Evaluating ORNL Cyber Security Tools

Katherine Williams

August 2012

Oak Ridge National Laboratory
Oak Ridge, Tennessee

Abstract- Finding vulnerabilities and how to fix them is a fundamental task in cyber security. At Oak Ridge National Laboratory, this takes place every day. The goals for this project were to assist with the integration of newly purchased and future security tools, as well as to better manage the data being produced by the tools. To achieve these goals research was required which involved working with tool administrators to determine and document how the current tools work, what data the tools produce, and the interconnections/dependencies between the tools. This project resulted in a tool flowchart, revealing connections between tools. Information on data management and recommendations for a new internal composite risk scoring system were developed as well. Completion of this project gives the security teams the ability to better understand their systems at a glance, as well as implement a new vulnerability detector.

The Research Alliance in Math and Science program is sponsored by the Office of Advanced Scientific Computing Research , U.S. Department of Energy. The work was performed at the Oak Ridge National Laboratory, which is managed by UT-Battelle, LLC under Contract No. De-AC05-00OR22725.
This work has been authored by a contractor of the U.S. Government, accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

DRAFT

1. Introduction

a. Cyber Security

Crime in our world is constantly evolving, changing to adapt to how people communicate and live. More threats are emerging in the online world every day, and most people do not completely understand the risk they expose themselves to. Just like in the physical world, not all thieves are the same. Some want to scam their victims out of money, while others want your identity to sell or acquire for themselves. There are also people who seek to break into the virtual world of a company, and steal data from that company. Part of cyber security involves protecting users' information by preventing attacks against these users. It is a dangerous place in the cyber world. As

stated by the United States Computer Emergency Readiness Team (US-CERT), "Among the dangers are viruses erasing your system, someone breaking into your system and altering files, using your computer to attack others, or someone stealing your credit card information [1]." Identifying and understanding what is lurking out in the cyber world can help better protect us from those dangers. If we cannot understand what is dangerous, how can we hope to develop ways to protect ourselves?

No one is safe from cyber-attacks, large companies and government facilities especially. The goal of these large corporations, in terms of cyber security, is to limit the number of vulnerabilities their systems have while still retaining the ability to connect outside their own network. This goal can be hampered in many ways. From budget constraints to limited security personnel, obtaining and keeping technically secure Information Technology (IT) resources can be difficult. With new technology being developed every day, it is a race between those securing that technology, and those wanting to exploit weaknesses in that technology for their own gain.

Everyone has data they want protected, but using data to help protect the system is not the first thing most people think of when considering cyber security. Yet, using data is a basic tool of cyber security.

b. Data Management

So how does data help protect a system? Every company has a way of securing their information and protecting it from people who are not authorized to have access to that information. These are often called security tools. There are thousands of different security tools to choose from, and there are hundreds of different types of security tools. They can range from free open-sourced software, generic off-the-shelf tools, to expensive custom designed systems built just for one company.

Take a simple anti-virus program. It runs on the computer, scans files and looks for known virus signatures and suspicious behavior, then alerts you if a problem is discovered. The alert is information derived from the tool's data, because the program is telling you that your system could possibly have an infection. This idea can extend to other security tools as well. Data gives you information that the company can then use to make an informed choice of what to do next.

DRAFT

However, there are several important points to make about using data with security. The first is that the data that is being examined is useful and understandable. A security team can gather just about any data they want as long as the tool they are using can be used for that purpose. However, not all of that data is useful. For a security team, they may have a tool that can identify the make/model, the age, and the Internet Protocol (IP) address of a machine. But the age of a machine is not really useful data in terms of security, so why pull it. If you are pulling in data about your security that is not useful, it is a waste of time, money and resources that could be spent elsewhere, potentially helping identify real threats to the security of the company's network. A company should not, and most likely will not, spend money on a tool that pulls in useless data.

Another point in data management that must be thought about is space and time. Again, security tools can be used to pull in information about a system. The problem is that the data being gathered has to be stored. It takes space on the company's network to pull in that data and send it to where it needs to go (e.g. the sensors that collect the data), but it also must take up space wherever it is stored. Large amounts of data can use up network bandwidth quickly, causing freezes and delays in other critical systems. Not only does a security analyst have to know how much bandwidth a data pull needs, but when the network can handle the extra load. Time also plays a factor here. Depending on the tool, it can take a lot of time to pull in the requested data. Then time has to be spent going through the data to understand what the data is telling the analyst. The more data being brought in, the longer it can take to analyze.

