June 07

There is something clearly going on with Max. It isn't often that a Dauntless leader spends so much time with someone from another faction, let alone the leader of the Erudite faction. He and Jeanine Matthews are always conversing over his computer. The Erudite developed the simulation serums that we use in our fear landscapes so I have a hunch this might have something to do with it. Max has also ordered Gus, my supervisor in the control room, to set aside video footage of all simulations. There is something afoot and I have to find a way to figure out what it is.

This is a dangerous path to take. If something happens to me, I must be able to let the others know what I've found. Keeping a diary has really helped me organize and track what I've done, but if these entries were to fall into the wrong hands, I'll likely end up being the next body they fish out of the chasm. Fortunately, the Dauntless have little patience in learning the ways of the Erudite. As part of control room training, I've come across a trove of secret message encoding techniques that are often used by the Erudite to secure their communications and computing systems. By applying them to my diary entries, no one in Dauntless will be able to decode them. Or perhaps, no one in Dauntless who isn't also Divergent. There is something different about Tris Prior. I had to delete her simulation results after she was able to manipulate the fear landscape in order to escape. If she is Divergent, I have a feeling she might find a way to learn how to break these codes.

Getting back to Max, having access to the Dauntless control room is quite useful. From there, one can access the hundreds of cameras that we use to monitor activity throughout the compound. There is even one in Max's office pointed at his computer. I think I have a pretty good idea how to get access to Max's computer to see what he's been up to. I'll need to do a little....

H E D S U L R O N R S U G F I

Fortunately, Max never learned how to touch type. He, like most other Dauntless, has spent his days at the shooting range, not the keyboard. This makes capturing his keystrokes easier. Scanning through multiple video replays of his login sessions, it appears that his password is 084628, although from the video it was difficult to see much below the top row of the keyboard. Even knowing his password, though, I can't just walk up to his computer and poke around. I need a way to access it remotely. Being a bit paranoid, Max has locked his computer down pretty tightly, making it difficult for outsiders to break into it. I believe I'll need to find a way to install some backdoor software on Max's computer so that I can access his computer from the safety of the control room. Visiting Day is only several days from now. Max will be out all day long attending to the initiates and their families in the Pit. That will be my best chance to get onto his system undetected. I have to quickly put together everything I need to compromise his machine. I've heard of a software tool that they once used called the swiss army knife of TCP/IP. It was often used to implement remote backdoors on systems. I will pwn Max's computer with:

T T C E N A

June 09

Getting a backdoor on Max's computer is one thing, but I'll also need to be able to copy the contents from the computer periodically. This might be difficult. If Max is working with the Erudite, he must be using their tools to detect and prevent data exfiltration. I have to make sure whatever I put on Max's computer is able to get the data across the network without alarms going off. In our control room training, we were given a set of security tools the Erudite recommended we install on our computer systems. They favored a lightweight, open-source, intrusion detection and prevention system that could perform real-time traffic analysis. As soon as the software sees an anomalous connection that matches one of its rules, it alerts the network administrator. It is highly likely that the tool defending Max's machine and the tool I'll need to find a way to bypass is:

T O S R N

June 10

Poking around the Dauntless systems it looks like they are set up to detect and prevent data leakages using deep packet inspection (DPI). Before the wars, the Erudite believed two researchers named Dyer and Shrimpton at Portland State University had managed to easily bypass DPI systems by combining encryption with steganography. They banned the technology and tried to eliminate any traces from historical record. Apparently, the software PSU developed had great success bypassing the Great Firewall of China many generations ago. I've managed to discover the system floating around in the underground forums. It looks like the software encodes data into normal messages so that the DPI system believes it to be innocuous. It's sort of like steganography, but applied to network protocols. Eric Schmidt, the chairman of Google at the time, apparently liked it quite a bit. The software they used was called:

P T F Y R O X E

Only a couple of days before Visiting Day now. There's not much more time to develop this payload. I'll need to make sure these next days count.

I definitely don't want to put all my eggs in one software basket. Since I'll likely only have one chance to install all the software I need on Max's computer, whatever I do install needs to count. The Erudite have referred to an approach they used in the past to protect computer systems called ``Defense-in-Depth''. The idea is that one never relies on just a single technology to guarantee the security of their systems. I'll likely need to take an ``Offense-in-Depth'' approach to make sure I have enough things installed on Max's computer to do the job. I've heard of another tool that people use to bypass intrusion prevention systems and move data off of target systems. It's a tool that a company called Rapid7developed which supports data exfiltration using an ICMP module. Their software is called:

M S P T E O T L A I

Tomorrow is Visiting Day. I'll have to go with this flash drive and hope that the password and software work.

