1-1-2014

A Command and Control Approach to Red Teaming

Kaitlin Britt Haynes

A command and control approach to red teaming

By

Kaitlin Britt Haynes

A Thesis
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Computer Science
in the Department of Computer Science and Engineering

Mississippi State, Mississippi

December 2014

A command and control approach to red teaming

By

Kaitlin Britt Haynes

Approved:

David A. Dampier
(Major Professor)

Robert Wesley McGrew
(Thesis Director)

Byron J. Williams
(Committee Member)

Edward B. Allen
(Graduate Coordinator)

Jason M. Keith
Interim Dean
Bagley College of Engineering

Name: Kaitlin Britt Haynes

Date of Degree: December 13, 2014

Institution: Mississippi State University

Major Field: Computer Science

Major Professor: Dr. David A. Dampier

Director of Thesis: Dr. Robert Wesley McGrew

Title of Study: A command and control approach to red teaming

Pages of Study: 29

Candidate for Degree of Master of Science

As the military has to react and respond to cyber attacks, they also are having to develop a way to apply cyber operations to the command and control hierarchy already in use. This thesis studies the requirements for a cyber command and control (C3) and conducts an experiment to test whether a C3 approach to red teaming helps users find more vulnerabilities. Since red teaming is similar in setting to the cyber operations setting, if the team finds that a C3 helps team members find more vulnerabilities, then a C3 environment can help the military better respond to cyber attacks. As a result of the experiment, the control team and the team using the C3 tied. However, participants surveyed indicated that using a C3 environment was more helpful than not using the C3 environment.

Key words: cyber command and control, command and control, red team

DEDICATION

I dedicate this work to my mother who has always supported me in every way possible and to the memory of my grandmother.

ACKNOWLEDGEMENTS

I would like to thank Dr. Robert Wesley McGrew for all of the help he has provided throughout the research process. I thank my committee for their comments on this thesis. I would also like to thank the students that participated in the CTF and provided helpful feedback.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Today's wars rely on computer networks to complete tasks from communicating with troops to gathering intelligence. With the internet playing such a large part in today's society, cyber warfare is becoming a more important aspect of war. Cyber warfare is still a newer concept and "General Alexander in 2007 said that we currently face many similar issues grappling with cyberspace as a war-fighting domain as the military did during the Interwar years from 1919 to 1938 understanding air-power" [6].

For the purpose of this paper, cyber warfare is defined as both defensive and offensive tactics used to gain information about networks, attack networks, or defend against attacks. Cyber warfare is a necessary characteristic of war today. Since so much personal information is stored and transferred using networks, protecting the information is highly important. In addition, gaining access to other information leads to intelligence that can save lives. Erbacher further explains the usefulness of cyber warfare by stating that "[b]y attacking a military network infrastructure a unit can be isolated just as well as they could be through a physical attack but through far less expenditure of resource" [3].

1.1 Command and Control

In conventional warfare a command and control (C2) hierarchy exists through sending information up and orders down a chain of command. Command and control allows the management of troops and all of the tasks that need to be completed for a successful military program. Since cyber warfare is still new, there still lacks a way to incorporate it fully into the traditional C2 system. Currently, the focus of cyber leans towards defense in a reactive form [4]. Whenever an attack is suspected, the victim system is quarantined and analyzed. The results are passed up the chain of command, and then the orders of what should be done in order to fix the vulnerability are passed back down the chain [4].

The traditional C2 system moves slower than the fast pace of cyber warfare. By the time that the suspected attack is passed up the chain of command and then back down to the people who patch the vulnerability, other attacks could have occurred [4]. The traditional C2 process does not work as well for the speed of cyber warfare.

1.2 Cyber Command and Control and the Tools Needed

Since cyber warfare is still being developed and formalized, the closest correlation that can be made to the cyber warfare environment is the red team environment. Red teams act as an adversary hacking into a network in order to find its flaws. In the cyber security realm they complete work similar to a vulnerability assessment and/or a penetration test. The study of how red teams complete their attacks and how they organize themselves leads to a better understanding of a cyber warfare environment and how a cyber command and control can be developed [6].

The cyber command and control (C3) will need tools to make it efficient. Current tools in existence that might help are made for red teams acting as penetration testers. Penetration testers are hired to find vulnerabilities on a network and/or system and deliver a report on the vulnerabilities so such vulnerabilities can be fixed.

In order to find out what kind of tools will assist a C3, the current status of C3 as well as the requirements of a good C3 were researched. Then current penetration testing tools were analyzed and searched for compatibility. The results of the study are reported in Chapter II.

1.3 Hypothesis

This thesis's hypothesis is as follows: A red team will be able to find more vulnerabilities if a cyber command and control approach is applied to red teaming.

In order to test the hypothesis, an experiment was conducted using two red teams. One team used a C3 approach to infiltrating the network and one did not. The experiment is further described in Chapter III.

The follow questions are goals of the research to better understand the results found:

- Are redundancies of the same task being completed reduced?
- Is the process for finding vulnerabilities more efficient because the team is more organized?

CHAPTER 2

LITERATURE REVIEW

To learn the status of the development of a cyber command and control, a literature review was conducted. Once the status of a C3 was found, then possible tools to assist in a C3 were reviewed.

2.1 Cyber Command and Control

2.1.1 Cyber Command and Control Requirements

The literary review revealed a list of requirements for an effective cyber command and control. The requirements included what a commander of a C3 would need and what the C3 should systematically complete.

A commander should be able to easily identify all of the cyber resources [3]. To make the best decisions, a commander needs to be able to imagine where to put all of his subordinates to best accomplish a task. The C3 should have a way to represent all of a commander's teams, the members of each team, and each of the members' abilities.

The system should have a visual way of showing where all cyber capabilities are located [3, 7]. Knowledge of where capabilities are located can impact decisions because of differences in time zones and ability to work with non virtual teams in person. The system should also have a way to sustain and survive "for continuous processing despite failure

on the part of one or more of its component" [10]. In fact, the C3 should be "essentially defect-free in the performance of their gathering, managing, and analysis function" [7]. If a commander cannot rely on the system to always work, then the C3 will never be able to be fully utilized. At the speed cyber warfare could potentially work, defects can make or break a defense or an attack. In addition, in the case of an attack against the C3, if part of the system fails, the C3 should be able to continue so that other systems can still be defended [10]. Otherwise, information could be potentially lost leading to worse consequences.