A best practice when managing data is to pull in only what is needed, have it in a format that is clear, and can be easily formatted into a report for others. A way to make a clear data reading is to create a scoring system. Within that score, certain elements are examined by the security tools and a score can be assigned to an asset (with an asset being defined by the company or security analyst). This score can be created to focus on a certain aspect, such as vulnerability exposure.

c. Composite Risk Index Score

One idea on the front of scoring is a composite risk index score. This score can be created as best suited to a company's needs and assets. Generally, the scoring system is

DRAFT

written so that it is the impact of a certain event multiplied by the probability of that event occurring. There are multiple other scoring systems. Some scoring systems are built into security tools while others are separate bits of code that calculate the score and create a report of the calculations. A common score in cyber security is the Common Vulnerability Scoring System (CVSS). On the National Vulnerability Website, it states that the CVSS "provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores [2]." For some groups, like government agencies and laboratories, there are specific guidelines that must be followed, to show that their cyber security is up to standards for protection against attackers and hackers who are trying to get in. Some guidelines include having an accredited scoring system like the CVSS.

A composite risk score can be very beneficial. Take for example a scoring system that rates the vulnerabilities of an asset (such as an individual computer), so that the higher the score, the more at risk the machine is. It allows security analysts to get an idea of where there are risks and what needs to be done to decrease that risk. Scoring systems can help security teams to focus on the most vulnerable areas of their network. An individualized risk assessment is better than a generic, industry-defined one because the individualized assessment takes into account the holes and fixes in the system. If a patch defined as critical is released for the Windows XP operating system, but the company only has a dozen XP machines that are not always on the network, then the patch really is not as important as it has been labeled by the industry. For a company, a patch for something else may be more important than that Windows XP patch. Security teams can then focus on the truly vulnerable areas, instead of using time fixing assets that do not pose a significant risk.

2. Background

a. Cyber security at Oak Ridge Laboratory

The cyber security teams at Oak Ridge National Laboratory (ORNL) use multiple security tools of varying sorts to help protect the lab from online threats. Because of the projects that are worked on at the lab, there are portions of information that are labeled

DRAFT

classified and have to be protected even more. Security tools are the weapons and defenses used against the cyber warfare that rages every day.

It takes a wide range of tools to protect any network. The types and number of tools depends on multiple factors, such as network size, budget, security staff, and goals of a security plan. ORNL has over 30 data tools, most of which are security related, though not all are, and most of these tools are interconnected in some fashion. All tools produce some form of data that provides valuable information to the Risk Management and Cyber Operations teams to identify, evaluate, and react to discovered vulnerabilities and problems within the network. While the processes in which to do these actions are not always complicated, time and manpower are limiting factors.

Most security scans performed at ORNL have to be focused and spread out, so as not to overload systems' capacities and overwhelm the security team with data about ORNL's network. It is a balancing game that has to be played out, creating the question of, "how to get the most useful data about the network, with the smallest impact on time and money?"

b. Managing data

For data management, the understanding of the data being harvested is invaluable. At ORNL, data is passed between tools, and then organized into reports that can be read by team leaders and directors. Different reports require different data, and the information has to be in a usable format for each team.

In terms of managing data, ORNL has several smaller databases that contain information about the lab. These tools, such as SAP (a people manager) and NetReg (a device database), are the supporting backbones in terms of providing information not only to other cyber tools, but to lab employees as well. ORNL does not have a configuration management database (CMDB), though the lab is in the process of implementing one.

Having a CMDB benefits in many ways. One feature of having a CMDB is its ability to sort the data within its databases and create reports that would be more difficult to generate if pulling from multiple tools. The CMDB does not replace any particular tools, it simply consolidates the data from those tools into one location. If a system needs to be taken offline for maintenance, a CMDB can create a report of what

DRAFT

users use that particular system and their contact information so the administrator can alert the users of the upcoming downtime. CMDBs can have many positive features. But what can be done with that to organize data?

c. Use of a composite risk index score

Having usable data is only part of the process to determine where vulnerabilities are lurking on a network. There are many ways to find individual problems, but sometimes, it is more efficient to find and focus on more at-risk wholes, than scattered pieces.

