Understanding the Cognitive Science of Cyber Security

Nancy J. Cooke
Arizona State University

LASER Workshop
5/26/2016

This work has been supported by the Army Research Office under MURI Grant W911NF-09-1-0525.
Overview

• Why is this so Hard?
• Definitions and Theoretical Drivers
• The Living Lab Approach
  – Cognitive Task Analysis
  – Testbed Development
  – Empirical Studies and Metrics
  – Modeling
• Conclusion and Next Steps
Why is this so Hard?

• Defining/scoping the system
  – Which humans? What roles?
  – What is the task?
  – What is the context?
  – How are they interconnected in the larger system?

• What are the Goals? Research Questions?
  – Measurement
  – Ground Truth

• Ubiquitous Internet
Definitions and Theoretical Drivers

- MURI (ARO) Cyber Situation Awareness
- Cyber Security as a Sociotechnical System
- Interactive Team Cognition
- Team Situation Awareness
Cyber Security as a Sociotechnical System

- Cyber defense functions involve cognitive processes allocated to
  - Human Operators of many kinds
  - Tools/Algorithms of many kinds
- Human Operators
  - Different roles and levels in hierarchy
  - Heterogeneity (Information, skills and knowledge)
- Tools
  - For different kinds of data analysis and visualization
  - For different levels of decision making
- Together, human operators and tools are a sociotechnical system
  - Human System Integration is required
Security Analysis: A Complex Cognitive System

Current Cyber System lack integration, top-down information sharing, and tools that meet analyst needs and capitalize on human strengths and limitations (dotted lines).
Interactive Team Cognition

Team is unit of analysis = Heterogeneous and interdependent group of individuals (human or synthetic) who plan, decide, perceive, design, solve problems, and act as an integrated system.

Cognitive activity at the team level = Team Cognition

Improved team cognition $\rightarrow$ Improved team/system effectiveness

Heterogeneous = differing backgrounds, differing perspectives on situation (surgery, basketball)
Interactive Team Cognition

Team interactions often in the form of explicit 
communications are the foundation of team cognition

ASSUMPTIONS

1) Team cognition is an activity; not a property or product
2) Team cognition is inextricably tied to context
3) Team cognition is best measured and studied when the team 
is the unit of analysis

Interactive Team Cognition, Cognitive Science, 37, 255-285, 
DOI: 10.1111/cogs.12009.
Implications of Interactive Team Cognition

• Focus cognitive task analysis on team interactions
• Focus metrics on team interactions (team SA)
• Intervene to improve team interactions
Team Situation Awareness

A team’s *coordinated perception* and action in response to a change in the environment

Contrary to view that all team members need to “be on the same page”
The Living Lab Procedure

Testbeds
1) CyberCog
2) DEXTAR/DETER

Field Data - CTA

Empirical Studies in Testbeds

EAST and Agent Based Modeling

Measures

Theory Development

Time (s)
Cumulative Speaking (s)
Cognitive Task Analysis Activities

• Conducted literature review
• Cyber SA Workshop 2011
  – one hour breakout session with 3 cyber security analysts.
  Topics:
   – Structure of defense CERT departments work of the security analyst
   – Tasks performed by each analyst
   – Tools used by the analyst to perform the task
   – Team structure
   – Interaction among analysts within a team
   – Reporting hierarchy

• Cyber Defense Exercises
  – Air Force Academy, Colorado Springs, CO
  – CTA collaboration with PSU – WestPoint CDX logs
  – iCTF – International Capture the Flag at US Santa Barbara (Giovanni Vigna)

• Cyber Survey – web responses
Lessons Learned: Cyber Defense Analysts

• High stress
• High attrition rate
• High False Alarm Rate
• Low Situation Awareness
• Cyber analysis task does not make the best use of individual capabilities
• Expertise is challenging to identify
Lessons Learned: The Analyst Task

