Network Security

Southern Utah University

Internship CSIS 4890

Professor Rob Robertson

04/18/2013

By

Alexander Cannell

Network Security – Internship

            I started my internship when I heard about the position with Mark Walton from Ethan Kleinman.  Ethan had rejected the job offer with Southern Utah University Information Department because the internship wasn’t a paid internship.  He was disappointed that he wasn’t accepting the internship with the campus, but he needed a paying position to  financially support himself.   My ears perked up at that point because I was looking for an internship not for the money (even though the money would be nice) but for the experience. I decided at that moment to email Mark Walton, who is over the Network Security Department at Southern Utah University Information Technology Department. I got an interview, then the internship. Rob and a lot of other professionals have told me, “the best thing for someone going into the technical field is to get as much experience as you can.” So, taking this advice into account needless to say I was very excited to accept a non-paid internship.

             I started my internship very fast, what I mean by this is my first day we started right off the bat. He asked me about flows and what they were; I realized quickly that I didn’t know as much as I thought I did about networks. I took a guess about what flows were, and guessed wrong looking stupid in the process. A great thing I learned from this experience is that it is okay to say “I don’t know what flows are”; Information Technology professionals can tell if you don’t know what you are talking about. Don’t try to act smart and try to guess what things are but ask, and by saying, “I don’t know,” won’t bring criticism but explanation.

           Mark started me with finding out what flows were. Flows or Traffic Flows is a term to describe a sequence of packets from a source node to a destination node, which may be another host, multicast group, or broadcast domain. In other words flows are conversations on a network.  Flows can contain a wide variety of information about the traffic more specifically Simple Network Management Protocol (SNMP), Interfaces, Timestamps, Number of Bytes, Number of Packets Observed, TCP and UDP Flows, Flags, and Layer Three Operations. What I mean by Layer Three Operations is layer three headers which include source and destination IP addresses, Internet Control Message Protocol (ICMP), Internet Protocols (IP), Type of Service Value, and Source and Destination Port Numbers and Types.

There are many different types of Network Flows such as NetFlow, sFlow, and jFlows. The type of flow I’m going to concentrate on is NetFlows. The reason being NetFlow is a Cisco technology, Southern Utah University uses Cisco routers. Anyways, after I was quizzed by Mark about what flows were. I was tasked with becoming an expert with a NetFlow analyzer called Scrutinizer. A NetFlow analyzer is a web based traffic analysis tool that provides detailed reports on the network traffic.

The NetFlow analyzer Scrutinizer is developed by a company called Plixer. Scrutinizer can recognize and look at breach attempts like Brute Force Attacks, Distributed Denial of Service (DDoS) Attack, Intrusive Scans, Domain Name System (DNS) Violations, ICMP Destination Unreachable, and Host Reputation Look-ups.  A Brute Force Attack is an attack where you are basically testing a lot of different passwords to try to guess the correct password. Distributed Denial of Service is where a lot of computers send request packets to a target server to leave it weak and shut it down. An example of Distributed Denial of Service is a BOTNET. Domain Name System Violations are when there is extreme number of DNS queries. ICMP Destination Unreachable is when a message that comes back from the router saying it doesn’t have a route to the destination on the network to go. Host Reputation Look-ups are programs and automatically go out to the internet, downloads, and updates programs. Some Intrusive scan examples FIN, SYN, TCP, UDP, Windows, and ACK Scans.

C:\Users\SUU\Desktop\Untitled picture.pngFigure 1: This show the information on a certain attack this one is a violation of IP protocols with an interface of 168 the violators port and ip address is displayed here too. This also shows the directory of where the violation record is stored.

Scrutinizer can do some cool things like Scrutinizer Mapping, Network Based Application Recognition (NBAR), and Simple Mail Transfer Protocol (SMTP) Mailizer. These are all add-on’s for Scrutinizer. Scrutinizer Mapping allows you to create a graphical representation of your network and its flows, mapping can also link up with Google Maps and show the flows in your Wide Area Network (WAN). A funny thing that happened when I tried to use the Google Map feature on Scrutinizer was when I plugged in the three main routers GW-CC, GW-ELC, and GW-SW, Google Map showed them just off the coast of Africa. When I saw where the three routers were situated on planet earth I asked Mark, “When did you move the routers off the coast of Africa?” He was stumped by this question until I showed him the routers. Network Based Application Recognition is an awesome application that can recognize and track non-critical applications including gaming, file sharing, social media, and etc. NBAR can also be used to prioritizing, policing, and block applications as needed. For example: you are able to see the amount of bandwidth that is utilized for FaceBook.com. Simple Mail Transfer Protocol Mailizer enables you to be alerted to the Scrutinizer when needed. Mailizer enables an administrator to keep an eye on Scrutinizer without watching Scrutinizer constantly. For example: an Distributed Denial of Service attack occurs, ideally the administrator of the network would need to be alerted about the attack; Mailizer will then send an email about the attack to the administrator to be acted upon. I really would have liked these functions if I could get them to work on the Flows serverFigure 2: Flow Expert Showing the top NetFlows and the threats overview. Just an overview of all the main flows and threats.