Considering the speed cyber warfare will be able to take place, the C3 should be able to systematically analyze data from different sources and record information about the network [7]. The ability to systematically analyze and record data frees up users to work on other tasks. The C3 also should have capabilities for autonomous decisions and actions to increase the speed at which the system can react [9]. In addition, the C3 should be able to work well with the traditional C2 system so that as cyber warfare and traditional warfare occur at the same time, the communication and planning works well [3].

2.1.2 The Prototype

Norman R. Howes, Michael Mezzino, and John Sarkesain [4] have created a successful C3 prototype in "On Cyber Warfare Command and Control." In conventional warfare a team member is only a part of one team at a time. However, in the cyber warfare organizational model Howes [4] proposes a team member can be a part of more than one team and teams can be created and removed as needed. He named these teams "virtual cells" [4]. Teams that can be created and removed as necessary are labeled as "dynamic virtual

cells" [4]. Cells are also dynamic in that they do not always consist of the same team members and members can come and go in shifts. Their organizational model consists of a network style organization with a hierarchal chain of command structure inside. Instead of one commander in charge of many people and so on, the model proposes a many-to-many style of communication.

Figure 2.1 shows the organizational model for Howes C3 prototype [4]. The overlapping cells demonstrate that at least one member is a member of both cells. The model also has regional commanders that are members of the different cells in their region. Regions may have more than one commander and those commanders also work with a traditional warfare commander, also known as a kinetic warfare commander.

Figure 2.1 the virtual cells labeled ID Cell, VA Cell, and IR Cell are called "core cells [4]. They are not dynamic, and they cover a particular region of cyber warfare. The figure illustrates some sample core cells. A region would have as many cells to cover whatever it needs as necessary. Core cells also have a commander who works with the regional cyber commanders.

The prototype also dictates an operational model that provides support for intelligence analysis, operations management, operations planning, and operational control. The prototype was written in Java in a publish and subscribe format. It contains windows that show cell members present with their skills and location, a map of networks and their status, a list of tasks to be completed, and more. However, although the prototype has been developed, the paper "On Cyber Warfare Command and Control System" lacks an experimental demonstration of the prototype being tested [4].

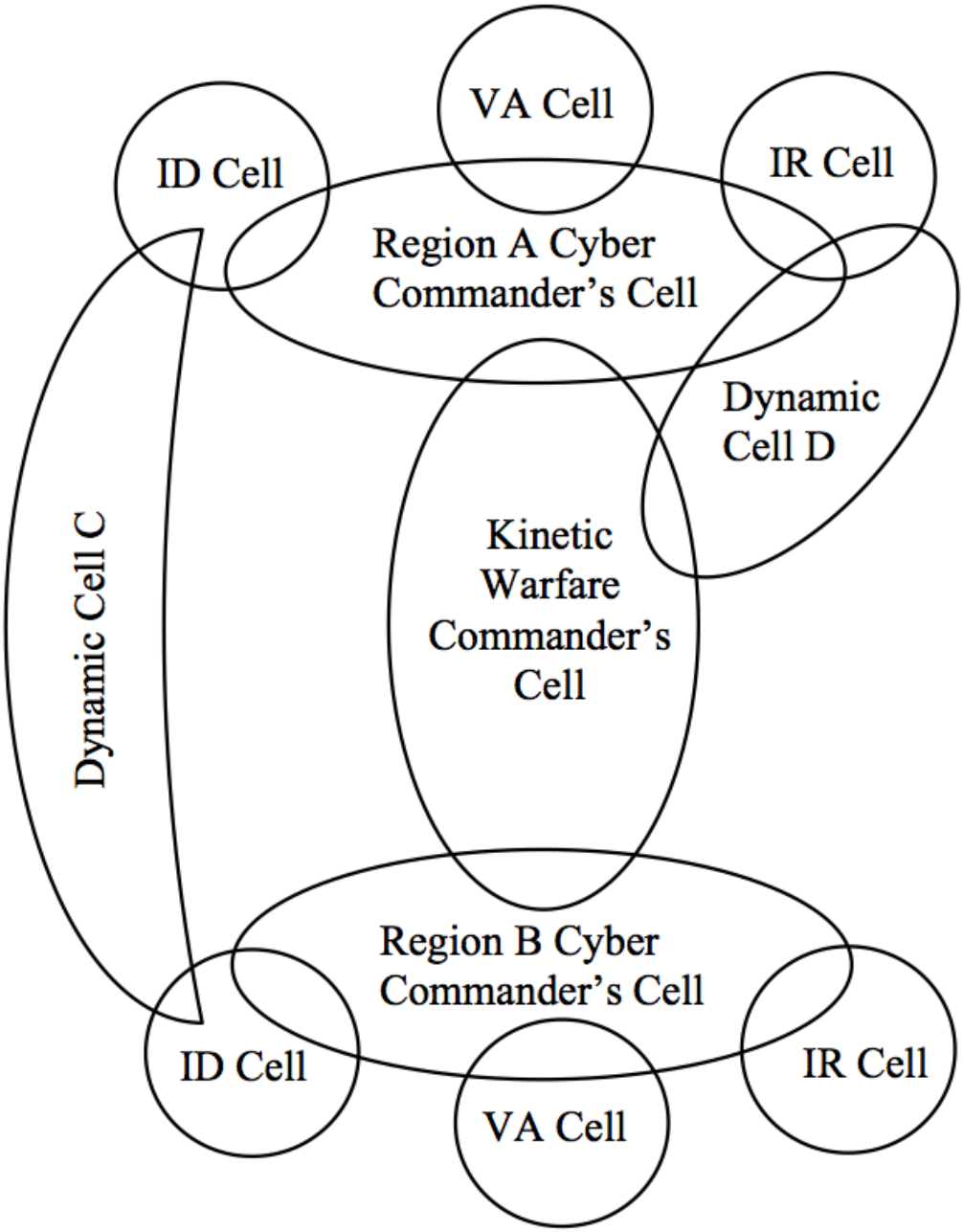


Figure 2.1

C3 Organizational Model [4]

2.2 Current Tools

The prototype also dictates an operational model that provides support for intelligence analysis, operations management, operations planning, and operational control [4]. The prototype was written in Java in a publish and subscribe format. It contains windows that show cell members present with their skills and location, a map of networks and their status, a list of tasks to be completed, and more. However, although the prototype has been developed, the paper "On Cyber Warfare Command and Control System" lacks an experimental demonstration of the prototype being tested [4].