- Unstructured task; hierarchical within government, but within units it breaks down
- Variance across departments, agencies
- Ill-structured with no beginning or end
- Little to no standardized methodology in locating and response to an attack
- Massive amounts of data, information overload, high uncertainty
- No software standards
- Metrics of individual and team performance and process are lacking
Lessons Learned: Training Analysts

- No cohesive training programs for specific tasks or not standardized enough
- No feedback
- No way to benchmark or evaluate the efficacy of individuals in the real world. No ground truth
- No performance metrics
Lessons Learned: Teamwork Among Analysts

• Teamwork is minimal in cyber security
• Cyber analysts work as a group – Not as a team
• Possible Reasons
  – Cognitive overload
  – Organizational reward structures
  – “Knowledge is Power”
  – Lack of effective collaboration tools
• Little role differentiation among teammates
• Low interaction; a collective with each working independently
• Informal, *ad hoc* interactions, loosely coupled system, and lack of distribution of task
CyberCog Synthetic Task Environment

- Simulation environment for team-based cyber defense analysis
- Emulating the work, interaction, and collaboration of Cyber Network Defense analyst teams
- A research testbed for:
  - Controlled experiments
  - Assessment of interventions, tools, aids
CyberCog Team Task

- Three team members monitor IDS alerts and network activity of 3 different sub-networks for a given scenario
- Find IDS alerts pertinent to the attack
- Find the systems affected and attack path
- On consensus, team submits their findings
## CyberCog Display

### Events

<table>
<thead>
<tr>
<th>Time</th>
<th>SourceIP</th>
<th>DestinationIP</th>
<th>Event Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>8:06:12 PM</td>
<td>69.141.62.18</td>
<td>10:15:20.8 Remote Login Attempt Failed ID:1002</td>
</tr>
<tr>
<td>Select</td>
<td>8:08:12 PM</td>
<td>200.38.31.66</td>
<td>10:15:20.18 Escalation of Privileges Attempt ID:1020</td>
</tr>
<tr>
<td>Select</td>
<td>8:10:12 PM</td>
<td>10.15.22.35</td>
<td>10:15:20.23 Buffer Overflow Attempt ID:1019</td>
</tr>
<tr>
<td>Select</td>
<td>8:13:12 PM</td>
<td>115.64.145.93</td>
<td>10:15:20.12 Remote Login Attempt Failed ID:1002</td>
</tr>
<tr>
<td>Select</td>
<td>8:16:12 PM</td>
<td>10.15:20.7</td>
<td>10:15:4.0-254 Port Scan Attempt ID:1009</td>
</tr>
<tr>
<td>Select</td>
<td>8:17:12 PM</td>
<td>119.30.36.53</td>
<td>10:15:4.57 Suspicious Email message ID:1001</td>
</tr>
<tr>
<td>Select</td>
<td>8:22:12 PM</td>
<td>10.15.20.30</td>
<td>119.162.39.235 Possible Information Leak ID:1008</td>
</tr>
<tr>
<td>Select</td>
<td>8:27:12 PM</td>
<td>10.15.4.35</td>
<td>10:15:20.18 Escalation of Privileges Attempt ID:1020</td>
</tr>
<tr>
<td>Select</td>
<td>8:31:12 PM</td>
<td>68.73.193.249</td>
<td>10:15:20.30 Port Scan Attempt ID:1009</td>
</tr>
<tr>
<td>Select</td>
<td>8:35:12 PM</td>
<td>10.30.4.10</td>
<td>10:15:20.9 Port Scan Attempt ID:1009</td>
</tr>
<tr>
<td>Select</td>
<td>8:36:12 PM</td>
<td>10.15.22.21</td>
<td>62.202.101.136 Connection to an unknown host ID:1025</td>
</tr>
<tr>
<td>Select</td>
<td>8:39:12 PM</td>
<td>60.84.121.37</td>
<td>10:15:20.18 Remote Login Attempt Failed ID:1002</td>
</tr>
<tr>
<td>Select</td>
<td>8:46:12 PM</td>
<td>121.246.251.140</td>
<td>10:30.4.55 Unauthenticated upload/download request ID:1023</td>
</tr>
<tr>
<td>Select</td>
<td>8:48:12 PM</td>
<td>93.139.123.84</td>
<td>10:15:20.9 Buffer Overflow Attempt ID:1019</td>
</tr>
<tr>
<td>Select</td>
<td>8:53:12 PM</td>
<td>10.15.22.2</td>
<td>10:15:20.9 Escalation of Privileges Attempt ID:1020</td>
</tr>
</tbody>
</table>
CyberCog Measures

