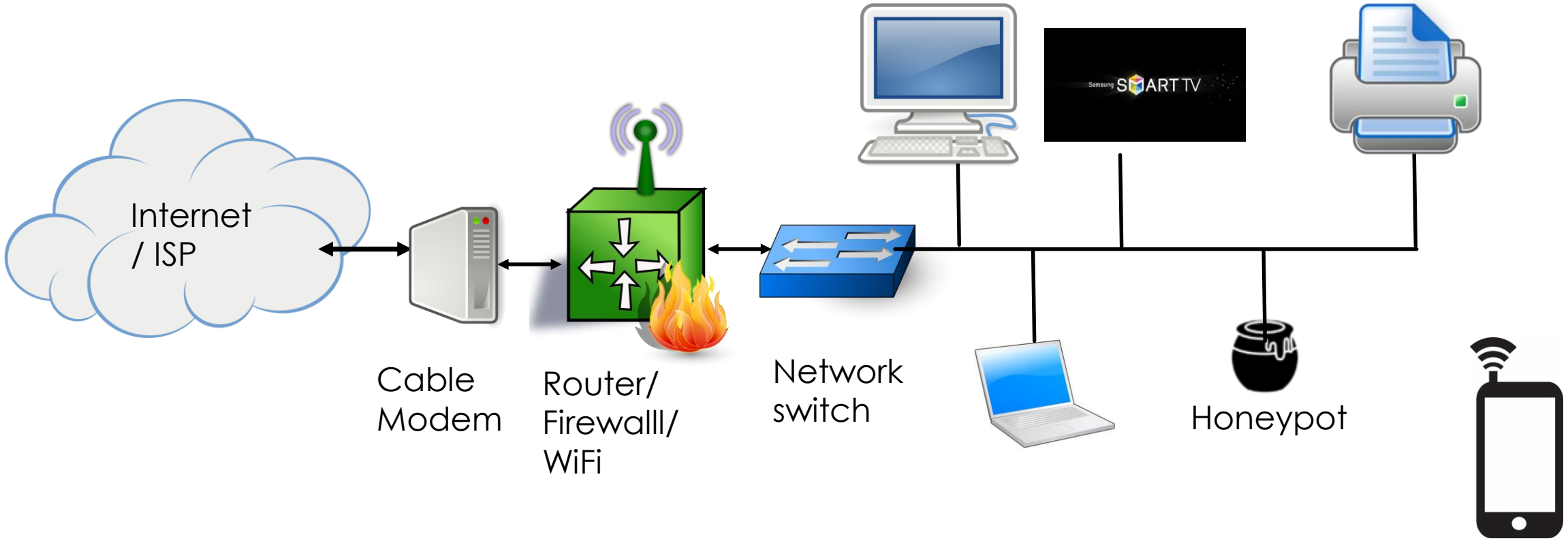
- Why you should employ a variety of IDS tools
  - Malware has become stealthy and can stick around for a long time extracting your data, spreading on your internal LAN, coopted into DDOS botnets, or crytomining at your expense
  - IoT devices come with poor or null security settings. Your TV, doorbell, DVD player and stereo receiver are now potential attack vectors
  - Many defence mechanisms are based on signature recognition so are susceptible to zero day vulnerabilities
  - Early detection of an intrusion is important for minimizing damage
  - Wikipedia page on IDS list ~20 open source IDS tools plus there are lots of commercial offerings as well

Honeypot Overview

From Wikipedia, the free encyclopedia

"In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked. This is similar to police sting operations, colloquially known as "baiting," a suspect."

Honeypot Overview
Typical Home Network



Honeypot Overview

- Honeypots can be targeted at specific intrusion attacks like malware, spam, databases, etc.
- Miscreants have tools to detect Honeypots based on their characteristics, so, as with antivirus tools, it is an ongoing game of cat and mouse.
- For home networks a very simple Honeypot for intrusion detection rather than a research oriented one to analyze attach methods is all that is needed unless you got lots of time on your hands or want to become a malware researcher.