June 12

What a relief. I think I managed to pull it off, but I may have aroused some suspicions. While Gus and the others were taking a break, I pulled the video feed from Max's office out of the rotation so it wouldn't appear on their screens. I slipped out of the control room and into the Pire, which was mostly empty as most everyone was out in the Pit. Reaching Max's office, I entered the password. A jolt of nervous energy went down my spine as the screen shifted, before beginning the login session. Whew! The password worked. I inserted the flash drive and installed its contents onto Max's computer before quickly slipping back out of his office. I thought I was home free until I got back to the control room and found Gus standing in front of my computer. Not knowing how much he saw, but seeing that he was clearly upset, I stalled before making up a story of going off to investigate something peculiar I thought I saw happening in Max's office. It seemed to work, but I'm sure it aroused Gus's suspicions. He'll likely be watching me closely from now on. I'll need to be more careful, especially in the control room. As a safeguard, I need to make sure that the systems don't record all of the hours that I'll be spending in the control room remotely sifting through and copying the content off of Max's computer. Long hours logged on any one account might catch Gus's attention. I know just what to do. There is a trick that hackers used in the past to poison reputation systems in peer-to-peer networks. They would forge multiple identities to hide the fact that all of the access was coming from a single source. I'll need to forge some identitiesof my own by creating some fake accounts or:

B S S L I Y

June 13

Creating several fake accounts and rotating through them will hopefully keep my activity under the radar. Still, I don't want to directly access Max's machine from the machine that I'm on. If he checked the network logs, he'd see traffic coming from my machine and if he looked at the video feed of the control room, he'd see I was in front of it. That would make it too easy to trace things back to me. In the past, network intruders would take great pains to hide their identity. In one of their methods, attacking commands were sent indirectly to the victim through a chain of compromised hosts. I will likely want to bounce my access over a number of Dauntless machines before entering Max's system in order to disguise the fact that the computer I'm using is the true source. I'll need to connect through a series of:

E P S T N G P I S S N E T O

Sending my connections through a maze of other computers will make it difficult for Max to trace the connections I make to his computer back to me. Still, I want to be careful and it would be ideal if all traces of my activity were removed after each session is over. There is a stealthy type of software that has been used to hide the existence of processes, programs, and files from normal methods of detection. One of the features of such software is the ability for network intruders to remove their log entries. The kind of software I need is called a:

I R K O T O T

Things can get tricky when deleting log entries. A famed hacker called Kevin Mitnick was detected using this method when he accessed a machine where the log files were e-mailed to the system administrator on every login event. When a subsequent log file came back smaller than a previous one, it exposed his access. I will need to disable this if it is being employed.

June 15

From the comfort of the control room, I've begun rifling through the contents of Max's computer. I have to be judicious as to what files I copy over in order to make sure I don't exceed any bandwidth caps that might trigger alerts from the intrusion detection system. So, I will use the backdoor to navigate Max's file system and then use the data exfiltration tools to transfer interesting files back to my computer. The digging was slow today. Most of the files on Max's computer were benign, mostly lists of members and schedules of events. Not knowing what I'm exactly looking for makes it necessary for me to manually go through each file. Towards the end of the day, however, I find a folder that lists supplies. Instead of supplies for food or clothing, however, it is for weapons. In the folder is a file named "Serum D2.AES". When I try opening the file, it gives back random data, which is a hallmark of data that is either encrypted or compressed. The file extension seems to give away the fact that it has been encrypted with AES. AES, or the advanced encryption standard,was once thought to be the strongest method for encrypting files. It supports several different ways to encrypt data each with varying security properties. One of the ways good block ciphers resist attacks is to chain the output of encrypting one block of plaintext into the input of the encryption of the next block of plaintext. In researching AES, it appears that there are insecure ways of using it that make its encryption trivial to break. It seems that I might be able to break the encryption on this file if it was done using:

B C E O D E M

June 16

In looking at the encrypted blocks, it does look like there are several repeating ciphertexts. This should never happen if the encryption scheme was done using proper cipher-block chaining. Unfortunately, time is of the essence and I may not have enough time to break the vulnerable encryption scheme. Perhaps there is an easier way of decrypting this file. Max likely knows the key to decrypt the file and the Dauntless don't exactly have a knack for memorizing passwords like the Erudite. It's highly likely that he used a simple key to encrypt the contents of the file. Perhaps I'll try a:

Y T A I O C I N R D T K C T A A

June 17

Pretty funny. I can't believe Max used `brownies' as his encryption key. I should've known. Dauntless brownies are legendary and Max is well-known for his penchant for them. The file, on the other hand, is chilling. In the file are the specific ingredients and quantities needed to produce thousands of doses of this mysterious D2 serum. Why would someone need so many doses? Initiation is when we use most of our simulation serum and the number of initiates is nowhere near this many.