PERFORMANCE
• Alert classification accuracy

TEAM INTERACTION
• Communication – audio data
• Computer events
• Team situation awareness
  » Attack path identified (systems, order)
  » Attack information distributed across 2-3 team members
  » Team coordination is required to identify and act on threat
  » Roadblock can be introduced through equipment malfunctions (e.g., tool crash)

WORKLOAD
• NASA TLX – workload measure
CyberCog Modifications

• Task Distribution – Through task training emulate individual and specialized experience
  - Analyst 1 - database containing system vulnerabilities
  - Analyst 2 - wiki-styled website forum-information on possible attack scenarios
  - Analyst 3 - network map-illustrated systems and their physical layout
• Each analyst receives a distinct set of intrusion events to analyze and classify into a given set of categories.
• To effectively classify the events, the analyst
  – Must integrate and analyze information from multiple sources (network activity logs, vulnerability data etc.)
  – Must interact with other analysts
• Data Sets scripted based on 2009 WestPoint CDX logs
• Measures team performance and logs interaction
CyberCog Issues

- Low-level triage task
- Signal detection
- Not capturing richer problem solving tasks
DEXTAR/DETER

Defense EXercises for Team Awareness Research/DEfense Technology Experimental Research

- Higher fidelity testbed for human-in-the loop cyber security research
- Marries CyberCog environment with DETER
- Analyze cyber-team performance with up to six members
- Collect user interaction and team performance data
- Screen capture and audio/video recording
- Large-scale virtual networks are fully customizable
- Supports Linux and Windows virtual machines and virtual servers
- Virtual network integration with real testbed machines
- Supports human, scripted, and agent cyberattacks
- Record temporal traffic and network performance data
- Requires skilled participants
The Living Lab Procedure

Testbeds
1) CyberCog
3) DEXTAR/DETER

Field Data - CTA

Empirical Studies in Testbeds

Measures

Theory Development

Social Network Diagrams
of Incident Response/Network Defense Teams

EAST and Agent Based Modeling
Experiment 1: Cyber Groups vs. Teams

Hypotheses

• Reward structures conducive to team work in cyber defense analyst groups performing triage level analysis will lead to higher signal detection performance.

• Improving interactions between analysts can improve overall cyber defense performance.
The Experiment

• 3-person teams/groups in which each individual is trained to specialize in types of alerts

• 2 conditions:
  – Team Work (Primed & Rewarded for team work)
  – Group Work (Primed & Rewarded for group work)

• 6 individuals at a time
  – Team Work - Competition between the 2 teams
  – Group Work - Competition between the 6 individuals

• Experimental scenarios:
  – 225 alerts
  – Feedback on number of alerts correctly classified - constantly displayed on big screen along with other team or individual scores

• Simulates knowledge is power for group condition

• Measures
  Signal Detection Analysis of Alert Processing
  Amount of Communication
  Team situation awareness
  Transactive Memory
  NASA TLX – workload measure
Cyber Teaming is Beneficial for Analyzing Novel and Difficult Alerts

• Working as team helps when alerts are novel and involves multi step analysis, not otherwise.
• Signal Detection Measure: $A'$ as performance measure
• $A'$ ranges from values 0.5 and 1 with 0.5 indicating lowest performance possible and 1 indicating highest performance possible.
Cyber Teaming Helps When the Going Gets Rough

