Choptank Electric Cooperative Internship

RICHARD ANDERSON

About the Company

- Choptank Electric Cooperative is a nonprofit utility cooperative that distributes electricity to rural areas in the Eastern Shore region of Maryland.
- The cooperative was founded in 1938 and is headquartered in Denton, MD.
- Around 160 employees
- They serve roughly 52,000 members

Choptank Electric Cooperative

A Touchstone Energy® Cooperative

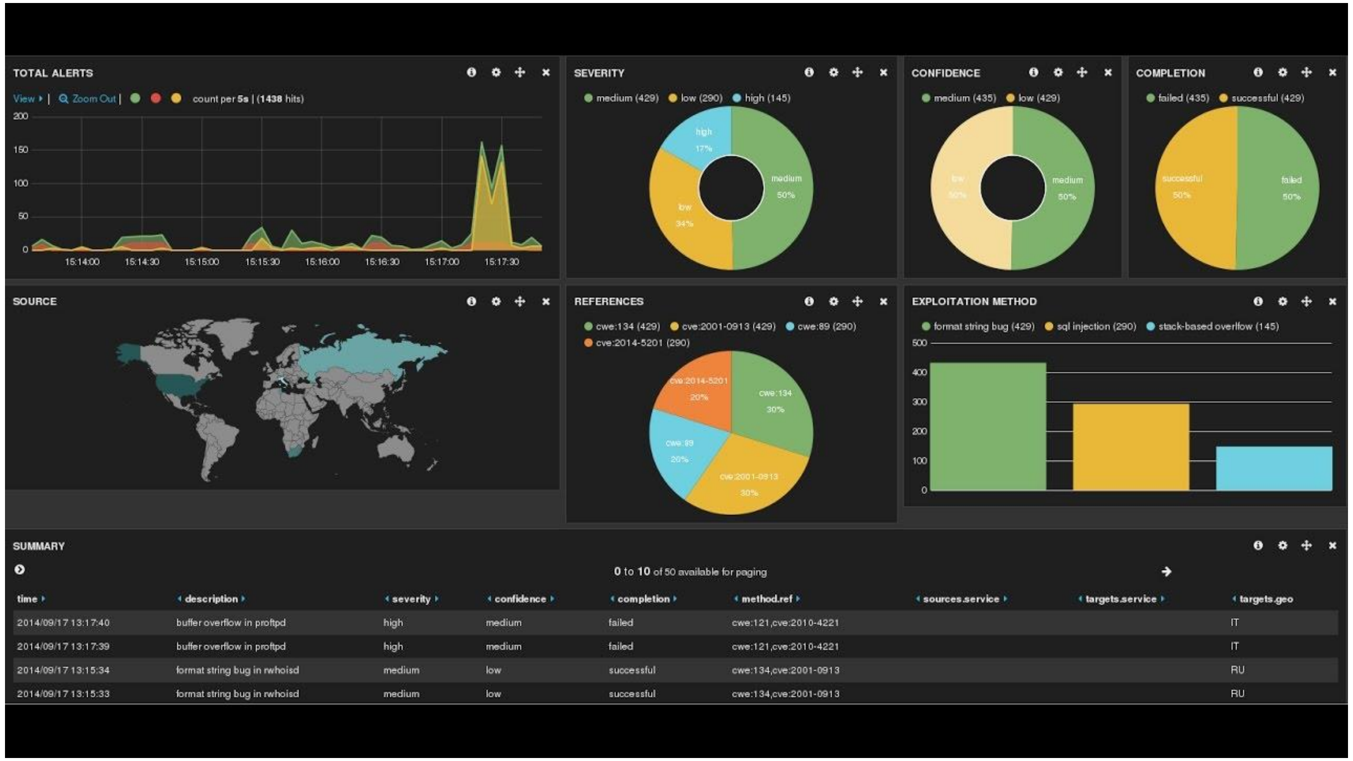
Responsibilities

1.) IDS Project

- The idea: build a distributed intrusion detection system across electrical substations
- In the event of an attack, we want to be able to respond quickly. Additionally, we want to be able to analyze data afterwards to assess the situation.
- Why was this so important?

Security Onion

- “Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management.”
- It includes many useful tools for packet captures and network data analysis
- It allows you to build an “army of distributed sensors” for your enterprise/network



SUMMARY

0 to 10 of 50 available for paging

time	description	severity	confidence	completion	method.ref	sources.service	targets.service	targets.geo
2014/09/17 13:17:40	buffer overflow in proftpd	high	medium	failed	cwe:121,cve:2010-4221			IT
2014/09/17 13:17:39	buffer overflow in proftpd	high	medium	failed	cwe:121,cve:2010-4221			IT
2014/09/17 13:15:34	format string bug in rwhoisd	medium	low	successful	cwe:134,cve:2001-0913			RU
2014/09/17 13:15:33	format string bug in rwhoisd	medium	low	successful	cwe:134,cve:2001-0913			RU

IDS Project

- **Step 1:** Installing the Operating System on the servers
  - This was a big task because we had roughly ~15 IDS servers to set up
  - Security Onion has a lot of specific requirements, so the disks had to be partitioned manually

IDS Project continued...

- **Step 2:** Running our custom-built newServerBuilder script
  - We wanted all IDS servers to be built in the same “standardized” way
  - We wrote a custom piece of software to build the file systems in the exact same manner for each machine
  - There was a lot of testing and debugging involved. We went through roughly 15 versions of the script throughout the testing phase

IDS Project continued...

- **Step 3: Thorough documentation**
  - We write information about each device to a MySql database
  - Each machine is given a name and device number
  - Thorough documentation of the setup process

IDS Project continued...

- **Final step**: Going out into the field and installing the machines
  - lots of driving involved!

UFW Analysis Application

- Generated UFW logs for each device
- Parsed the data and pulled out which packets were blocked (dropped by the firewall)
- Sent email reports containing a data summary to each team member
- Two reasons we look at these logs:

  1. If packets are blocked from devices we want to allow, there could be an issue with our existing UFW rules

  2. If many packets are being sent from outside IP addresses, it could be indicative of a potential attack

Other responsibilities

- Creating detailed network maps
- Automating everyday tasks with bash scripts
- Host/network monitoring
- Writing detailed documentation and README's

Challenges

- Lack of networking knowledge beyond the basics
- Learning the network topology (company specific)
- Needing a deep knowledge of Bash/Linux OS
- Learning about industry-specific terms

Coursework that helped me

- COSC 370 – Intro to computer networks
- COSC 350 – Included a brief introduction to scripting/the Linux CLI
- COSC 220/320 – Provided experience with Linux, as well as general programming knowledge

What I learned (Summary)

- Deep networking knowledge (analyzing packet captures, monitoring hosts, setting up servers, firewall rules, ...etc.)
- Industry-specific knowledge about electricity and electrical substations
- Experience working on a team, testing other people’s code, debugging
- Experience writing documentation
- In-depth Bash scripting
- Text parsing using sed and Awk