Getting Down To Business

CCDC Bootcamp Week 6
https://da.gd/DYj91

whoami

Taylor Nguyen
Ex-CCDC Team Captain
CPTC Team Member
Gym-goer

Agenda

1

Injects in CCDC

2

Presentations in CCDC

3

Inside an Inject

4

Lab

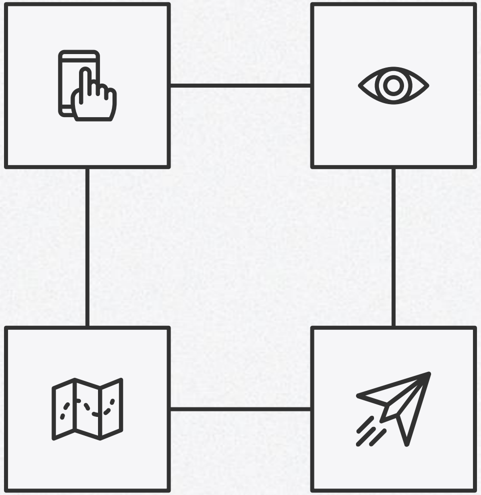
1

Injects in CCDC

What are injects?

- Business tasks
- Test your knowledge on the following:
    - Can you implement XYZ
    - Can you provide a report/summary on XYZ
    - Can you present on XYZ
    - Can you communicate the technical stuff to a non-technical audience
- Typically written in email format
- Very important in cyber!

Example Topics



Draft a BYOD Policy

Perform a vuln scan

Asset Inventory

IPv4 to IPv6

What makes a good inject?

Be professional

Be concise

… do what it says

From: Herschel Shm oikel Pinchas Yerucham Krustofsky

To: New IT Team

Subj: Intrusion! Who? What? Somebody call a cop!

Hey Kids,

“Krustyland has a new ride: The Eyeballs of Death. It only passed the safety by a 3-to-2 vote, and that third didn’t come cheap.”

Whoops! Sorry wrong company…

So, Sideshow Bob had a question. (That guy scares me!)

“It has come to my attention that we are not using any kind of Intrusion Detection / Prevention system. As you may know, these systems are vital to identifying potential breaches in security and alerting IT staff to potential real-time threats. Furthermore, it may help with our upcoming reports that we need to provide to our potential buyer. “

Smarty Pants!

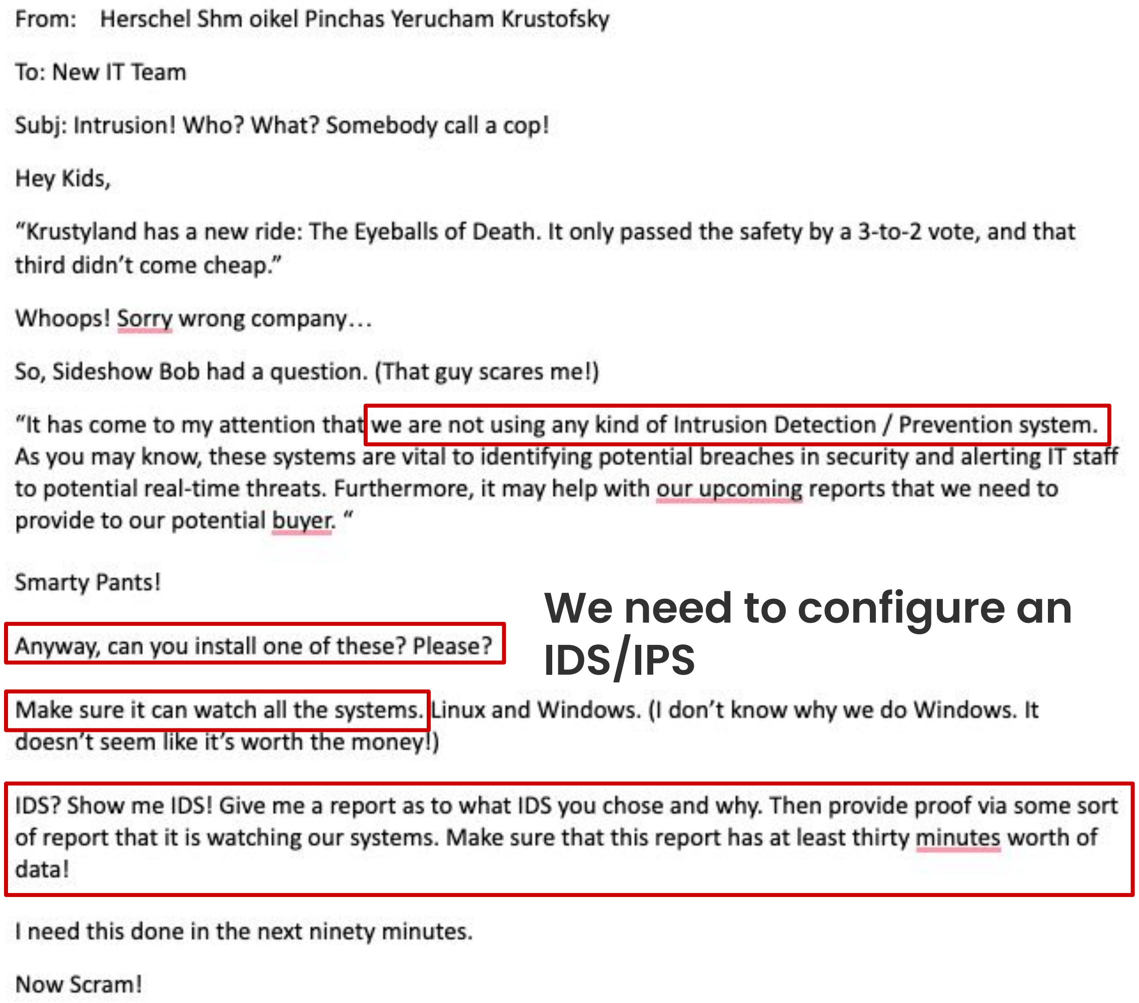
Anyway, can you install one of these? Please?