Mark Walton, Jerry Carpenter, David Barlow, and I examined Scrutinizer and determined that the current version of Scrutinizer was not user friendly at all. There is two variables called Interfaces and Instances, which we could not for the life of us, find out what they do or what they mean. I could decipher that Interfaces and Instances are curtain events that happened on the network. Each Interface and Instance has a corresponding number with it categorizing an event that happened. The problem is that Plixer doesn’t have any type of dictionary, index, or glossary that describes what the Interface and Instance number is.  I had a problem also with editing maps, getting email alerts to work, NBAR to work, and understanding the general information. The things I liked about Scrutinizer are the ability to see the top bandwidth, top countries, top alerts, and top ports being used. I worked on Scrutinizer on and off for almost three months. I also liked being able to use other programs and websites to find the locations of IP addresses that were not private. I have to admit that I didn’t know that a 172.16.X.X addresses are private addresses, which was cool to learn by using Scrutinizer.

After working on Scrutinizer for so long and seeing me stuck, Mark decided to scrap the $2,000.00  program and go to some open source NetFlow Analyzers. The Analyzers I used was Ground Works, OSSIM, NFSEN, and we were about to try out NTOP. Finding a NetFlow Analyzer perfect for Southern Utah University has been my ongoing project for me I have yet to narrow down a program that would work for Southern Utah University. Through the process of finding the perfect NetFlow Analyzer I was able to use many different programs, and operating systems, and configurations to get this NetFlow Analyzer to work. I had very little experience working with Linux, Unix, and Ubuntu Servers, but installing these NetFlow Analyzers has given me a lot of troubleshooting skills especially working with the NetFlow analyzer Linux. This includes Linux command line commands, installing packets, setting up an eth0 and ls network connection, working with VMware, and just trouble shooting. We had a lot of troubles with VMware from the virtual CD Drive not disconnecting to the whole InfoSec2 server going down (Very Frustrating).

I have found that Mark’s saying, “Google is your best friend, in this career choice” to be so true. I used Google constantly for trouble shooting. The thing that took up most of my time was research. I researched a lot of stuff for Mark, but mostly NetFlow information. Google would have to be the greatest tool I used while doing research.

I quite enjoyed working and interacting with the other members of the Information Technology Department. The person I interacted with most from the Information Technology Department would have to have been Jerry Carpenter and his intern David Barlow (who is in CSIS 4700 with me). I had the pleasure of working with Jerry and David on NetFlows, Subnets, VLANS, Ports, Router Information, Diagramming, and etc. I don’t know what they think but I feel I developed a close working friendship with these guys and Mark too. My father is a manager over a Respiratory Therapy Department so he has the first and last say on who they hire for his department. My father has always emphasized the point that he will not hire someone that doesn’t work well with others, a person is at a disadvantage if they can’t deal with people. I have found working with Mark Walton, Jerry Carpenter, and David Barlow has been a great experience.  The road to my chosen career has become clearer while working alongside these guys. For that reason it was worth it alone to have done this Network Security Internship. I always felt comfortable to ask Mark, Jerry, and even David questions about the current problem or troubleshooting I was having problems with (when Google was no help). I do have to admit at the beginning of my internship I wasn’t as comfortable with asking questions as I should have been. I didn’t become comfortable with asking questions until I was working with Scrutinizer; I got so fed up with trying to figure out the most simplistic tasks on Scrutinizer. I went to Mark and explained my situation and he was very understanding and said we will give it to David and Jerry to work with in the meantime research new NetFlow analyzers. Two days later Jerry and David came in and said we are scrapping Scrutinizer, I learned if I only explained my situation sooner it would have saved me a whole lot of time, but I did learn a lot about Scrutinizer (that it is not user friendly) all the same. What I found surprising was Mark worked with a lot of incidence with students using the Southern Utah University network impropriety. I can think of three cases where he asked me to leave because he was going to talk to students about their miss conduct.  I unfortunately didn’t hear any of the interviews or what they did, and I think I had the common sense not to ask.