I decided to do a bit more digging. The fact that Max took the time to encrypt this file instead of the entire file system just made the task a whole lot easier. Now, rather than sifting through all of the files on his system, I can just search for those that look like they consist of random data or that have the AES file extension. Those are probably the ones deemed important enough to hide from prying eyes. I found one such encrypted file in a sister folder to the serum file that is quite large. Using Max's key, the file decrypted into a map of the city marked with letters and numbers. Cross-referencing it to a Dauntless location database, I'm floored as it shows that the locations all fall in the area belonging to the Abnegation faction: the faction all of us have entrusted to govern the city.

This has the makings of a coup organized by the Dauntless and Erudite leadership to overthrow the Abnegation. Checking the modification date on the map file, it looks like it was modified just in the last day. The plans are imminent. I think I'll need to know exactly what's going on in real-time from now on. There is a program that is installed on all of our computers, including Max's, that might help me monitor what is going on. It is an open-source network packet and protocol analyzer that can be used to read live data being sent over the network. If I launch this software on Max's computer, I might be able to capture the plans as they are making them. The tool that I'll be using is:

K A S I R H W E R

June 18

I've been caught. They cut off Max's computer from the network and it looks like they have discovered all of the software I placed on it. I knew something was up when a whole crew of Erudite showed up. I recognized one of them as Caleb, Tris's brother. Tris mentioned that Caleb was particularly good with computers.

How much do they know? Can they trace it back to me? I can't stop thinking about all of the traces I might have left on Max's machine that they could use to find their way back to my computer. Thinking back to all of the different machines I used before reaching Max's, I quickly scramble to remove any trace of activity from the log files of those machines. Being up against the Erudite, I can't be too sure they won't find something that I've left behind and identify me as the intruder.

How did they figure it out? Replaying all of yesterday's events in my head, it finally dawns on me. The program that I was using to try and capture network traffic must have set off the alarms. Careless. The program worked exactly as I had expected, but perhaps I should have checked more carefully to make sure that the program was authentic and not a fake program or:

J R A N T O

June 19

The Erudite boxed up Max's computer and took it with them. I'm guessing they no longer trust him to keep their plans safe. I can't help but wonder if they know that I was able to decrypt the files on it and if so, whether they will now try to change their plans. One thing for sure is that I'll need to be a lot more clever to uncover what is going on now.

The computer the Erudite left behind for Max looks like one of those thin client computers. Thin clients have a minimal amount of software installed and instead, rely upon being connected to the network in order to run. I will need to find a way to compromise this new machine if Iwant to get to the bottom of this plan. The operating system Max's machine runs is basically the Linux OS with almost all of the applications stripped out of it. In its place, a single application has been added back: a web browser. This is a common security technique in which security is increased by reducing the software surface area available to attack. It seemed to have worked. As I began digging around for information on this particular system, it was one that managed to survive a bug-hunting competition called Pwnium one year unscathed.

With a minimal amount of programs installed, I will need to be clever. In addition, this system blocks arbitrary applications from being installed and executed on it, thus eliminating my previous avenue for attack. To get at these plans, I will need to be able to find a way to exploit a computer running the operating system:

O U M M R H C I

or perhaps the person using it....

June 20

As a result of my hacking being discovered, it appears that Max's new computer has been set up to prevent him from saving any sensitive information locally. It looks like all of his sessions on his computer are via a web browser that he uses to login to the Erudite systems. The last thing I did on Max's machine before being caught was capture all of the network traffic that occurred for the day on his machine. It looks like Max was accessing several different Erudite systems in order to download updated plans and to communicate with Jeanine. I find one site that he appears to log into everytime. This must be an Erudite server.

I have Max's credentials from his old machine that I could potentially use to try and log into the Erudite system, but I am wary of getting caught. It's one thing to hack into Max's machine as he was quite the luddite, it's another to try and log into Erudite systems knowing that the Erudite are much more adept at computer security and network forensics. I have heard in the past that people used something called Tor to bounce their requests around the web in order to maintain their anonymity. This sounds similar to what I had employed in compromising Max's computer. Since Tor was so prevalently used before, it's likely the Erudite have spent a lot of time and effort attacking it. I've found an older, more obscure, anonymizing web proxy that might fly under the Erudite radar and keep me hidden. This particular one dates back to 1997 and protects your privacy and data for free. I will try logging into the Erudite system after setting up my web browser to use the web proxy at:

E N S O O A Y N U M

June 21

After setting up access to the anonymizing service, I tried using Max's 084628 password to log into one of the Erudite web servers I found in the packet trace. It didn't work. Either Max changed his password after my software was discovered or he used a different one for his account on the Erudite system. Either way, I need to find a way to get his login credentials. Going back to the control room, I bring up the video feed of Max's office while no one is watching. Perhaps I can find his credentials by inspecting video footage. To my dismay, it appears that Max has become much more paranoid about how he enters in his credentials. He now sidles up closely to the keyboard as he logs in.