Make sure it can watch all the systems. Linux and Windows. (I don’t know why we do Windows. It doesn’t seem like it’s worth the money!)

IDS? Show me IDS! Give me a report as to what IDS you chose and why. Then provide proof via some sort of report that it is watching our systems. Make sure that this report has at least thirty minutes worth of data!

I need this done in the next ninety minutes.

Now Scram!



From: Herschel Shm oikel Pinchas Yerucham Krustofsky

To: New IT Team

Subj: Intrusion! Who? What? Somebody call a cop!

Hey Kids,

“Krustyland has a new ride: The Eyeballs of Death. It only passed the safety by a 3-to-2 vote, and that third didn’t come cheap.”

Whoops! Sorry wrong company…

So, Sideshow Bob had a question. (That guy scares me!)

“It has come to my attention that we are not using any kind of Intrusion Detection / Prevention system. As you may know, these systems are vital to identifying potential breaches in security and alerting IT staff to potential real-time threats. Furthermore, it may help with our upcoming reports that we need to provide to our potential buyer. “

Smarty Pants!

Anyway, can you install one of these? Please?

Make sure it can watch all the systems. Linux and Windows. (I don’t know why we do Windows. It doesn’t seem like it’s worth the money!)

IDS? Show me IDS! Give me a report as to what IDS you chose and why. Then provide proof via some sort of report that it is watching our systems. Make sure that this report has at least thirty minutes worth of data!

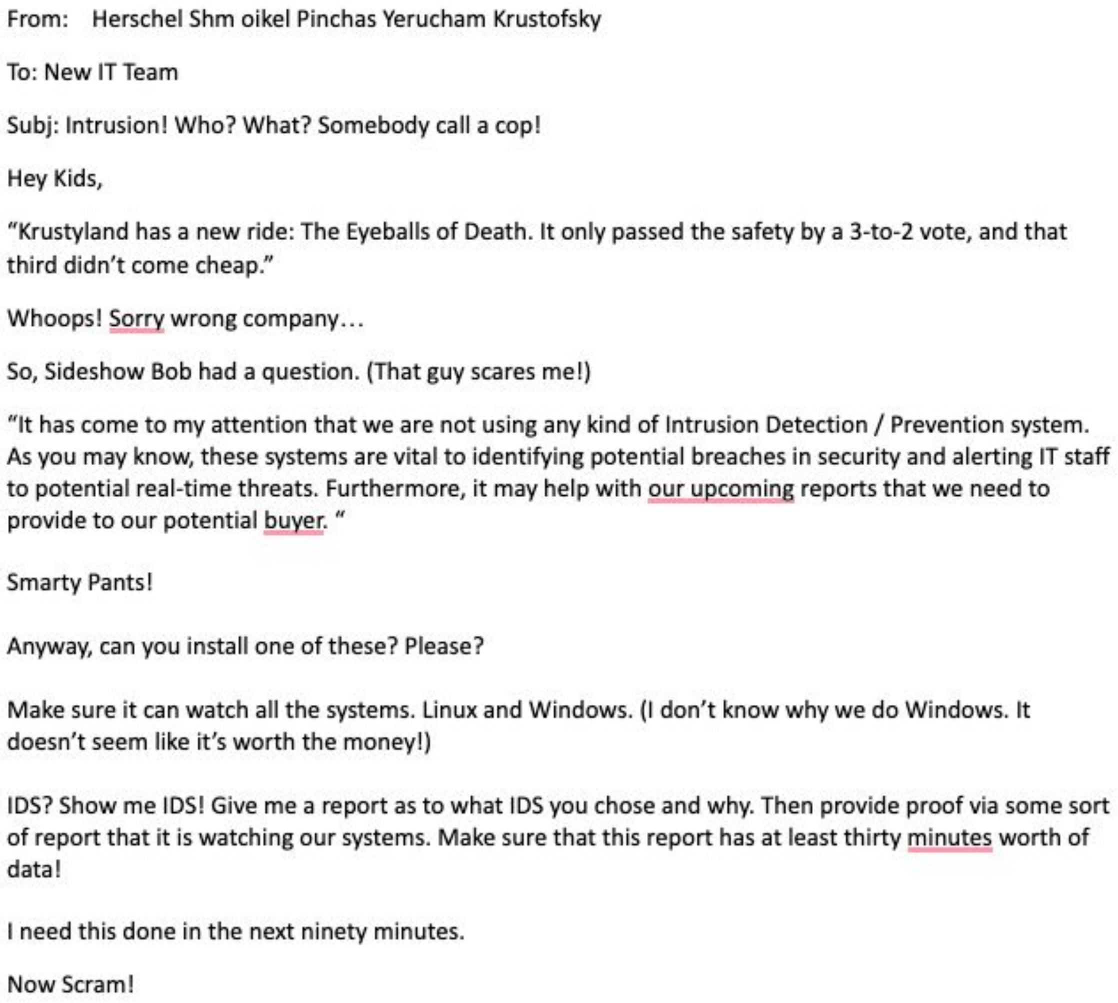
I need this done in the next ninety minutes.