At Oak Ridge, security tools search and report designated issues and holes in the system that opens the lab up to threats. For example, Nessus, a vulnerability scanner, searches for known vulnerabilities on the ORNL network. When it finds issues, it sends a report back to the administrator alerting them to a problem. Every tool has its own policy and procedure. Oak Ridge can also look at outside sites and by comparing it to a known threat database and calculating the risk, can determine if a site is potentially dangerous to ORNL and block it. The lab has many tools to help identify and gauge risks to the lab's network. However, there is another useful solution that has not been created: an internal risk scoring system.

3. Project Objectives

a. Integration of newly purchased/future tools

One of the first objectives of this project is to find ways to better integrate new tools, as well as future tools. Any security tool purchased, or being considered for purchase, has to be able to be assimilated alongside ORNL's current set of cyber tools so that it does not duplicate data that is already being gathered by other tools. Newly implemented tools, such as the new RiskVision, are trying to be tied into ORNL's current system so there is a more efficient use of data to identify cyber security risks. By creating a flowchart of data being produced, and where that data is going, managers will be able to examine ORNL's current structure and see where gaps lie within the system, so they may expand a current tool, or purchase another tool, to cover the data gap.

In order to help find ways to better integrate the security tools, it is decided that a visual aid of the data moving between the tools would be created in the form of a flowchart. The flowchart will be a high level view, meaning that a line would represent

DRAFT

the connection, but the specific data would not be listed on the chart. A separate table will list all of the connections between the tools and have the specific data that is being transferred.

As these pieces are being created, information about the security tools and related IT tools will be gathered. That information will help with the understanding of how the tools work, how they fit into use at ORNL, and how future tools can be integrated. With a visual representation, as well as a basic understanding, it is hoped that with the completion of this project, there will be a better idea of how new and future tools can be added to ORNL's arsenal of equipment so those tools can have maximum effectiveness.

b. Better management of data

Another point that was accomplished as part of this project is with the understanding of how data is used at ORNL now, recommendations can be made for future data management. This is to be accomplished by doing a literature study, and researching a number of best practices to see if a particular practice would be relatable to ORNL's systems and adjustable for the lab's goals. At the end of the project, a goal is to be able to recommend a practice that will benefit ORNL by being able to better manage data in terms of data gathering and data usage.

c. RIFIS (Risk Index for Internal Systems)

The third goal of this project is to make a recommendation for a new tool. This new tool would be used as a risk index for internal systems. In other words, create a scoring system that would rate how vulnerable of an asset within ORNL is to the outside world. There is no tool that has this functionality in ORNL's current group of systems, though there are tools with scoring systems built in. By recommending an internal risk scoring system, it is hoped that by comparing test runs of the new scoring system against current tool scores, the new internal risk score will help the Risk Management team (RMT) and Cyber Operations team (CO) identify assets operating within the lab that leave ORNL at risk for attack, instead of just focusing on outside concerns. The firewall has two sides, and the lab already has measures in place to protect the network from attackers trying to get in. Creating an internal risk score gives the security teams a way

DRAFT

to identify weak points in security on the inside of the network. By covering both sides of the firewall, ORNL find ways to better protect itself from attackers trying to break into the network to steal valuable information.

4. Methodology

a. Working with tool administrators

A large percentage of information that went into this project came from the administrators and staff that work at ORNL. This research project differs from most in that information cannot be found in a book. In fact, most information about the cyber security tools and IT tools comes from the staff who works with these systems. There are some tools (seven total in the scope of this project) that were created "in-house" meaning they were created at ORNL for ORNL. They are not systems that anyone else has. You cannot go out onto the web and look up information about these tools. The rest of the tools (approximately twenty in the scope of this project) used at ORNL are considered "off-the-shelf" meaning they are created by outside companies for any company to buy. Software that is considered to be off-the-shelf can be tweaked to fit the needs of the company purchasing it, but the underlying structure is not created specifically for ORNL operations. Some functions of these software programs are changed to benefit the company, while other features are not even used. Only by talking to those at ORNL who manage and run this software, can information about these tools be gathered. There is no database or book to lookup this information.