2.2.1 Faraday

Faraday is an "Integrated Penetration-Test Environment" developed by Infobyte [5]. The console consists of a large command line like interface in the top right, a log across the bottom, and a tree of available hosts on the right. The command line like console is to make the tool familiar to penetration testing users. The tool also generates a webpage log once the user is finished. Below Figure 2.2 shows the user interface of Faraday. The image demonstrates user friendly features of the program such as text highlighting, host tree, filters, and the console.

Faraday is written in Python and is meant to be used on a Linux host. Faraday works with over 40 tools used by penetration testers and has an API for developers to add more tools. Faraday detects conflicts between information gathered about IP addresses by different tools, import reports from Metasploit, and filters data. This tool allows live debugging and multiuser capabilities for up to five people for the community version.

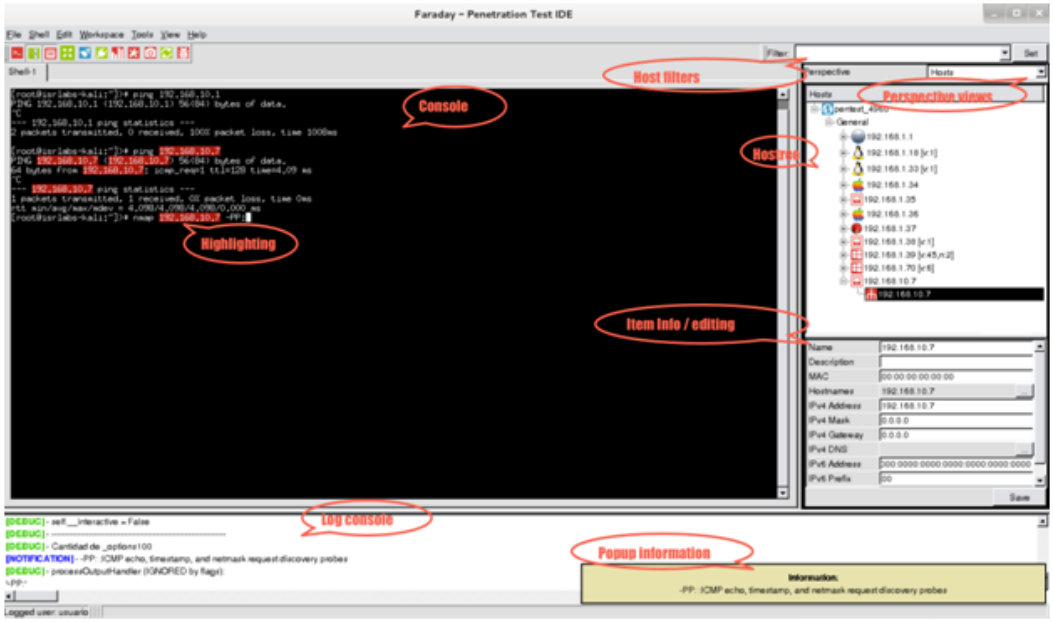


Figure 2.2

Faraday [5]

2.2.2 Armitage

Armitage is a "red team collaboration tool for" the Metasploit framework [8]. Metasploit is an open source penetration testing framework that contains an exploit library [2]. Since Armitage runs in Metasploit, it can complete most tasks that Metasploit can do [8]. Metasploit has attacks for common and typically well-known vulnerabilities [2]. However, a warfare environment will be working with more custom tools and zero days in order to have a more stealthy approach to the attack. Zero days are unreleased vulnerabilities of a system. Armitage has capabilities that allow for a team to work together to infiltrate a network [8]. Armitage creates a log of events that take place during the usage of the tool as well as the chat between teammates. Armitage, written in Java, can run slowly and

has bugs that cause the user to click multiple times in order to complete a task. Armitage user interface consists of a module tree in the top left third and the targets in the top other two-thirds. The bottom of the interfaces contains a tab system that the user can control.

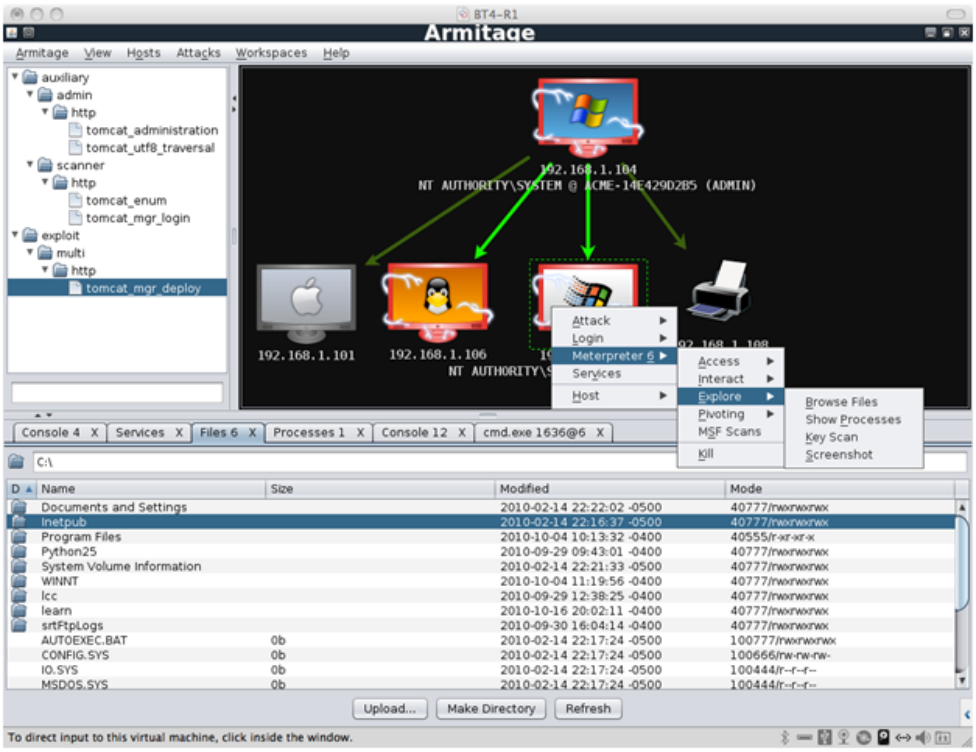


Figure 2.3

Armitage [8]

Figure 2.3 shows the user interface for Armitage [8]. In the top right of the interface, the images of computers demonstrate the different operating systems detected in the network. The computers with red borders are available to attack. In the image, the user has right clicked on one computer. From there, the viewer can see the menus that demonstrate the attacks a user can complete. The bottom of the interface shows all of the files located on an

infiltrated computer. The multiple tabs also demonstrate that the user can have a console, a list of services running, a list of processes running, and a command prompt.

