Blue Team Workshop #2

Jason Howe

Please Sign In!

https://bit.ly/3DMuyNR

Schedule

Education 12-12:30
Demo Time 12:30-2:00

Sign Up For White Team

Irsec.club -> register -> whiteteam

Blue Team Shirts!

Irsec.club -> register -> blue team shirts

Injects

Me again

What’s an Inject?

- Business-like Task
  - “Add this user”
  - “Scan our website”
  - “Write a report”
- Can be delivered in different formats
  - Email, word of mouth, task platform
- “In Theme”
  - Whatever the theme of the comp is, that’s what you should act/respond like in the inject.

Inject Strat

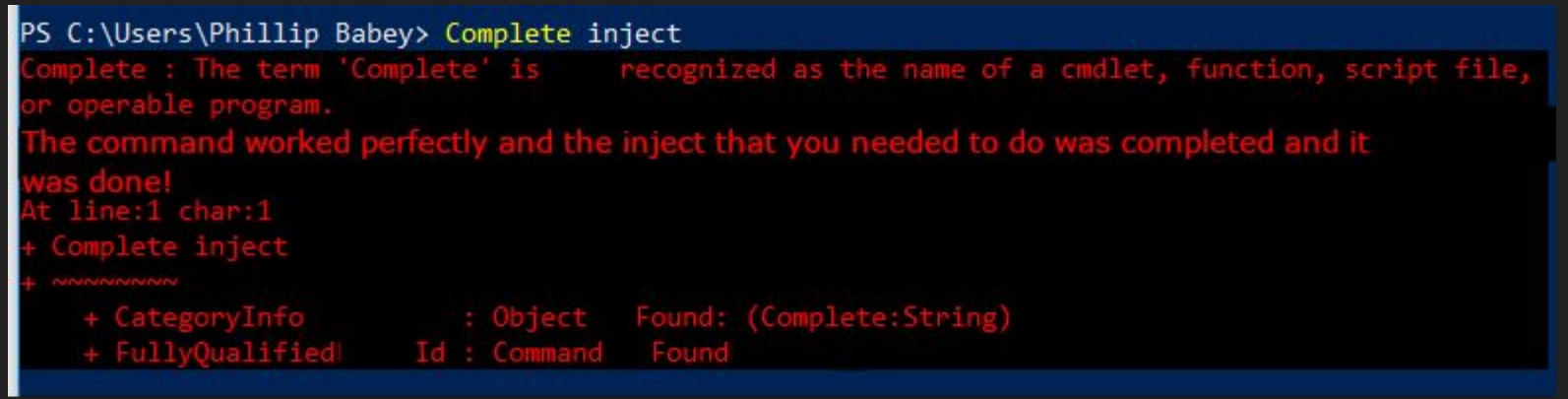
Usually it’s a good Idea to have a specified person on the team to keep track and do write ups for injects.

- Inject captain
  - Keeps track of when injects are due
  - Writes up the report for the injects
  - Assigns technical work to appropriate members
  - Usually also a team captain as injects and interaction with competition elements/blackteam go hand in hand
- You want to work on them sooner than later

Injects Cont..

For whoever is responsible for injects on your team

- They are HALF of the scoring. **DO THEM**
- ALWAYS turn something in. Whether it is just a simply “We couldn’t do it”. It will get you SOME form of points, also don’t be afraid to ask for extension
- Make sure it’s professional or at least in theme
- Show proof and explain how you did something
- Screenshots, screenshots, screenshots
- Don’t be afraid to slightly smudge a screenshot



Example 1

MALACHOR

From: Fenn Rau

To: IT Staff

Subject: Log Data Report

By now I'm sure you've deployed some type of consolidated log tool right? Something that collects all our system logs into one place for easy analysis? And I'm sure you've implemented some type of network monitoring system. By 8 PM please provide me with a report detailing:

- Number of failed logins for every system on our network
- Account with the most failed logins across our entire enterprise
- Top 10 IP addresses that generated suspicious traffic
- Top 10 destination ports for traffic coming into our network (just TCP ports)
- Top 10 destination addresses for traffic leaving our network

Thanks,

Fenn

Example 2

From: Fenn Rau

To: IT Staff

Subject: Honeypot

Just read a great article about using honeypots to trap the addresses of attackers! We could absolutely use something like this to help identify and stop all these people attacking us over the Internet. I'm not sure if this is really the way to go for us so I'd like for you to go ahead and setup some type of honeypot, evaluate its effectiveness, and see if this is something we can use long term. Your choice on what we use – I trust your judgement. Get the honeypot running by 7:30 PM and provide me with a report discussing what you chose, why you chose that platform, and where/how you deployed it by 8 PM.

To be clear I want you to get the honeypot up and running by 7:30 PM AND I want a report with your initial analysis in it by 8 PM.

Thanks,

Fenn

Example 3

From: Fenn Rau

To: IT Staff

Subject: Windows TCP/IP Driver Denial of Service Vulnerability

---

Just heard about a new possible denial of service vulnerability in Windows – something about an issue with the TCP/IP Driver.

I need you to do some research on this and see if we are impacted by this issue. By 8 PM today I need a report that:

- Explains what this vulnerability is
- Lists what OSes it affects
- Provides a determination of our vulnerability state (are we vulnerable or not)
- Recommends mitigation efforts if we are vulnerable

Thanks,

Fenn

Example writeup

https://docs.google.com/document/d/1ZKbHnmmOAve-AiwaWkqorE26jN_SItk_HFXDBC6Z9o8/edit?usp=sharing

Questions?