Another thing I was able to help write and research an Incident Security Response for the Information Technology Department. An Information Security Response sometimes referred to as an “Incident”; “is any activity that harms or represents a serious threat to the whole or part of Southern Utah University computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. Routine detection and remediation of a ‘virus,’ ‘malware’ or similar issue that has little impact on the day-to-day business of the University is not considered an Incident under this policy.” (SANS, 2011) While doing the research, I learned that most Universities Incident Policies were along the same guide lines that SANS (System Administrator, Audit, Networking, and Security) put out.  Each policy consisted of Communicating the Incident, Containing the Damage and then Minimizing the risk, Identifying the type and severity of the compromise, Protecting Evidence, Notifying External Agencies, Recovering Systems, Assessing Incident Damage and Cost, and Reviewing the Response and Updating Policies. What I found interesting was none too little of these plans left out an obvious final part to the Incident Policy, which is what you did to fix the problem and what you learned from the incident. I don’t know about you but I feel understanding and how you fixed a problem is a very important part to an incident report. While the Incident Report is very important I think that rating the severity of the Incident is important. Say that you have many Incidents happening at once I would be very hard to tackle them all at the same time that is why we set a severity priority. So if you do have multiple situations that require your attention, you can set higher and lower priorities to these incidents.

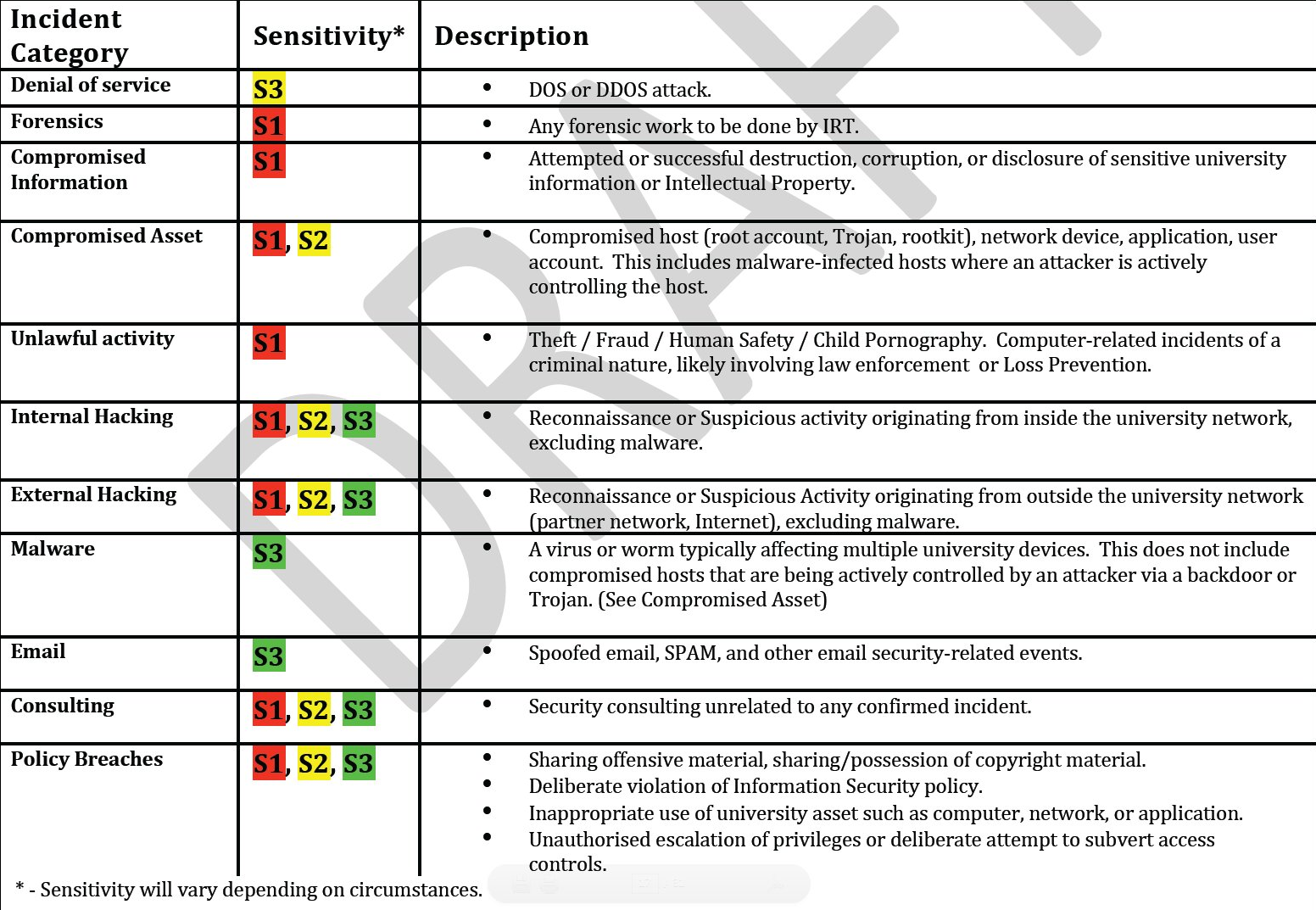
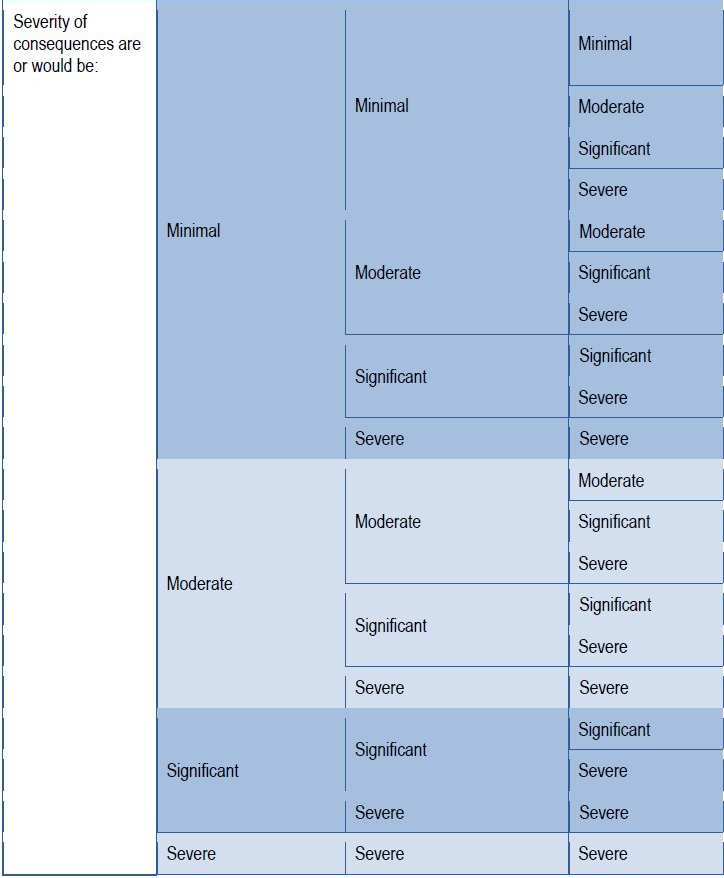