There must be another way to get his login information. I do a bit of research and discover a popular method that was used to acquire usernames, passwords, and credit card details in the past by masquerading as a trustworthy entity in an electronic communication. Perhaps if I can lure Max into entering in his credentials in a site I control, I'll be able to grab his credentials. I just have to do a bit of:

I H N P G S I H

I send Max a luring e-mail that appears to come from Erudite administrators telling him that his quota has been exceeded and that he needs to login to increase it. The e-mail has a link to a web server I temporarily bring up on a control room computer. While some people have been trained to avoid clicking on links in e-mail messages and instead type in URLs manually when visiting critical websites such as banking ones, I don't think Max has the awareness not to. If he does click on the link, it will direct him to my bogus website which I've made to look exactly like the Erudite login page he is expecting. Once he submits his credentials, I'll just pull them out of the logfile and I'm good to go.

After sending the message, I lie in wait in the control room for Max to get back to his office. After about an hour of waiting, I see Max enter his office and go to his computer. Looking over at Gus, he has fallen asleep at his station and is hunched to one side drooling all over himself. I should have no problem observing Max without being caught. While I still can't see what he is typing, I can make out the windows he has on his computer screen. He brings up his e-mail and clicks on a message. It launches a browser window that brings up what appears to be an Erudite login page. Could it be the bogus one I've included in my e-mail? Max pauses, closes the window, and clicks on the message again. Again, the login page appears, but Max makes no attempt to login. Instead, he leans back in his chair for a moment, grunts, and then closes the window again. I pull up the log files on the bogus site I've set up and, sure enough, Max is bringing up the fake site I created. Something is keeping him from logging in. The attack isn't working. Instead, Max launches a new browser window and clicks on a bookmark. It sends him to a page that again looks like the Erudite login page. This time, though, a window pops up on his computer asking him whether or not he'd like to login to the site with a saved password. He clicks OK and is logged into the Erudite system. Then, it dawns on me. Max is using a password management service to log himself into web sites. He probably doesn't even *know* his password to the Erudite system. Moreover, the password management service will never send his credentials to a bogus site masquerading as the real thing. In looking at the logo in the pop-up window, he is using one of the most secure password services out there called:

P S L A S A T S

June 23

I'm running out of options and out of time. It's been days since I've had access to any of the plans. My attempts to get Max's login credentials have failed and I'm running out of ideas. There must be another way to get access to the Erudite systems as him. If I can't get his username and password, I wonder if there is a way of tricking the Erudite servers into giving us access. I've learned that the way a web server remembers that a client has authorization to its site is to issue an HTTP cookie to it. The client that is given this cookie must present it on subsequent requests in order for it to be given access to the site. If these authentication cookies are sent in the clear, then if an eavesdropper is able to see it, they could use it to pretend to be the client. There was a piece of software called Firesheep that used this method to monitor the network and steal all of the cookies it saw going across. Doing so allowed the tool to perform:

O S I S N S E I C A J I N G H K

Fail. The Erudite have protected their web site by using HTTPS, the secure version of HTTP. HTTPS, unlike HTTP, encrypts the HTTP cookies used to authenticate clients. In order to get access to those cookies, I'd need to break some pretty mighty strong encryption. I am back to square one. The idea of stealing cookies is intriguing, though. In my research on HTTP cookies, I stumbled across another kind of attack that has been used to pilfer them. The attack relies on JavaScript, a scripting language that all browsers execute. JavaScript allows web servers to send arbitrary code to the client for it to run and is used to make web sites highly interactive for users. Unfortunately, it also gives hackers the ability to control the execution on the client. If hackers can somehow inject rogue code into the web content the user is looking at, they can do things like pull the HTTP cookies out of the browser. There was a specific mechanism hackers use to do this called cross-site scripting (XSS). Web sites embed dozens of scripts on a page from a multitude of sources. These scripts implement things like analytics, advertising, user-tracking, and other kinds of widgets. If one can place a script into a legitimate page such as in the comment section of a news article or within a link embedded in an e-mail, one can control the client and have it do something like send its authentication cookie to a random web site or forge requests to websites the client is logged into. There are several types of cross-site scripting attacks that have been used in the past. It doesn't look like I can use the persistent XSS one. Since Max has a penchant for clicking on links in e-mail messages, I think the type that I will try instead is the non-persistent one or:

E D F T E L E R C

June 25

Another fail. How frustrating. I sent another spoofed e-mail message to Max with a link that included a script that would send his cookie to me if he clicked on it. As before, Max clicked on the link in his e-mail which launched another browser window that brought up the Erudite web site. I quickly check the log file on my ``cookie-stealing'' server, but again, nothing. It appears Max's web browser has been set up to block certain scripts. Whoever set this computer up knew what they were doing.