CHAPTER 3

METHODOLOGY

To test the hypothesis an experiment was conducted. The experiment exposed two red teams to a network to attack. One team was educated on the use of a C3 environment while the other team took a standard approach for a red team to attack the network.

3.1 Experiment

Both teams consisted of Mississippi State University students with some cyber security knowledge. Students included had a variety of skill levels from graduate studies to students taking introduction to computer security. Twelve students participated in the study, and each student spent anywhere from two hours to the eight hours participating. The study ran from 9:00 in the morning until 5:00 that afternoon.

A network was set up in a capture the flag (CTF) red team style competition. In a CTF red team competition, flags are hidden across a network and participants hack into the network in order to try to find the most flags. In the experiment's CTF, flags consisted of ten digit hexadecimal strings. The CTF used during the experiment contained over thirty flags hidden throughout seven servers available in the attackable range. The difficulty in finding flags ranged from flags that were hidden in text files to executables that required reverse engineering. Users submitted flags to the scoring server which displayed the current score

of the game and the time and date of the last submitted flag for each team. Participants were given the IP address of the scoring server at the beginning of the game, and the scoring was in the attackable range of the network. Not only did the scoring server keep track of the score and the time and date of the last flag submitted for each team, the scoring server also kept track of all of the flags each team submitted and the time and date they were submitted.

The competition was hosted in a lab with a closed network. Students either worked on lab computers already plugged into the network or used their own laptops and connected to the network. The students were also allowed to use any operating system they wanted. Participants were only allowed to attack computers in a certain range and were not allowed to attack each other's computers. The rules of the competition also did not allow the students to edit or to remove any of the flags.

Participants competed as a member of one of two teams with six members each. One team, the experimental team, used a C3 environment that was developed for the experiment and had a commander that was chosen to lead the team. The C3 environment that was developed focused on a subset of the requirements that a C3 should have to test the validity of the hypothesis. The environment consisted of a website that aimed to help the team with team management and task management, and only the C3 team was able to access the website. Through team and task management, the commander and members of the team could see all of the cyber resources the team had by viewing pages that detailed on what tasks each person and each team were working. More details about the C3 environment are explained in Section 2 of Chapter III.

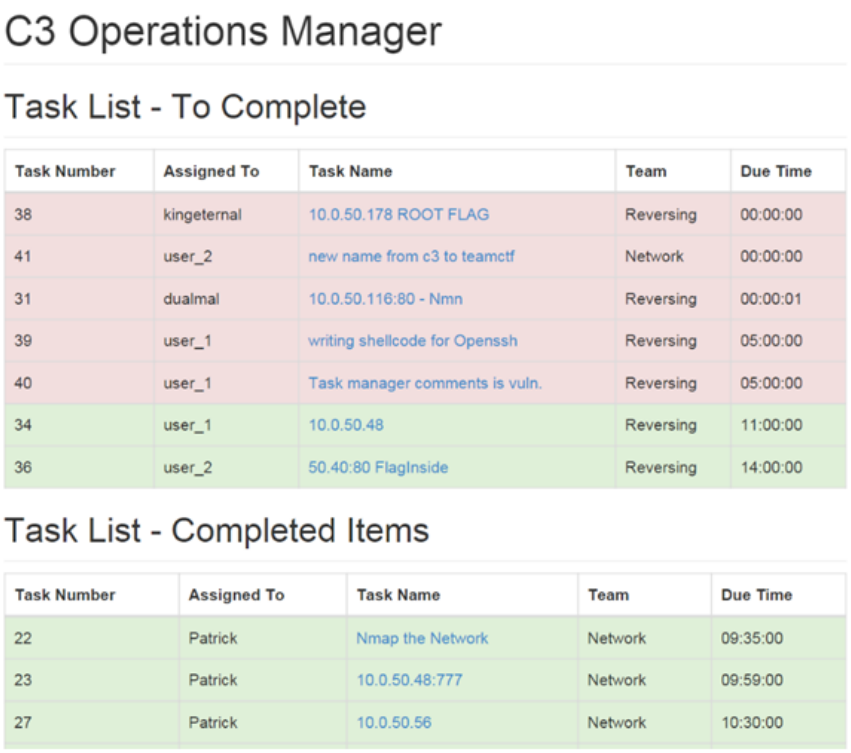
The experimental team was introduced to the C3 environment at the beginning of the CTF. The commander showed the team how to use the interface and all of the features of the environment. The team developed an organized structure meant to duplicate a C3 with a commander, sub teams that focus on certain types of tasks, and team leaders for each of those sub teams. The other team, the control team, was left to organize and divide tasks as they wanted, without assistance. Both teams were instructed not to communicate with the other team about the CTF in order to keep the opposing team from securing any advantages and to keep the two organizational structures distinct.

The students were surveyed to attain a better understanding of what happened beyond the final score of the competition. Both teams were asked the strengths and weaknesses of their approach to finding vulnerabilities and flags on the network. The teams were questioned about how they divided tasks, how they communicated, how they organized the team, and how or if they kept track of what tasks had been completed.

Constraints on the experiment limited its accuracy. Since participants were selected to be on a team at random, one team could have had a much higher skill level than the other team. This experiment also only had one trial which limited the accuracy of results. Students also took part in the study for different amounts of time even though overall the experiment lasted eight hours. Since some students participated all day and some students only worked a couple of hours, the total amount of time spent participating by one team may have been different than the total amount of time spent by the other team. The differences in time could have given one team an advantage.