There were a wide variety of people that had to be surveyed to in order to cover the number of tools being examined in this project, including many technical support specialists working in a specific area, such as risk assessment, network operations, service and support, etc. Therefore, those specialists only focus on specific tools that help them with their job, and those tools they understand the best. Sometimes, multiple specialists had to be consulted in order to cover all of the points a tools hit because a tool had a large area of functionality.

b. Secondary research

Some secondary research, in the form of online research, was conducted. Most online research was conducted in order to better understand how something, like

DRAFT

network packets, worked. There was not a lot of previous background experience to rely on, and some self-teaching was needed to understand finer details on certain processes. Readings on best practices for data management were conducted. Articles and essays on the subject were read through, and notes taken down. Any useful articles or essays were noted or downloaded for future referencing. Aside from this, there was little research conducted outside of the lab due to previously stated reasons.

c. Creation of end-project pieces

Once information about the tools was gathered, it had to be sorted into useful information, and secondary information. While some information was interesting, it was sometimes out of scope of the project. The project had a limited time frame in which to be completed, and precedence had to be given to the areas of research being focused on. The information relevant to the project was written out, and adapted to fit into a form to best showcase it. In the case of this project, a flowchart was formed to show the data connections between tools. The data table was a simple table that listed the tool data was coming from, where it was going to, and a box that listed all of the data moving between the two tools.

5. Results

a. Research into ORNL Risk Management

There are many different types of tools used within the cyber security world. The same goes for the management tools that this project covered. There are twenty-eight tools that were covered by the scope of this project, although there are many more tools at ORNL. These twenty-eight tools were the main focus of this project, and the most heavily used by Risk Management and Cyber Operations. A flowchart was created to show all of the tools in scope, naming each tool, giving a short description, and showing the connections to other tools. Several properties were identified within the flowchart (See ***Appendix A*** for generic flowchart).

The first task was to identify the classification of each tool. Another team at ORNL, which was working on a database management project, classified a percentage of tools that ORNL had. Their three classifications were discovery, agent, and repository:

DRAFT

- Discovery classification: considered to be highly automated and machine driven, not needing special configurations to run.
- Agent classification: tools that need client and server software to run. The software has to be installed on the asset (such as an employee's computer) and on the server, so the tool can pull data about the asset onto the server.
- Repository classification: human interaction is required for the tool to populate data. These tools often have to be updated manually and given a command to run in order to gather data.

Not all tools were given a classification, but if a tool had one, it was listed on the flowchart so that it could be determined at a glance what kind of action the tool took.

After identifying the classification, each tool was labeled with a short description of what it was. The labels on the flowchart were brief, though greater detail was provided in the tool summary. Most tools had different labels, since most functioned differently. Tools had titles like Firewall Exception Manager, Network Access Controller, Device Database, among others. The only tools with the same description was SourceFire, Snort, and Snot, all considered Intrusion Detection/ Penetration Systems. However, each of these three tools functioned differently and pulled different data.

Every tool had its own job, though several tools shared similar jobs. The tool summary lists all of the tools and gives a brief description about those tools. As shown in that document, some tools have a complex job, while others are very simple. The tool summary also includes notes about the primary function areas of IT, as well as a technical contact list for each tool.

There is no single written source of information about the tools at ORNL. All of the information for this project had to come from the administrators themselves. This spread into data management as well. However, research into managing data was supported with online research on the topic.

b. Research in Data Management

A wide variety of data can be produced by any security system. ORNL is no different as every tool, security or not, produces some sort of data. Non-security tools such as eProp can tell what inventory ORNL has, where it is located, who is the owner of

DRAFT

that property, and other important information. Security related tools do the same thing. Cyber Security Reports (CSR) creates reports that have a wide variety of information that managers and department heads need to know about their group in terms of computer security. The main question is then, what is being done with the data that is being produced by these tools?

According to Roger Wolter and Kirk Haselden of the Microsoft Corporation, "There are essentially five types of data in corporations: unstructured, transactional, metadata, hierarchical, and master [3]". The security tools produce metadata, which is simply data about other data. In other words, ORNL security tools pulls data about systems and organizes that data into organized and readable formats.

Data at ORNL is often viewed in online reports. For example, the Device Exception System (DES) can produce a report that shows the exceptions for a certain asset. The data at ORNL is often stored this way, and looked up when needed. It is not often exported into a regular file format such as Word or a PDF because the data within that report can change frequently, making the report invalid soon after being created.