Honeypot software - Raspberry Pi

- My unused Raspberry PI 2B was the inspiration to try a home network Honeypot after seeing an advertisement for Canary – an enterprise honeypot/ Honeynet system.
- There are lots of Honeypot applications for the Raspberry PI as well as other Linux distros
- I think this is an ideal application for a low powered device like an old Raspberry Pi

Honeypot software - Raspberry Pi

Raspian:
HoneyPi - TCP connect alerts
Kippo - SSH brute force logger
Dionaea - SMB/HTTP/FTPTFTP/MSSQL/MySQL/SIP logger
Glastopf - Python web application honeypot logger

Demo - Raspberry Pi setup

- Pi model B specs:
  - 32bit BCM2835 chip, 700MHz single core ARM CPU, 512MB ram
  - 2 x USB ports
  - 1 x 100 mbps NIC
- came with an 8GB class 10 SD card with NOOBS
- Current Raspbian OS needs 16GB SD Card
- Raspbian Lite (no GUI) runs fine on 8GB SD card
- Demo will start from point after Raspbian lite install

Demo - Raspberry Pi setup

- Configure Raspian lite Linux
  - **sudo raspi-config**
    - Set locale, timezone etc
  - **sudo dpkg-reconfigure keyboard-configuration**
    - Setup US keyboard + font (VGA -> 16x32)
  - If monitoring via wireless:
    - **sudo iwlist wlan0 scan**
    - **wpa_passphrase “<SSID>" “<pw>" >> /etc/wpa_supplicant/wpa_supplicant.conf**
    - **wpa_cli -i wlan0 reconfigure**
    - **ifconfig wlan0**