3.2 Implementation of a C3 Environment

To test whether a C3 environment increased the vulnerabilities found by a red team, a C3 environment was set up for the experiment. This thesis focuses on testing the requirement that the commander and the team must be able to see all of the resources that are available so that informed decisions can be made [3]. With that requirement in mind, a website was created to help the team manage teams and tasks.



C3 Operations Manager

Task List - To Complete

Task Number	Assigned To	Task Name	Team	Due Time
38	kingeternal	10.0.50.178 ROOT FLAG	Reversing	00:00:00
41	user_2	new name from c3 to teamctf	Network	00:00:00
31	dualmal	10.0.50.116:80 - Nmn	Reversing	00:00:01
39	user_1	writing shellcode for Openssh	Reversing	05:00:00
40	user_1	Task manager comments is vuln.	Reversing	05:00:00
34	user_1	10.0.50.48	Reversing	11:00:00
36	user_2	50.40:80 FlagInside	Reversing	14:00:00

Task List - Completed Items

Task Number	Assigned To	Task Name	Team	Due Time
22	Patrick	Nmap the Network	Network	09:35:00
23	Patrick	10.0.50.48:777	Network	09:59:00
27	Patrick	10.0.50.56	Network	10:30:00

Figure 3.1

C3 Task List

The website gives the users a way to see all of the tasks that users are assigned and that teams are assigned. Each task has a task number, a user assigned to that task number,

a name, a team assigned to that task number, a due time, a recording as to whether the task has been completed or not, and a user that created the task. Figure 3.1 exhibits the main table that the users of the C3 see when viewing all of the tasks. The red rows present tasks that are past their due time while the green rows demonstrate tasks that still have time before they are due. The completed tasks appear in a different table below the table that contains all of the tasks that have yet to be completed. By separating the two tables, users are able to see quickly what needs to be done.

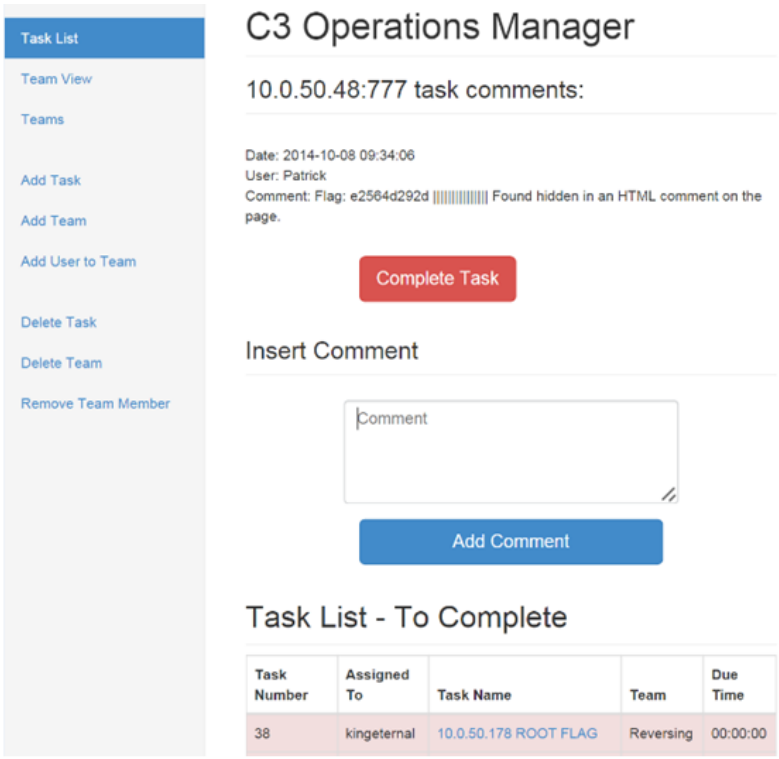


Figure 3.2

C3 Task Comment

Any user of the system is able to create a task. The user that creates the task also names it, assigns the task to a team, enters a due time, and based off the users assigned to the assigned team, selects a user to work with the task. The user who creates the task is the only user that can delete that task.

Tasks also can have comments that users can create. Users are able to click on a task name in order to see all the comments others have made about the task, make comments themselves, or mark the comment as complete. Figure 3.2 shows a comment a user made about a flag that was found. By naming the task the IP address of the vulnerable server and then detailing what the flag was as well as where it was found, other users were able to know quickly not to submit the same flag if another team member had already found the flag. Any user of the website can view the task and comment on it. However, only the user assigned the task can complete a task.

Teams can also be managed on the website. The teams page of the website demonstrates a list of all of the teams created and all the members on each team. The goal of the page is for all users to have an idea of the capabilities of every user so that the best choices can be made when assigning a task to someone. The team view page displays all of the tasks that are assigned to each team. The team view page is most helpful to the team lead because this page presents the tasks that each team is assigned and their status in separate tables based on the team. The team lead is the only person that can delete that team and add or remove users from that team.

Figure 3.3 exhibits two tables on the team view page. The top table reveals the team's list of tasks. Users are able to see all of the information about each task that is assigned

to the reversing team. Below the reversing team's task table is the table of tasks for the network team.