However, while most security data is not exported into external formats, it used by other tools to help them create their reports. CSR pulls data from multiple tools, such as NetReg, DES, and VSWeb, and compiles that data from those tools into one report. Many of the security (and non-security) tools converse between each other, sending data back and forth between them. Tools pull data from other tools so that they do not have to use processing power to gather data that is already available. Also, having fewer sets of the same data means fewer problems and errors.

c. RIFIS

The goal of creating an internal risk score was accomplished in this project. The Risk Index for Internal Systems, otherwise called RIFIS, is a scoring system that pulls data already gathered by other tools. This scoring system is only in the beginning development stage, meaning tests of the scoring system have been done by hand. Below is the first tested scoring system used to determine the risk of several test machines:

1. Vulnerabilities
    - From: Tenable SC *Adds per vulnerability
    - 1pt for a mild vulnerability

    - 2pts for a moderate vulnerability
    - 3pts for a high/critical vulnerability
2. Asset Status
    - From: CSR
    - Orange Status: 5pts
    - Red Status: 25pts
3. Asset Data Sensitivity Level
    - From: RiskVision
    - Low sensitive data: 5pts
    - Moderate sensitive data: 15pts
4. External, Inbound Firewall Rules
    - From: SSR
    - 25pts (total, not multiplied)
5. Security Alerts
    - From: SourceFire and Bro
    - 5pts (x number of alerts)
6. Anti-Virus
    - From: ePO
    - 5pts (x number of flags)
7. VIP Status
    - From: RiskVision
    - 25pts if machine is VIP

See ***Figure 1***, ***Figure 2***, ***Figure 3***, and ***Figure 4*** for examples of the test runs of the scoring system.

It was decided that for the first scoring system, seven risk factors would be looked at. For factors that calculate points if the asset has a problem, a simple equation is set up. For factors that are a yes or no, the equation is set where 0 is no, while 1 is yes. Figure 1 was the score of the worst test machine, while Figure 2 was the best test machine.

For the first point, vulnerabilities, the original idea was to include the Common Vulnerability Scoring System (CVSS), which is included in Tenable's report of problems with scanned assets. As stated by first.org, the CVSS score is, "(a) rating system is designed to provide open and universally standard severity ratings of software vulnerabilities [4]". The CVSS score was to be pulled from Tenable Security Center (Tenable SC), squared to help quantify the number, and then multiplied by certain points depending on the severity of the vulnerability. Each individual vulnerability would go through this equation, then added together. The CVSS score is often given as a

DRAFT

number, resulting from an equation built into the system. In Tenable's case, it was discovered that vulnerabilities are given in terms of low, medium, high or critical, based on the CVSS score. Because the CVSS score was already built into the level of the vulnerability, it was decided to eliminate the CVSS score from the equation. This left the first equation to be the number of vulnerabilities per category (mild, moderate, or high/critical) multiplied by the number for that category (1pt, 2 pts., or 3 pts.), and then added together for a total.

The second factor was if the asset in question had a compliance problem in CSR. If an asset does not meet all ORNL rules/regulations, then it has a compliance error, and is listed in CSR with a color code. Orange assets have compliance issues that must be taken care of in 30 days, while red assets are critical and must be fixed immediately. The second point in the equation adds 5 points if the asset is orange and 25 points if it is red. An asset cannot be both, and it is possible to be neither orange nor red. Green is another code, but indicates compliance and therefore not built into the score.

Factor 3 adds points if an asset contains sensitive information, with there being two levels of sensitivity (low sensitive data and moderate sensitive data). No assets have critical sensitive data. Factor 4 adds 25 points to the total score if there are one or more inbound firewall rule exceptions for an asset. This number of points stays the same no matter if there is 1 exception or 10. Factor 5 is the number of alerts from SourceFire and Bro, which indicates how many times an asset has tried to be breached by outside attackers. The alerts were from a week time period, and the report had been run three days before. 5 points are added for every attack by different groups, but multiple attacks by the same attacker are considered to be only one instance. A single attacking agent can hit the same system 100 times, and counting every hit (even if by the same attacker) would badly skew the score and make it unbeneficial. Factor 6 gives points for every flag from the anti-virus system, ePO agent. These flags would indicate issues with an asset's anti-virus, such as viruses, or out of date software.

Factor 7 was calculated into the test score, with two systems being deemed VIP for testing, adding 25 points to their total score. However it was determined that the VIP status factor will be a future addition to RIFIS. At this time, ORNL does not have a list of assets that would be considered VIP.

DRAFT

The first test run of the score shows promising results. The scores appear to reflect the criticality of that particular asset. However, the test run is still being evaluated and the scoring system is still under consideration.