Figure : From the Department of Defense, showing an Severity examples minimal, moderate, significant, and severe.

I was also able to use a program called DIA Diagrams which is an open source diagramming software to Diagram Southern Utah University VLAN layout for Mark and Jerry. Diagramming was the greatest part of my experience/internship I would have to say, I got to get away from research and work with a new program. I got to work with understanding Southern Utah University subnet, VLAN’s, and the layout of the network. This project took me about a month to do fully, mostly because of the miss communication between Mark and I.

I feel the most important thing I learned in working in the Information Technology Department is that good communication is the key to problem solving. When doing research/trouble shooting it is very important to input into your favorite search engine (Google) the problem you need to be fixed. I was implementing a new NetFlow analyzer called Nfsen I got everything downloaded, Nfdump installed, and during the process of installing Nfsen I received an $Path linux error because you don’t have the right packages installed on your computer like Flex and Lex. Explaining your problem to Google is very important to finding a solution to a problem. Communication is especially important when trying to explain your problem to your fellow coworkers to get their help. I remember a time when I was having a problem with one of my Ubuntu Servers and I couldn’t explain my problem to Ed and Mark I ended up leaving Marks office looking stupid.

I enjoyed working with Mark, David, and Ed in the Network Security Department, I learned a lot that I can apply to my future career path. Plus I got an awesome tee shirt at the end of it all. If I could continue working there as an intern I would, but they don’t have any funding (He did say check back with him in July here is hoping).

CITED WORKS:

- Plixer, . N.p.. Web. 25 Apr 2013. <http://www.plixer.com/Scrutinizer-Netflow-Sflow/scrutinizer.html>.

- Wright, Craig. "The Incident Handlers Handbook." *www.sans.org*. SANS, 12 5 2011. Web. 25 Apr 2013. <http://www.sans.org/reading\_room/whitepapers/incident/incident-handlers-handbook\_33901>.

- Stikvoort, Don, and Georgia Killcrece. "CSIRTS.com." . CSIRT, 04 04 2003. Web. 25 Apr 2013. <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CEEQFjAA&url=http://www.cert.org/archive/pdf/csirt-handbook.pdf&ei=yAR6UZvEO8XTqwHxkoG4CA&usg=AFQjCNHMFuppljOQx4yIdakFewA0uLrJ\_w&sig2=mfivM1\_AmKDqBWDAv4fv-Q&bvm=bv.45645796,d.aWM>.