Mean Performance ($A'$) by Condition

Sensitivity to true alerts

$F(1, 18) = 5.662, p = .029^{**}$ (Significant effect of condition)
Groups that Share Less Information Perceive More Temporal Demands than High Sharers

- NASA TLX Workload Measure: **Temporal Demand**
- Measures perception of time pressure
- Higher the value higher the task demand

Statistically significant across scenarios and conditions (p-value = 0.020)
Groups that Share Less Information Perceive Work to be More Difficult than High Sharers

- NASA TLX Workload Measure: **Mental Effort**
- Measures perception of mental effort
- Higher the value, more mental effort required

Statistically significant across scenarios and conditions (p-value = 0.013)
Conclusion

• Break the “Silos”
• Use the power of human teams to tackle information overload problems in cyber defense.
• Simply encouraging and training analysts to work as teams and providing team level rewards can lead to better triage performance
• Need collaboration tools and group decision making systems.
Experiment 2: Information Pooling Bias

The tendency for group members to spend more time and energy discussing information that all members are already familiar with (i.e., shared information), and less time and energy discussing information that only some members are aware of (i.e., unshared information)

• Poor decision-making can result
• It is impossible for every team member to know all the information (rely on others expertise)
• This may be an issue in the cyber domain

Research Questions

1. Does information pooling bias affect cyber forensic analyst team discussions and decisions?

2. Does a tailor made collaboration tool lead to superior analyst performance compared to using off-the-shelf collaboration tool such as wiki software?
Procedure

• 30 teams of 3 participants
• Trained on cyber security concepts, types of attacks and tasks to be performed
• Pre-discussion reading and discussion
• Practice mission
• 2 main missions
• Goal – Detect large scale attacks
Attack Data Distribution in Missions

Attacks

Analyst 1
- Shared 1
- Shared 2
- Shared 3
- Shared 5
- Unique A1
- Unique B1
- Isolated 1
- Isolated 2

Analyst 2
- Shared 1
- Shared 2
- Shared 3
- Shared 4
- Unique A2
- Unique B2
- Isolated 3
- Isolated 4

Analyst 3
- Shared 1
- Shared 2
- Shared 4
- Shared 5
- Unique A3
- Unique B3
- Isolated 5
- Isolated 6
# Experimental Design

<table>
<thead>
<tr>
<th>Tool Type</th>
<th>Trial 1 - Baseline</th>
<th>Trial 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slide Based</td>
<td>Slide Based</td>
<td>Slide Based</td>
</tr>
<tr>
<td>Slide Based</td>
<td>Wiki</td>
<td>Collaborative Visualization</td>
</tr>
<tr>
<td>Slide Based</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Collaborative Visualization Tool

• Collaborative visualization tool designed from a cognitive engineering perspective

• To mitigate the information pooling bias in cyber defense analysts

• Improve information sharing and decision making performance
Observation Description

Title: Intrusion

Analyst: 1

Time of Attack: 11:30 AM April 11 2014
Source IP: 154.48.48.48
Destination IP: 105.10.10.X
Type of Attack: Intrusion

A brute force intrusion from a remote IP - 154.48.48.48 was detected on different machines on the sub-network. A unknown remote machine tried to gain access to employee machines through several brute force logins. Further investigation revealed that the remote system was successful in logging in to a router machine.

Used the login id - admin and password - arsenal123.

Using the login, the attacker tried to copy the address tables in the router. Possibly to gain access to other machines in the network.
Measures

• Communication coding
  – Amount of time spent on discussing each attack
  – Number of mentions of each attack

• Decision quality
  – All attacks detected?