If implemented, RIFIS would be a valuable addition to ORNL's security teams. By creating a score to reveal at-risk assets within ORNL, instead of just external threats, the security teams can shift part of their focus onto taking care of and protecting those critical assets, so they cannot be exploited by outside threats. Covering and fixing the weak spots in a security system helps make the network as a whole stronger. After all, security can only be as strong as the weakest point in the defense against the outside world.

6. Recommendations

a. Recommendations towards security tools?

Currently, ORNL has a strong set of tools at its disposal. However, these tools may not be being utilized to their full potential. With the completion of this project, there are several points that should be made. The first point is that there is a lack of documentation and information about the tools used at ORNL. This lack of information is not exceptionally harmful to the operation of the security teams. However, the lack of documentation may make implementing new tools more difficult, and these tools may not fit into the current schema as well as they could, because information about how current tools work and what areas of data they cover is not readily available. When experts or administrators of tools leave, they take their knowledge of those tools with them, which only furthers the gap. Having a set of documentation can help any IT team at ORNL make better decisions when looking to renew current tool licenses or purchase new tools, no matter if the tools are for cyber security or not.

A second point is that not all of the current tools are being used at maximum efficiency. Bro for example, is installed on the network but its deployment is incomplete due to resource constraints. Some tools may be able to do more than they are currently being used for, which can save money and time. It may be better to have two tools that cover a large amount of area well then five tools that sort of cover the same area but do not talk to each other. It is recommended that current tools be reexamined for more efficient use both individually and within the data exchange field.

DRAFT

b. Recommendations towards data management?

Data management within ORNL is very effective, especially within the cyber security area. Data is pulled and reviewed to seek any areas of concern within the network. The only recommendation for this area would be to review for more efficient data flow between ORNL's security tools. There are many data connections, as indicated by the flowchart in ***Appendix A***. Some data connections are not used to their full benefit, while other connections are not efficient for running reports. A solution would be to have the tools feed into one database, such as a configuration management database (CMDB). This would help eliminate duplicate information being passed around, as well as making it more efficient to run reports on security concerns.

c. Recommendations towards RIFIS?

RIFIS is set to become a useful tool for ORNL security. At this time, if the first run testing is deemed successful, it is recommended that RIFIS be taken to the next step. That next step could be the building of code to run the equation, or the reevaluation of the suggested scoring equation to create a more accurate score for problem assets. As it stands, RIFIS is off to a strong start to become a useful tool in ORNL's arsenal against attackers.

A second recommendation for RIFIS is the compiling of a VIP list. VIP status would indicate an asset that is important to the functionality of ORNL or has access to important parts of ORNL's network, such as severs or sensitive data areas. A flag could be place in a security tool, such as RiskVision, to identify assets that are VIP. This is a future project that should be considered by ORNL security teams, as it would benefit security teams in determining criticality of an asset.

7. Conclusions

a. Security tools

The current tools cover a large area of data that resides at ORNL. It is important to note that even though some of these tools cover the same data, these tools do not always provide the same *information* about the data. By having that realization, it

DRAFT

allows for a new look at both the data that is being harvested and the tools being used to gather it.

b. Data management

The data for security analysis is invaluable. It provides a look into what is not only coming in from the outside, but what is going out into the world. Managing security data is only a part of security, but important none the less. It is a balancing act of reading the data, translating it into information, but at the same time, keeping an open mind and a thought to what is going on within the big picture.

c. *RIFIS*

With completion of this project, it is hoped that the risk index score becomes a defining feature of the security teams. Many corporations, ORNL included, have ways to combat and identify assailants from the outside cyber world. However, having an internal system that identifies assets that are at risk for attack is a positive feature.

d. Final Thoughts

The cyber world is constantly changing. New technologies are developed every day, and with that new technology comes new ways for invaders to infiltrate security networks and steal valuable data. ORNL's cyber security teams work every day to help prevent these attacks from breaching the defenses. Adaptability is essential, and ORNL is showing its ability to adapt to new threats. The tools that ORNL employs to combat these threats are a mixture of old and new, high-tech and simple code. They are the cyber security's backbone, and have allowed them to combat threats that threaten to wreak havoc against new research and government support. No system is perfect, and no security defense if fool-proof. However, as long as these tools are adapted and adjusted for their maximum benefit, the security teams at ORNL can continue to strive for the strongest defense against attackers they can provide.