Now Scram!

We don't have an IDS/IPS

We need to configure an IDS/IPS

Describe choosing of IDS, provide proof of IDS + 30 min of data



From: Herschel Shm oikel Pinchas Yerucham Krustofsky

To: New IT Team

Subj: Intrusion! Who? What? Somebody call a cop!

Hey Kids,

"Krustyland has a new ride: The Eyeballs of Death. It only passed the safety by a 3-to-2 vote, and that third didn't come cheap."

Whoops! Sorry wrong company…

So, Sideshow Bob had a question. (That guy scares me!)

"It has come to my attention that we are not using any kind of Intrusion Detection / Prevention system. As you may know, these systems are vital to identifying potential breaches in security and alerting IT staff to potential real-time threats. Furthermore, it may help with our upcoming reports that we need to provide to our potential buyer. "

Smarty Pants!

Anyway, can you install one of these? Please?

Make sure it can watch all the systems. Linux and Windows. (I don't know why we do Windows. It doesn't seem like it's worth the money!)

IDS? Show me IDS! Give me a report as to what IDS you chose and why. Then provide proof via some sort of report that it is watching our systems. Make sure that this report has at least thirty minutes worth of data!

I need this done in the next ninety minutes.

Now Scram!

Tasks:

- Deploy an IDS
- Make sure it gets 30min of data
- Take screenshot of IDS + 30 min of data
- Write up report on why I chose X product + paste screenshot

2

Presentations in CCDC

Presentations in CCDC

- Presentations are injects of their own
- Occur in the middle of competition
- 20 minutes presentation & 10 minutes Q&A
    - That's how much time you're allocated - you don't have to fill up that entire time

Example Topics

Security Assessment

CEO's computer got hacked

Phishing

What makes a good presentation?

Know your stuff

Keep your cool

Keep it simple

Mock Presentation (next week)

- Choose a topic →
- 1 week to prepare
  - Slides
  - Practice
- 5 min pres + 1 min Q&A
- Out of time = 🥾

1. Multi-factor authentication
2. Phishing countermeasures
3. Bring-Your-Own-Device
4. Acceptable Use Policy
5. Single-sign on
6. Data loss prevention
7. Disaster Recovery Planning

3

Inside an Inject

shorturl.at/fquE0

4

Lab

About the inject

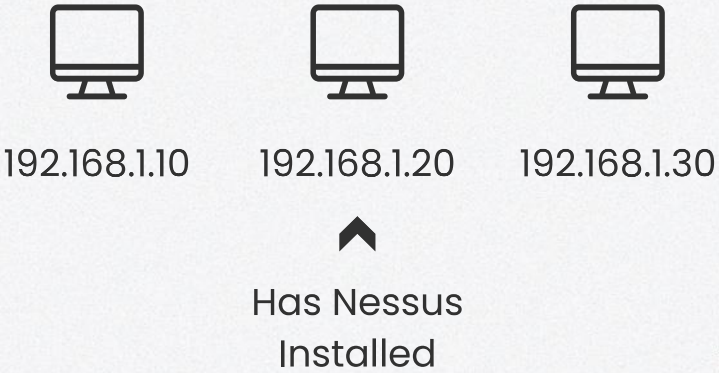
You have 3 injects:

- Inject 1 - Security Assessment
- Inject 2 - ??
- Inject 3 - ??

All injects are due next Saturday at 5:00AM.

Good luck!

Scope:



192.168.1.10

192.168.1.20

192.168.1.30

Has Nessus Installed