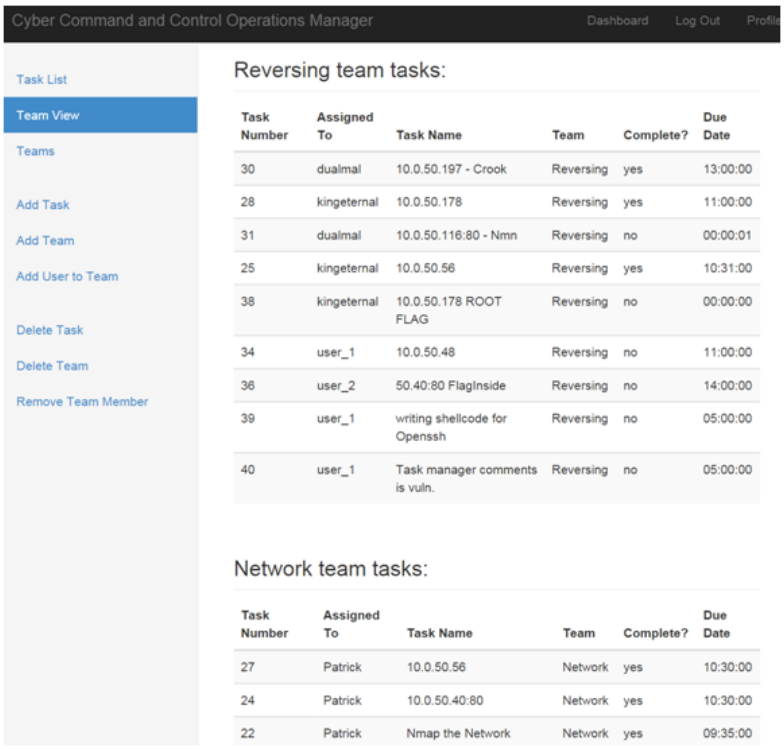


Figure 3.3

C3 Team View Page

The profile page allows users to see all of the teams of which they are a member and all of the tasks that they are assigned. Pages like the profile page and the team view page become advantageous when so many tasks exist that searching the main task page becomes confusing. By breaking down the pages, users are able to quickly process information. Figure 3.4 is an image of the C3's profile page. In the image the user admin is a member of one team and is assigned task 26.

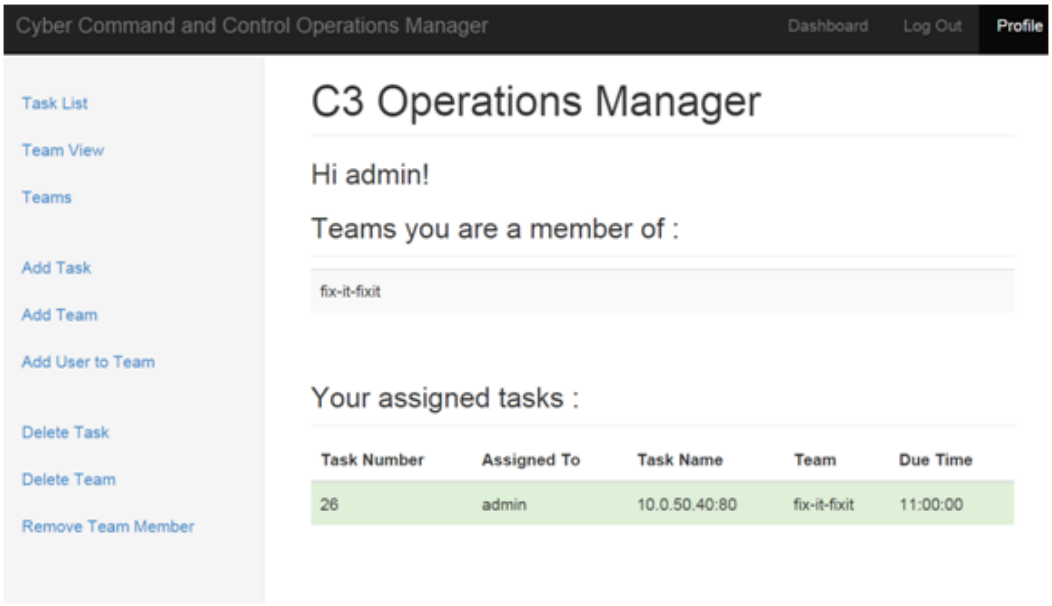


Figure 3.4

C3 Profile Page

The C3 website also has a sign in page and a registration page. The registration page built for the experiment allows anyone who has the address of the website to register and gain an account. Figure 3.5 displays the registration page. The registration page validates that emails entered are in the correct format and that passwords meet the minimum requirements described on the page.

The C3 environment website's backend was developed in PHP with a MySQL database. The database was made up of five tables: task, task_comments, team, team_users, and users. The task table consists of rows for the id, assigned user, name, completeness, team, due time, and creator. The table task_comments table recorded the id, task name, date it was created, comment, and user who created the comment. Rows for the team table were created for the team name and the team lead. The team_users table displayed rows