8. Acknowledgements

There are many thanks to be given for the completion of this project. First would be to the mentors, Kevin Kerr and Tina Heath who helped support and encourage the

DRAFT

growth of the project and its direction. Matt Disney also receives thanks for recommendations on next steps and help with completion of the project. Thanks also go to the rest of ORNL's ITSD, for all of the staff members who gave up time to answer questions and explain how tools functioned. Finally, thanks go to Debbie McCoy and the RAMS internship for the opportunity to work at Oak Ridge National Laboratory.

9. References

[1] NIST. (2007). *National Vulnerably Database Common Vulnerability Scoring System* . Retrieved from http://nvd.nist.gov/cvss.cfm?version=2

[2] McDowell, Mindi & Householder, Allen. (2009, May 6). *Why is Cyber Security a Problem?*. Retrieved from http://www.us-cert.gov/cas/tips/ST04-001.html

[3] Roger Wolter, & Haselden Kirk (2006, November). *The What, Why, and How of Master Data Management*. Retrieved from http://msdn.microsoft.com/en-us/library/bb190163.aspx

[4] *Introduction to CVSS*. (n.d.). Retrieved from http://www.first.org/cvss/intro

DRAFT

Name	Asset 1	Points
1. Vulnerabilites		
Mild	0	0
Medium	0	0
High/Critical	0	0
2. Asset Status		
Orange?	0	0
Red?	0	0
3. Sensitivity		
Low	0	0
Moderate	0	0
4. Firewall Rules		
Rules?	0	0
5. Alerts		
Number of alerts	0	0
6. Anti-Virus		
Number of flags	0	0
7. VIP Status		
VIP?	0	0
		0

Figure 1 – 1 of 4 tested assets. This is a behind-the-firewall desktop that kept up to date on patches.

Name	Asset 2	Points
1. Vulnerabilites		
Mild	2	2
Medium	11	22
High/Critical	1	3
2. Asset Status		
Orange?	0	0
Red?	0	0
3. Sensitivity		
Low	0	0
Moderate	0	0
4. Firewall Rules		
Rules?	1	25
5. Alerts		
Number of alerts	2	10
6. Anti-Virus		
Number of flags	0	0
7. VIP Status		
VIP?	1	25
		87

Figure 2 – 1 of 4 tested assets. This asset is a sever that sits on the network. It has some concerns that make it a possibly vulnerable system.

Name	Asset 3	Points
1. Vulnerabilites		
Mild	0	0
Medium	0	0
High/Critical	0	0
2. Asset Status		
Orange?	1	5
Red?	0	0
3. Sensitivity		
Low	0	0
Moderate	0	0
4. Firewall Rules		
Rules?	1	25
5. Alerts		
Number of alerts	30	150
6. Anti-Virus		
Number of flags	0	0
7. VIP Status		
VIP?	1	25
		205

Figure 3 - 1 of 4 tested assets. This asset is a sever that sits on the network. It has more concerns that make it a more vulnerable system than asset 2.