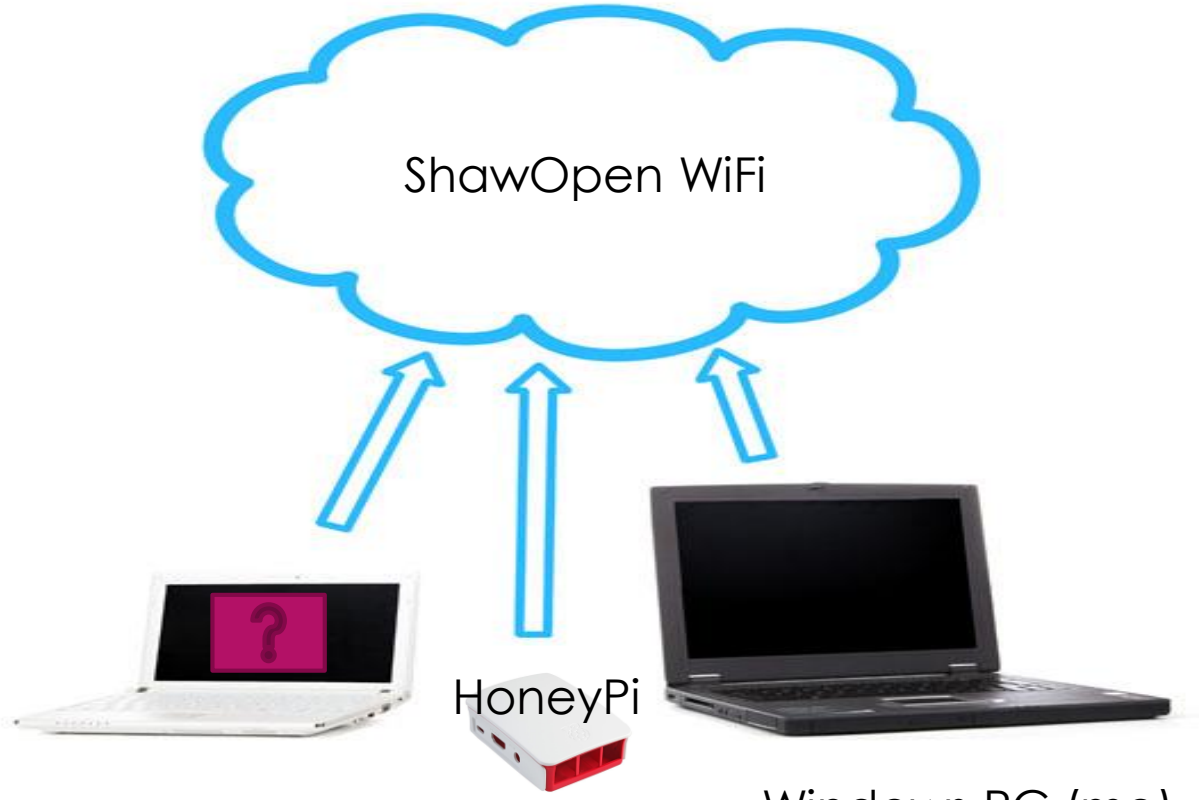
Demo - Raspberry Pi setup

- **wget** https://github.com/mattymcfatty/HoneyPi/archive/master.zip
  - Get HoneyPi software
- Unzip and run install script:
  - **unzip master.zip**
  - **cd HoneyPi-master**
  - **chmod +x *.sh**
  - **sudo ./honeyPiInstaller.sh**
- Install script will prompt needed info. Will probably break other apps on the Pi

Demo - Raspberry Pi setup

- Objective
  - to offer a reliable indicator of compromise
  - little to no setup or maintenance costs
  - flags a few surefire triggers that would catch most attackers snooping around on an internal network
    - 1. Port Scanning Activities
    - 2. FTP Connection Attempts
    - 3. Telnet Connection Attempts
    - 4. VNC Connection Attempts

DEMO



Other resources

- Mint/Ubuntu:

labrea

tinyhoneypot

- Debian:

Open canary

- Honeyd - a small daemon that creates virtual arbitrary hosts on a network.

Miscellaneous Other tools
- Snort (https://www.snort.org/)
- ntop (http://www.ntop.org/)
- Remote packet capture (https://github.com/frgtn/rpcapd-linux)

Modern Honey Network (MHN) - Console for managing multiple Honeypots

Other Resources

- Honeeepi distro (Pi B+)

- Conpot (http://conpot.org/) - Industrial control

- Dionaea (https://github.com/gento/dionaea, with IoT honeypot feature - Internet of Things)

- Glastopf (http://glastopf.org/)

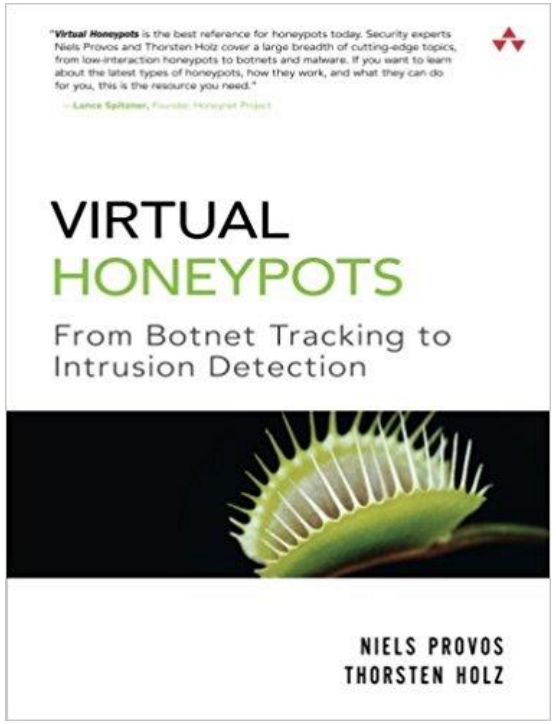
- Cowrie (https://github.com/micheloosterhof/cowrie) - SSH

- Kippo (https://github.com/desaster/kippo) - SSH

- honeyd (https://github.com/DataSoft/Honeyd)

- amun (http://amunhoney.sourceforge.net/)

Other Resources



Niels Provos received a Ph.D. from the University of Michigan in 2003, where he studied experimental and theoretical aspects of computer and network security. He is one of the OpenSSH creators and known for his security work on OpenBSD. Provos is currently employed as senior staff engineer at Google, Inc.

Thorsten Holz is a Ph.D. student at the Laboratory for Dependable Distributed Systems at the University of Mannheim, Germany. He is one of the founders of the German Honeynet Project and a member of the Steering Committee of the Honeynet Research Alliance. He regularly blogs at http://honeyblog.org

Q&A

?

Honeypot Overview