• Workload & Demographics
Team Level Measures

• Shared Discussion
  – Percentage of discussion spent on discussing attacks that are shared among members

• Unique Discussion
  – Percentage of discussion spent on discussing attacks are unique but are part of a large scale attack

• Detection Performance
  – Number of attacks detected (Both shared and unique)
  – Max possible = 18 (4*3 + 2*3)
Percentage of shared information discussed compared between Missions

Mean Shared Percentage

<table>
<thead>
<tr>
<th>Condition</th>
<th>Mission1</th>
<th>Mission2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slide</td>
<td>60.50</td>
<td>63.15</td>
</tr>
<tr>
<td>Wiki</td>
<td>64.52</td>
<td>67.20</td>
</tr>
<tr>
<td>Visual</td>
<td>64.33</td>
<td>50.29</td>
</tr>
</tbody>
</table>
Percentage of unique information discussed compared between Missions

![Bar Chart: Mean Unique Percentage](image)

- **Slide**: Mission1: 17.16, Mission2: 18.51
- **Wiki**: Mission1: 15.20, Mission2: 17.41
Number of shared attacks detected (Performance) compared between Missions

![Bar chart showing mean shared attack detection performance for different conditions and missions.](chart.png)
Number of unique attacks detected (Performance) compared between Missions

Mean Unique Attack Detection Performance

<table>
<thead>
<tr>
<th>Condition</th>
<th>Mission1</th>
<th>Mission2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slide</td>
<td>0.40</td>
<td>1.80</td>
</tr>
<tr>
<td>Wiki</td>
<td>1.20</td>
<td>0.80</td>
</tr>
<tr>
<td>Visual</td>
<td>1.00</td>
<td>3.70</td>
</tr>
</tbody>
</table>
Summary of Results

• Significantly more shared attack information discussed
  – Cyber Defense analysts undergo information pooling bias
  – Prevents detecting APT kinds of attacks
• Use of cognitive friendly visualization reduces the bias, improves performance
• Off the shelf collaboration tools don’t help
The Living Lab Procedure

Testbeds
1) CyberCog
2) DEXTAR/DETER

Field Data - CTA

Empirical Studies in Testbeds

EAST and Agent Based Modeling

Measures

Time (s)
Cumulative Speaking (s)

BEGIN

END
Agent-Based Modeling

• Human-in-loop experiment
  – Traditional method to study team cognition
• Agent based model
  – A complimentary approach
• Modeling computational agents with
  – Individual behavioral characteristics
  – Team interaction patterns
• Extend Lab Based Experiments
Model Description

• Agents: Triage analysts
• Task: Classify alerts
• Rewards for classification
• Cognitive characteristics:
  — Knowledge and Expertise
  — Working memory limit
  — Memory Decay
Model Description

• **Learning Process:** Simplified – Probability based
  – 75% chance to learn
    – Cost: 200 points
    – Payoff: 100 points

• **Collaboration:** Two strategies to identify partners
  – Conservative (homogeneous partners) or Progressive (heterogeneous partners)
    – Cost: 100 points for each
    – Payoff: 50 points for each

• **Attrition**
Irrespective of Team Size Agents in Progressive Condition Classified More Alerts

Conservative – select homogeneous partners;
Progressive – select heterogeneous partners
Conclusions

• Small heterogeneous teams of triage analysts could be beneficial.

• Agent based modeling
  – Can extend lab based experiments
  – Can be used to ask more questions quickly
  – Can raise new questions and identify gaps
Two Case Studies and EAST Models
EAST
Event Analysis of Systemic Teamwork) framework (Stanton, Baber, & Harris, 2012)

• Integrated suite of methods allowing the effects of one set of constructs on other sets of constructs to be considered
  – Make the complexity of socio-technical systems more explicit
  – Interactions between sub-system boundaries may be examined
  – Reduce the complexity to a manageable level

• Social Network
  – Organization of the social system (i.e., communications structure)
  – Communications taking place between the actors working in the team.