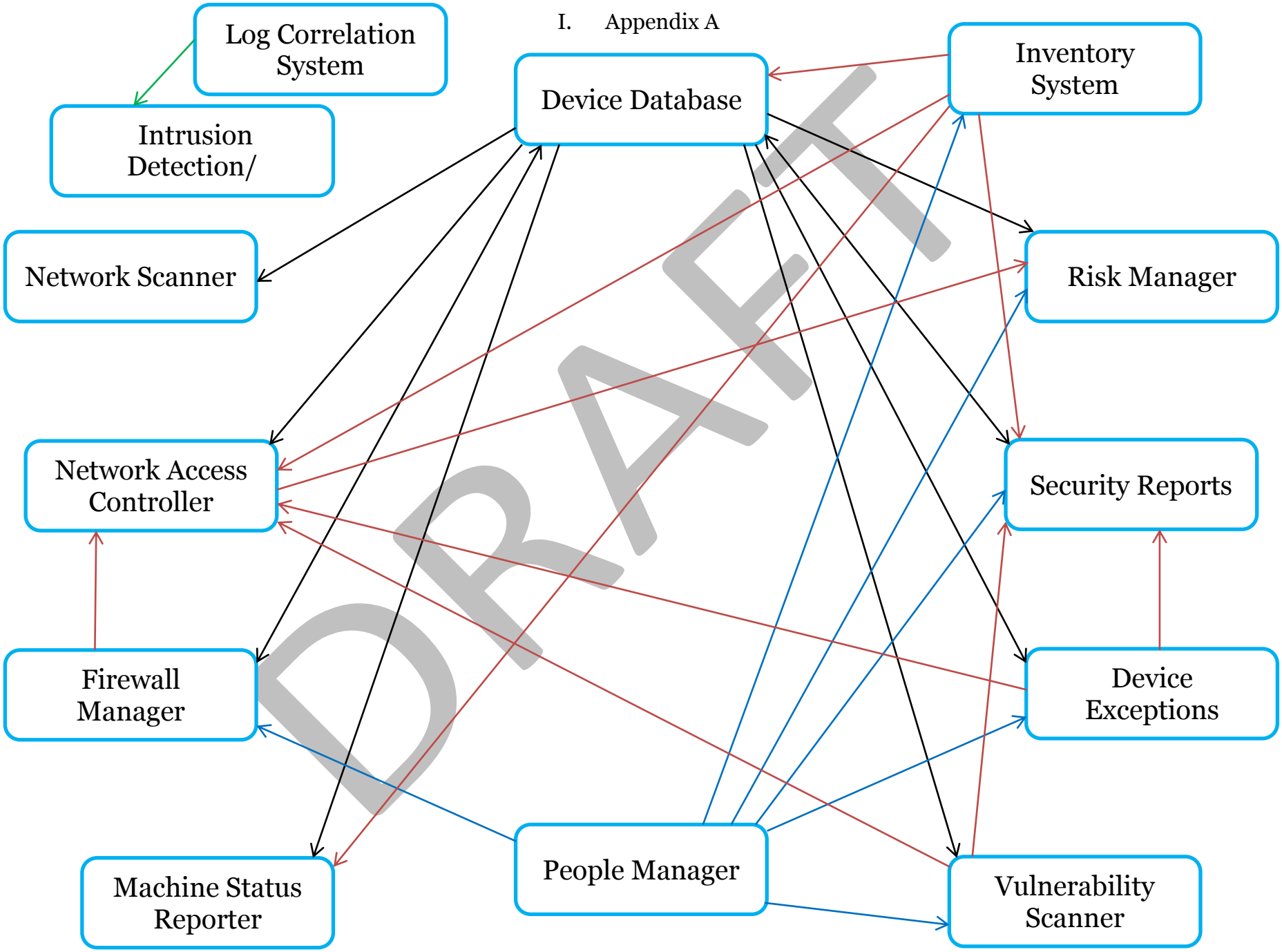
DRAFT

Name	Asset 4	Points
1. Vulnerabilites		
Mild	0	0
Medium	47	94
High/Critical	205	615
2. Asset Status		
Orange?	1	5
Red?	0	0
3. Sensitivity		
Low	0	0
Moderate	0	0
4. Firewall Rules		
Rules?	0	0
5. Alerts		
Number of alerts	0	0
6. Anti-Virus		
Number of flags	0	0
7. VIP Status		
VIP?	0	0
		714

Figure 4 - 1 of 4 tested assets. This is a server that is considered high risk due to its high score. As shown by the score, this sever has many vulnerabilities making it the most critical of the four assets tested.

DRAFT

I. Appendix A



DRAFT

II. Appendix B

From	To	Data being transferred
Tool A (Device Database)	Tool B (Machine Status Reporter)	▪ Device Name ▪ IP Address ▪ Location ▪ Mac Address ▪ Operation System (OS)
Tool A (Device Database)	Tool D (Network Access Controller)	▪ Device Type ▪ IP Address ▪ Mac Address ▪ Owner Information ▪ Router
Tool A (Device Database)	Tool E (Risk Manager)	▪ Alert Flags ▪ Device Type ▪ IP Address ▪ Mac Address ▪ Owner Information
Tool C (People Manager)	Tool D (Network Access Controller)	▪ Department Name ▪ Group Name ▪ Owner Contact ▪ Owner Location ▪ Owner Name/ID
Tool C (People Manager)	Tool E (Risk Manager)	▪ Department Name ▪ Owner Contact ▪ Owner Devices ▪ Owner Location ▪ Owner Name/ID
Tool D (Network Access Controller)	Tool E (Risk Manager)	▪ IP Address ▪ Mac Address ▪ Network Exceptions ▪ Network Location ▪ Time Stamps

DRAFT