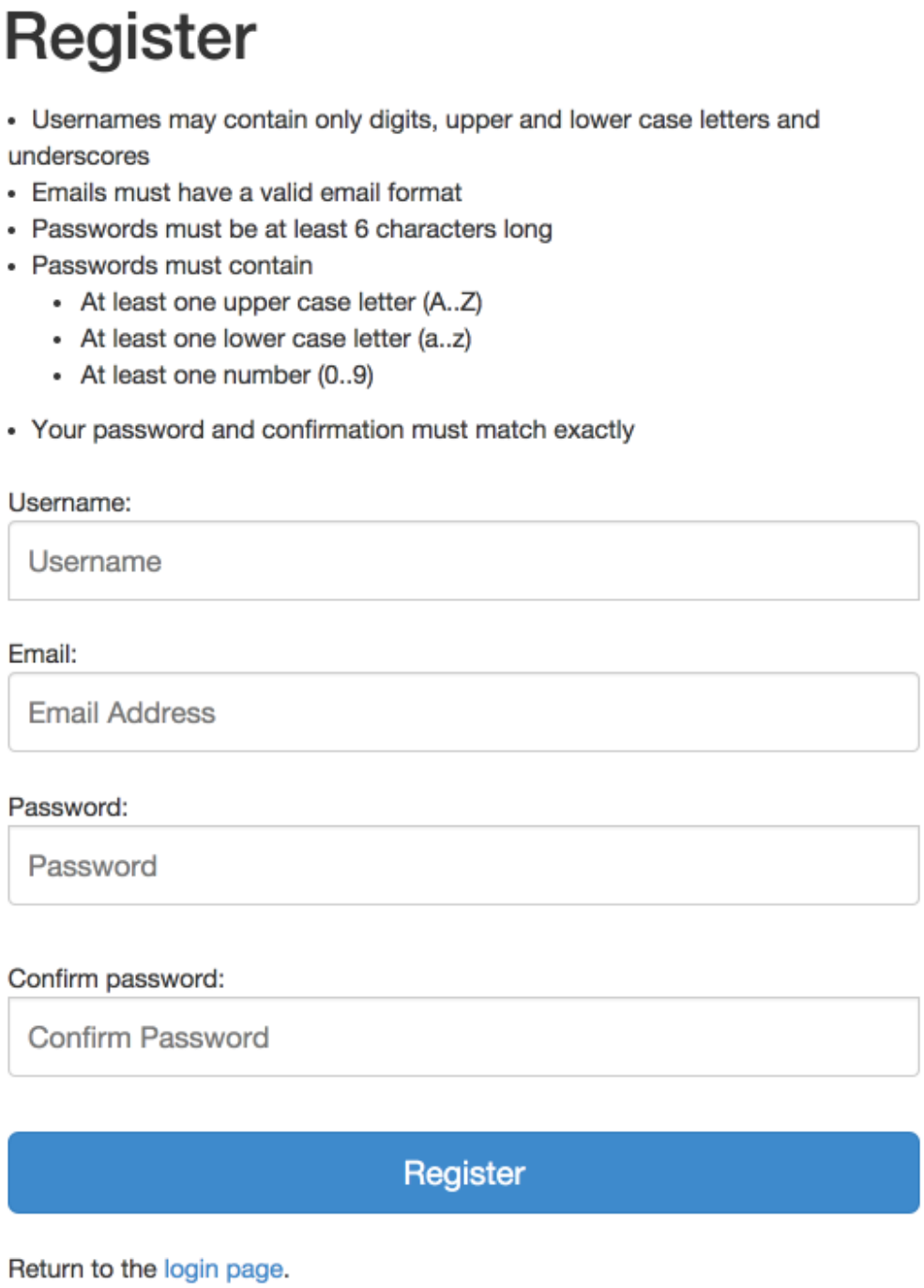


Figure 3.5

C3 Registration Page

to represent the id, team name, and the user on the team. Rows included in the users table were the id, username, email, password, and salt for each user.

The front end was created by using the Bootstrap 3.2.0 framework. Bootstrap is a framework of HTML, CSS, and Javascript code meant to help developers create websites quicker [1]. Bootstrap provided the support for certain extra features of the website such as the colored rows of the task table, the time format, and the front end template.

CHAPTER 4

RESULTS

The results of the study are broken down into the results of the CTF competition and the survey completed by the participants of the study.

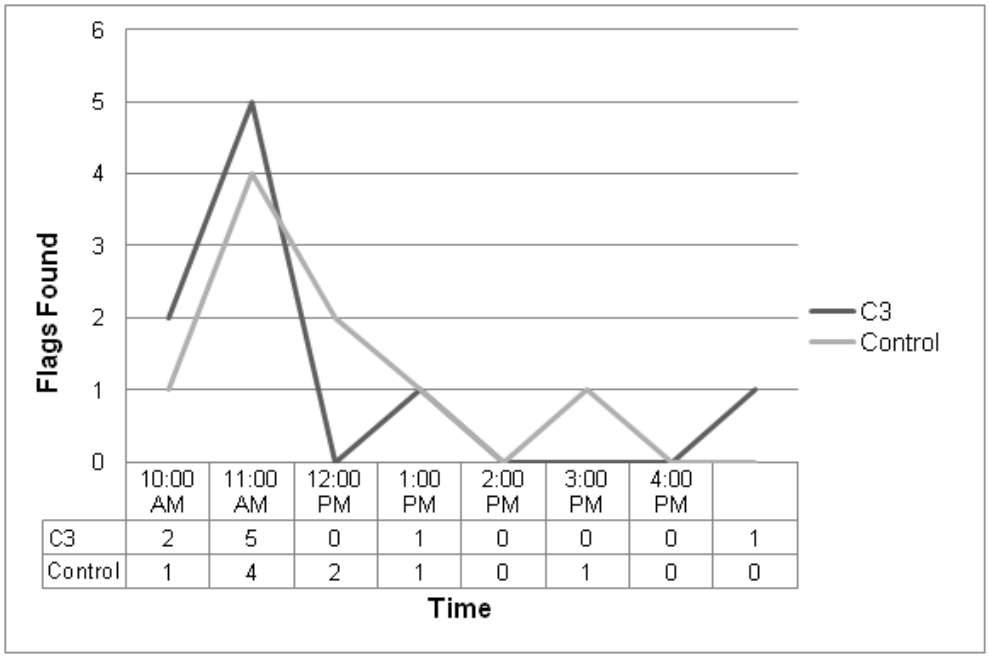
4.1 Results of the Competition

To help understand whether the C3 gave the experimental team an advantage, the score of the CTF did not reveal much data. The experimental team and the control teams tied with a score of nine each. A majority of the flags for both teams were found during the morning with the most flags being found between 10:00 AM and 11:00 AM. After noon both teams found only two flags. The teams found six of the same flags throughout the day.

Figure 4.1 presents the number of flags found throughout the competition. By 10:00 AM both teams had found at least one flag, and the most flags were found between 10:00 AM and 11:00 AM with the C3 team finding five flags and the control team finding four.

4.2 Results of the Survey

The survey that the twelve participants completed after the competition revealed that the C3 team benefited from the use of the website. All of the C3 team members that



	10:00 AM	11:00 AM	12:00 PM	1:00 PM	2:00 PM	3:00 PM	4:00 PM	
C3	2	5	0	1	0	0	0	1
Control	1	4	2	1	0	1	0	0

Figure 4.1

CTF Flags Found

worked multiple hours and that used the C3 felt it benefited them and made them more efficient. The only team members that felt they repeated tasks commented that tasks were repeated because either they did not refresh the website and, therefore, did not have access to the latest information or because a teammate did not provide adequate information in the comments on the task about the flag that was found. Every member of the C3 team except for one felt that they knew what all of their teammates were working on most of the time during the competition.

The C3 team used the C3 website to keep track of tasks. They also talked in the lab to strategize about what tasks to complete and who should complete them. Verbal communication also played a part in helping keep track of what teammates were working

on and what they needed help with in order to fill gaps where teammates were not using the system. At the beginning of the CTF the commander assigned tasks to the team members, but as the day progressed and different team members were present at different times, the structure became more relaxed and the users contributed in the way they felt was the best. Most users kept the C3 website up on the side of their desktop to view while looking for flags. In the survey team members mentioned that they felt the team would have benefited if some of their teammates followed the protocol better by using the website more, adding the tasks more often, and documenting the tasks in more detail. In addition, a user felt the commander would be more effective if the commander was able to focus more on managing the team instead of finding flags.