• Task Network
  – Relationships between tasks
  – Sequence and interdependences of tasks

• Information Network
  – Information that the different actors use and communicate during task performance

With Neville Stanton, University of Southampton, UK
Approach

• Interviews with cyber network defense leads from two organizations on social structure, task structure, and information needs

• Hypothetical EAST models created

• Surveys specific to organization for cyber defense analysts developed

• Surveys administered to analysts in each organization to refine models
Social Network Diagrams of Incident Response/Network Defense Teams

Industry

- Op Team
- Responder (6)
- Detector (6)
- Threat Analyst (1)

Military

- Cyber Command
- Analyst 1
- Analyst 2
- Analyst 3
- Analyst 4
- Customer
Sequential Task Network Diagram
Military Network Defense Team

1. Handoff
2. Customer Assignment
3. Review Events
4. Gather Batch of Reports
5. Review Alerts
6. Dispatch
7. Cyber Command
8. Customer
EAST Conclusions

• A descriptive form of modeling that facilitates understanding of sociotechnical system
• Can apply social network analysis parameters to each of these networks and combinations
• Can better understand system bottlenecks, inefficiencies, overload
• Can better compare systems
• Combined with empirical studies and agent-based modeling can allow us to scale up to very complex systems
Conclusion

- Analysts tend to work alone
- Teamwork improves performance
- Work is heavily bottom up
- Much technology is not suited to analyst task
- Human-Centered approach can improve SA
Next Steps

• Use DEXTAR-DETER to explore more complex tasks of cyber analyst
• Use DEXTAR-DETER to compare analyst tools, models, and visualizations
• Examine other human roles and tasks
Thanks & Questions

Army Research Office (Cliff Wang)
Sandia Research (DEXTAR)
USC DeterLab

Jim Blythe, PhD
Aaron Bradbury
Rachel Howes
Sarah Kusumastuti
Prashanth Rajivan, PhD
Steve Shope, PhD
Jessica Twyford

ncooke@asu.edu
<table>
<thead>
<tr>
<th>Time</th>
<th>SourceIP</th>
<th>DestinationIP</th>
<th>Event Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:25:31 PM</td>
<td>134.240.12.254</td>
<td>10.15.20.5</td>
<td>WebServer: Data received beyond the timestamp</td>
</tr>
<tr>
<td>1:25:43 PM</td>
<td>194.266.32.45</td>
<td>10.15.20.6</td>
<td>FTP Server: Remote Login attempt failed</td>
</tr>
<tr>
<td>1:26:03 PM</td>
<td>198.129.64.69</td>
<td>10.15.20.6</td>
<td>WebServer: Port Scan attempt</td>
</tr>
<tr>
<td>1:26:04 PM</td>
<td>158.129.64.69</td>
<td>10.15.20.5</td>
<td>WebServer: Port Scan attempt</td>
</tr>
<tr>
<td>1:36:16 PM</td>
<td>3.75.190.161</td>
<td>10.15.20.6</td>
<td>WEBServer: user/pass.txt file modify attempt</td>
</tr>
<tr>
<td>1:26:28 PM</td>
<td>3.75.190.161</td>
<td>10.15.20.5</td>
<td>WEB-Server: Unauthorized file g-recommended.ini added to usurprograms - possible virus</td>
</tr>
<tr>
<td>1:26:40 PM</td>
<td>10.15.20.5</td>
<td>3.75.190.161</td>
<td>WEB-Server: Possible Information Leak</td>
</tr>
<tr>
<td>1:26:53 PM</td>
<td>178.89.63.233</td>
<td>10.15.20.9</td>
<td>DNS-Server: Port Scan attempt</td>
</tr>
<tr>
<td>1:27:04 PM</td>
<td>10.30.4.6</td>
<td>10.15.20.6</td>
<td>Web-Server: config/web.xml file access attempt</td>
</tr>
<tr>
<td>1:27:17 PM</td>
<td>192.121.86.47</td>
<td>10.15.20.8</td>
<td>Binary Code detected in the network stream</td>
</tr>
</tbody>
</table>
### Search Options

