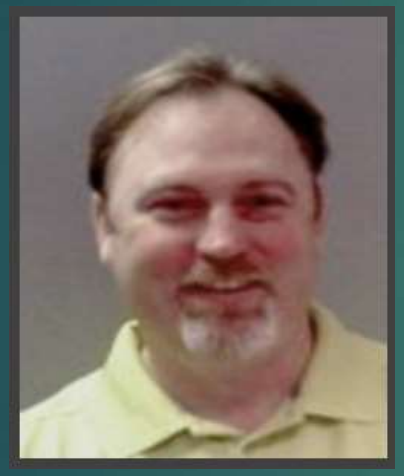
Hacking for Defense (H4D)™

Team Malware Hunters

The Sponsor
NSA

The Problem
Associating IP Addresses with Malicious Activity

Team Members



Jeremy Graves

Justin Johnson

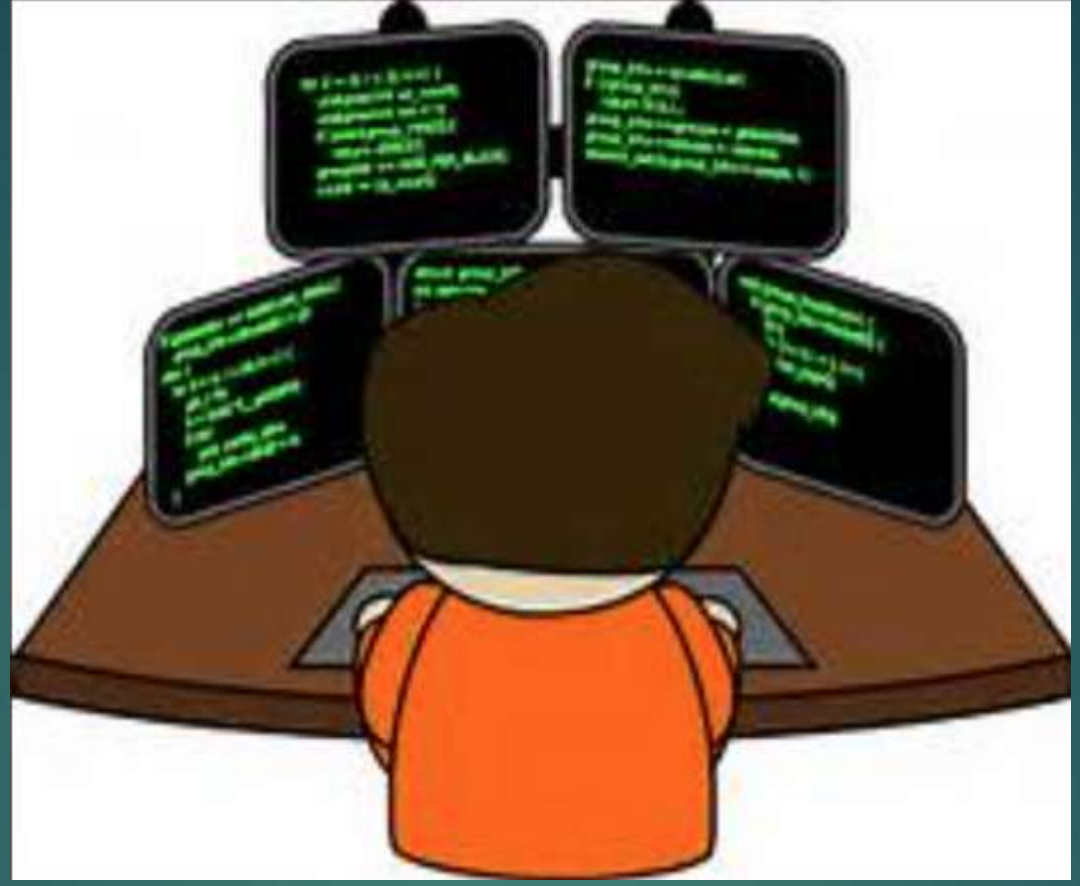
Week 1:

The Problem

Associating IP Addresses with Malicious Activity

The Solution

Create a software for the Intelligence Community to use



Week 10:

The Problem

Associating IP Addresses with Malicious Activity

The Solution

Create a web based platform that analysts can login to.

Week 1
June 5th - 11th

The Struggle Begins

- The team began with 3 members
- We picked our problem from the provided list of problems
- Started Brain storming the way forward
- Connected with problem sponsor

Week 2
June 12th – 18th

- Started the first interviews with the Analysts and Campus Police Chief
- Our initial thought was to create a software for the Government
- We learned that developing software for the Government can be tedious and time consuming
- Installing software on government systems can take up to two years
- Found out that developing a web based UI would be the best solution

Week 3
June 19th – 25th

"Analysts are used to working with visually unattractive tools, and if our tool could have a real nice visual aspect and user friendly environment it would be well accepted by analysts." (# 24)

- In Week two the team lost a member
- In Week 3 the team gained a new member
- Found potential uses for our brainstormed product

Malicious IP

Key Partnerships

- NSA
- Competitor Collaboration & Partnership
- Developers
- Big Data Expert

Key Activities

- Information Security Groups
- Co-Creation
- Common Vulnerabilities & Exposures and other feeds
- Identifiy IP address(s) or URLs that are potentially malicious.
- IP Reputation
- Self-Service

Key Resources

- WHO IS
- Knowledge and experience for Analyst/Researchers
- Database Expert NOSQL
- DNS
- GEO Location
- Shodan

Value Propositions

- Reduce time spent researching
- NSA
- Personal assistance
- Dedicated personal assistance (Growth dependent)
- Increase the amount of IP's analysts can research
- Expose basic research of cyber analyst to other analysts/researchers