The control team had conflicting points of view about task redundancies, task management, and communication. The participants were asked if they felt that the same tasks were completed over and over again. Three of the members of the control team replied yes and three replied no. The team did not organize itself, and team members agreed that they worked on the tasks with which they were familiar. A majority of the team stated that they did not know what others on their team were working on throughout the competition and that they communicated verbally when they did work together. The team overall disagreed when asked if their method of communicating worked well. At one point in the experiment the more advanced members became a sub team to complete tasks.

Some team members stated that they did not think that they failed at keeping track of what tasks had been completed, but multiple team members believed that by keeping track of tasks verbally was not the most effective. Team members stated that either writing down

the tasks they had completed or having some visual way of sharing information would have helped them keep track of tasks better. A majority of team members thought that better organization, keeping track of tasks, and communicating better would have improved the team.

4.3 C3 Environment Additions

The survey asked participants what would make their experience better. The students took the question as an opportunity to request more features they felt the C3 needed. A majority of participants would have preferred to have a chat client in the environment to help communications and so that the other team could not overhear their discussions. A user also suggested a general discussion page. A general discussion page might provide users with a place to strategize and still have easy access to review the plans later.

The website did not automatically refresh when tasks were added. Whenever users were finding several flags quickly and when a majority of the team was present participating in the CTF, the other users would miss updates and accidentally repeat the task just completed.

In addition to refreshing, a participant requested a notification system. A notification system would help users be able to find a task to work on quicker. If users were notified with each task added to the system or completed, they would no longer need to scan the task list to see what others had done. They would automatically know what had been completed since they last checked. However, a notification system like the one described would need a lot of customization capability for users so that they could choose the notifications they

receive. The customization would be especially important in an environment with a very large team since the amount of tasks being added and worked on would also be very large. A system where users heavily rely on the sub teams would probably only need notifications for the sub teams with which they work. However, on a team as small as the one in the CTF experiment, getting notifications for all of the tasks would probably be helpful.

Also, users would have benefited by having notifications from the system when a task was assigned to them. Since the team was only six people and they were located next to each other while working, the teammates were able to tell each other when they needed someone else to work on a task and to check the C3 website. However, user tasked notifications would be beneficial for both the experimental team and a much larger team. The experimental team would not have had to risk being overheard by the opposing team nor would they have had to interrupt the other user while working unless they had wanted. Task notifications would be just as useful for a larger team which heavily utilizes the sub team structure and assigns tasks to others using the C3 website.

Another request made by a participant was for the website to have a way to upload files so that files would not have had to be manually transferred or found again. Participants came across instances where one user found an executable that needed to be reverse engineered and the user had to find a way to get the file to another participant that could reverse engineer it. In such instances a file upload page would have been beneficial. A file upload page might also be helpful if users wanted to show screen shots or other files to users to help them find more flags.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

This thesis covers the testing of a C3 type environment in a red team CTF event. Although the score of the CTF did not reveal that a red team was able to find more vulnerabilities if a C3 approach were applied, the results of the survey presented to participants in the experiment showed that users felt the C3 approach was a better approach.

The follow questions were asked in the introduction to better understand the results found:

- Are redundancies of the same task being completed reduced?
- Is the process for finding vulnerabilities more efficient because the team is more organized?

All of the C3 team believed that they were not completing the same tasks over and over again except for when users did not properly use the system. In contrast, the control team did not agree that they were not repeating tasks. The general consensus of the control team was that they would have done better if they had been using a system for managing tasks.

All of the C3 team believed that they were not completing the same tasks over and over again except for when users did not properly use the system. In contrast, the control team did not agree that they were not repeating tasks. The general consensus of the control team was that they would have done better if they had been using a system for managing tasks.

Future work for this topic should include both more trials and an improved environment. The experiment should be run for a longer period of time with both team sizes of less than ten as well as larger team sizes. A longer period of time will give team C3 users more time to work on the difficult tasks in order to take advantage of the task management system beyond posting results. Running the experiment with larger teams will test the use of the sub teams more than the experiment ran in this thesis. In the experiment ran for this thesis the C3 environment only tested part of the requirements of a C3 environment. Also, the system should be tested with the improvements the participants suggested including a chat client, a notification system, and an uploading page.

REFERENCES

[1] "Bootstrap," www.fastandeasyhacking.com/manual (current 14 Oct. 2014).

[2] "Metasploit," http://www.metasploit.com (current 16 Oct. 2014).

[3] R. F. Erbacher, "Extending Command And Control Infrastructures To Cyber Warfare Assets," *Proceedings: 2005 IEEE International Conference on Systems, Man and Cybernetics*, Waikoloa, Hawaii, Oct. 2005, IEEE, pp. 3331–3337.

[4] N. R. Howes, M. Mezzino, and J. Sarkesain, "On Cyber Warfare Command and Control Systems," *Missile Defense Agency*, 2007, http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA465692 (current 14 Oct. 2014).

[5] Infobyte, "Faraday," https://github.com/infobyte/faraday/blob/master/README.md (current 14 Oct. 2014).

[6] S. Liles, J. E. Dietz, M. Rogers, and D. Larson, "Applying Traditional Military Principles to Cyber Warfare," *Proceedings: 4th International Conference On Cyber Conflict*, Tallinn, Estonia, Jun. 2012, IEEE, pp. 1–12.

[7] J. M. Prescott, "Autonomous Decision-Making Processes And The Responsible Cyber Commander," *Proceedings: 5th International Conference on Cyber Conflict*, Tallinn, Estonia, Jun. 2013, IEEE, pp. 2325–5366.

[8] Strategic Cyber, "Armitage Manual," www.fastandeasyhacking.com/manual (current 14 Oct. 2014).

[9] E. Tyugu, "Command And Control Of Cyber Weapons," *Proceedings: 4th International Conference on Cyber Conflict*, Tallinn, Estonia, Jun. 2012, IEEE, pp. 1–11.

[10] D. Vukelich, D. Levin, and J. Lowry, "Architecture For Cyber Command And Control: Experiences And Future Directions," *Proceedings: DARPA Information Survivability Conference and Exposition*, Anaheim, California, Jun. 2001, IEEE, pp. 155–164.