#### Source IP

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

#### Destination IP

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

---

**Payload Description**

Control Packet: fragment 4 - size: 54 Bytes - Duplicate packet 1

<table>
<thead>
<tr>
<th>Time</th>
<th>SourceIP</th>
<th>DestinationIP</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:20:22 PM</td>
<td>134.240.12.264</td>
<td>10.16.20.6</td>
<td>Data Transfer Packet</td>
</tr>
<tr>
<td>12:20:56 PM</td>
<td>194.268.32.46</td>
<td>10.16.20.8</td>
<td>Failed Login request</td>
</tr>
<tr>
<td>12:21:36 PM</td>
<td>156.129.64.59</td>
<td>10.16.20.6</td>
<td>Scan on ports between 8001 - 9000 port range</td>
</tr>
<tr>
<td>12:21:56 PM</td>
<td>166.129.64.59</td>
<td>10.16.20.6</td>
<td>Scan on ports between 8001 - 10000 port range</td>
</tr>
<tr>
<td>12:22:36 PM</td>
<td>3.75.190.161</td>
<td>10.16.20.6</td>
<td>File Modified: userpass.txt - Failed</td>
</tr>
<tr>
<td>12:22:56 PM</td>
<td>3.75.190.161</td>
<td>10.16.20.6</td>
<td>New File Added to the path: /usr/programs/</td>
</tr>
<tr>
<td>12:23:29 PM</td>
<td>10.16.20.5</td>
<td>3.75.190.161</td>
<td>File transfer</td>
</tr>
<tr>
<td>12:24:00 PM</td>
<td>178.88.63.233</td>
<td>10.16.20.9</td>
<td>Scan on ports between 8011 - 7000 port range</td>
</tr>
<tr>
<td>12:24:32 PM</td>
<td>10.30.4.5</td>
<td>10.16.20.6</td>
<td>File Accessed: configweb.xml</td>
</tr>
<tr>
<td>12:25:02 PM</td>
<td>192.128.16.47</td>
<td>10.16.20.8</td>
<td>Data Packet transfer</td>
</tr>
<tr>
<td>12:35:34 PM</td>
<td>194.268.32.46</td>
<td>10.16.20.6</td>
<td>Successful Login</td>
</tr>
</tbody>
</table>
Search Options

Source IP

1942563245

Destination IP

From Time

hr min sec

To Time

hr min sec

Show All

Search

Payload Description

Control Packet- fragment 4 - size - 54 Bytes - Duplicate packet 1

<table>
<thead>
<tr>
<th>Time</th>
<th>SourceIP</th>
<th>DestinationIP</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select</td>
<td>12:20:55</td>
<td>194.256.32.45</td>
<td>10.16.20.8</td>
</tr>
<tr>
<td>Select</td>
<td>12:26:34</td>
<td>194.256.32.45</td>
<td>10.16.20.8</td>
</tr>
</tbody>
</table>
Employee ID: 104
First Name: Oliver
Last Name: Paul

Work Role: Staff

Access and Permissions:
Is a staff at the company. Has access to workstations and FTP server.
Post from Analyst1:

WEB-Server: Possible Information Leak

Reply to the post:

Your teammates will reply here.

Your response would be here.
### Systems

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select App Server</td>
<td>10.30.4.3</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select NIDS(Network Intrusion Detection System)</td>
<td>10.15.20.4</td>
<td>10.15.20.0/24</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.19.59.6</td>
<td>10.19.59.0/21</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.19.59.7</td>
<td>10.19.59.0/21</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.19.59.8</td>
<td>10.19.59.0/21</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.19.59.9</td>
<td>10.19.59.0/21</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.5</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.6</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.7</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.8</td>
<td>10.30.4.0/20</td>
</tr>
</tbody>
</table>

### Systems Affected

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Web Server</td>
<td>10.15.20.5</td>
<td>10.15.20.0/24</td>
</tr>
<tr>
<td>Select App Server</td>
<td>10.30.4.3</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.5</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.6</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.7</td>
<td>10.30.4.0/20</td>
</tr>
<tr>
<td>Select PC</td>
<td>10.30.4.8</td>
<td>10.30.4.0/20</td>
</tr>
</tbody>
</table>

Submit Plan