Buy-in & Support

- Team
- Analyst
- Researcher
- Government (Three letter agencies)

Deployment

- Subscription Service Model
- Data Scientist
- Chief Information Officer (CIO)
- Contract

Beneficiaries

- Police Chief
- Security Officer
- Intrusion Analyst
- Financial Officer
- Health Care

Mission Budget/Costs

- Equipment
- Programmer
- Sales
- Legal
- Subscription Services

Mission Achievement/Impact Factors

- Funding
- New Team Members
- Hardware/ Licensing Costs

Product

Benefits

-Speed in comparing datasets
-Analysts can look at more IP's
-The data is co-located

Experience

-Excited to try the tool
-When is going to be ready
-Holy Grail

Features

-Summarization of the data
-User default settings
-Ability to search multiple sources from one tool
-User Friendly UI
-Help comments used to inform the user of the features

Customer

Wants

-User friendly UI
-Summary of Data
-History of the data
-Geolocation

Fears

-Legalities
-Too difficult to use
-Inaccurate data
-To expensive

Needs

-Simple UI
-Summary Report
-One location to find data
-Quick and accurate data
-Visualization of data

Week 4
June 26th –July 2nd

"We desperately need something that can go to multiple sites, and places to search by just using one source."(# 32)

- We learned that an analyst has to use multiple different tools in order to receive the information needed
- This process can take hours to search for the data required
- The sharing of information from different classified networks is a difficult process and can only go up in classification and not down
- How to parse data from different sources and data structures and return that data into one report

Week 5
July 3rd – July 9th

"Pulling information into summaries that are accurate would be very useful." (# 43)

- We discovered that summarizing the data would be extremely useful for an analyst
- If we are providing a summary we also need to include all of the data that was used for the summary
- Some data sources are going to be more reliable and accurate than others
- Analysts need the supporting document in order to trust, but verify the information given

Week 6
July 10th – 16th

"To retrain the people to use a tool is always an issue and costs money." (# 56)

- The level of knowledge has an impact on the use of each tool
- We need to create something that is user friendly
- The User Interface (UI) has to be easy to interact with
- If we create a tool that is intuitive and easy to learn it will save manpower and money by reducing the time spent training new users

{Paste IP or Subnet}
192.168.1.0/24

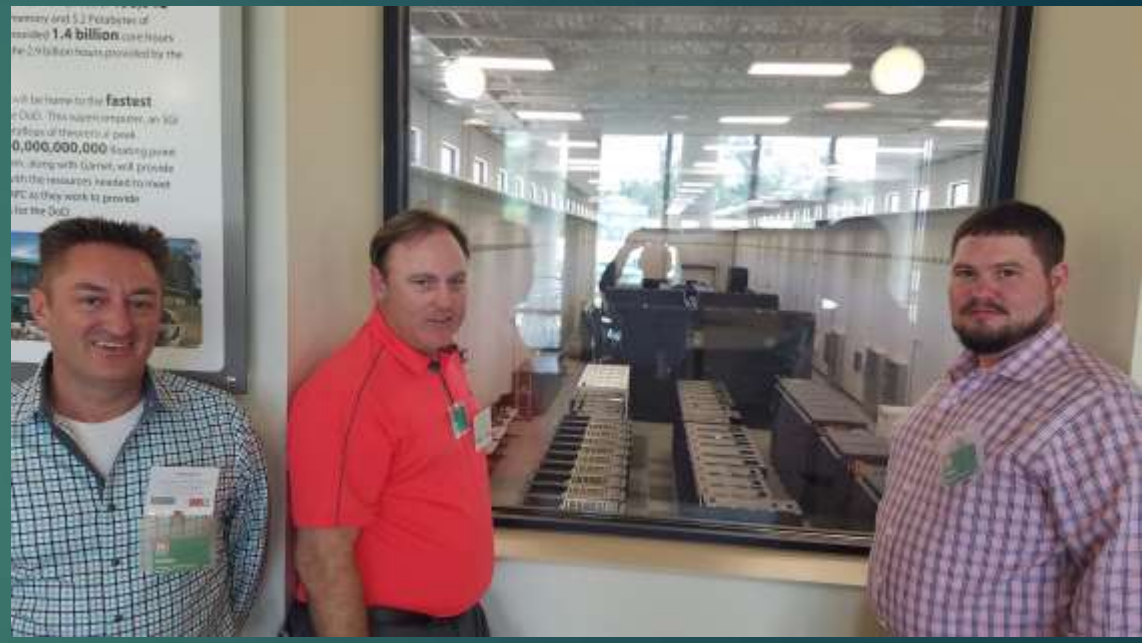
Chose your the probes to launch below and press "GO"

GO

Week 7
July 17th – 23rd

"Some of the people might not be the Subject Matter Experts (SME)'s and know what they are looking for." (# 69)

- We took a field trip to Engineer Research & Development Center (ERDC)
- After speaking to the Cyber Security Division our vision for the product was validated
- Even with the super computers at their disposal they are still unable to analyze the data in the time they desire



Week 8
July 24th – 26th

- Over the last 8 weeks we interviewed over 90 people from Analysts, Developers, Military, Pen Testers, and Chief of Police. During these interviews we were able to gain inside knowledge of the struggles of the intelligence community.
- With our newly enhanced knowledge we now believe we have a clear picture of what is needed
- We are going to continue our efforts of creating this product

The Hurdles

- The loss of team members in the 2nd week as well as the 4th week
- The time it took to ensure all of the interviews were attended
- Detail were hard to come by due to the nature of the sponsors work
- Not having a Programmer/Developer on the team
- Budget
- Due to the issues with the programmers and budget we were unable to have a working prototype

This is the end of the class, but only the beginning of the future!