This is looking pretty futile. I need to change strategies. Up until now, I've been targeting Max's computer and Max himself. However, the data I'm really interested in on the Erudite system. Dare I try to attack it directly? Can I even outwit the Erudite network and system administrators? What would a Dauntless do?

I begin digging deeply into the documentation that the Erudite have given us. It is likely that what they recommended for us is what they use in their own networks as well. Figuring out any weaknesses will allow me to penetrate their systems without Max's credentials. One of the first things the Erudite recommend is to block all incoming connections to non-essential network servers and ports. Much like reducing the software surface area available for attack can be done by removing software, one can reduce the network surface area available for attack by blocking unnecessary traffic. By controlling the incoming and outgoing network traffic based on a rule set, one can then establish a barrier between a trusted network and an untrusted one. In sifting through history I find that back in the late 1980s researchers from AT&T created one of the first implementations of this technology that became known as a:

L E F I L R W A

Before getting caught on Max's computer, I managed to get a packet trace revealing Max's network connections to, among other things, Erudite servers. Since the Erudite have likely blocked many incoming connections to their systems, it will be helpful to find out which services are available. Manually checking each potential network address and port would take me forever, but I've learned that there are many automated tools that can help. One such tool is called nmap. It is a network scanner that will automatically probe a network to see what servers and services are open. While that will be clearly helpful, what I really need is something to tell me what is open *and* vulnerable. For that, there is another tool that people in the past used. The scanner I found that does this was released in 1998 and is quite tenable (pun intended):

U N S E S S

The output of the network vulnerability scan shows a web site that hosts an out-of-date version of a web forum. Perhaps this forum is used by the Erudite to communicate with each other. According to the tool, this version might be exploitable. It suffers from a problem common in manyw eb sites: a lack of input validation. This is a weakness where input obtained from the user such as a username or password contains special characters that are not handled properly by the server. Instead of sanitizing the input and removing these characters, the server instead is tricked into executing rogue commands embedded in the input. One of the most common forms of this tricks databases into executing arbitrary instructions. Since the databases affected contain the usernames and passwords of everyone on the site, such a vulnerability can reveal all of the stored credentials of users. There was once a little boy named Bobby Tables whose mother once taught everyone how to perform a:

I C I E T J S Q O L N N

It's no wonder the forum software was out-of-date. After performing the attack and dumping the database backend, it is clear that the forum was abandoned long ago. They just hadn't bothered to take it off-line. That's definitely a no-no. It takes only a well-crafted username for me to pull out the usernames and password hashes from of the site. One username, in particular, caught my eye: jmatthews. This must be Jeanine's login to the Erudite systems. It's likely that her account has special access to everything on the network. I run a password cracker on her password hash, but hours later, it returns nothing. Either Jeanine has picked a strong password for herself or she is also using a password management system like Max is.

I try a bunch of other accounts and it returns a trove of successes. Passwords such as '123456', 'qwerty', 'abc123', 'iloveyou', 'password',and 'letmein' abound. Logging in as these users allows me to poke around in the forum, but the most recent messages on the site are years old. Just having access to an Erudite machine is valuable, though, even if the accounts I compromised don't have many privileges. It is like having a beachhead from which one can infiltrate the rest of the network. There is a common attack that network intruders use when they get access in which they take advantage of programming errors or design flaws to obtain elevated access to the machines and networks they are on. The attack I'll try next is:

L R E I P I V G E A C O S L A T N I E

June 29

In searching for attack methods to raise my access level on the forum, I found a buffer overflow vulnerability in a SetUID program that is on the machine. SetUID programs temporarily increase access levels for users to do very specific tasks. If there is a vulnerability in these programs, rogue users can permanently get elevated access for all tasks. Now that I've gotten administrator access to a machine on the Erudite network, I begin loading it with software that will help me break into other Erudite systems. I use the scanner and it reveals a whole host of internal Erudite systems that might be vulnerable. These systems were completely invisible to the outside world, but now that I'm on the inside, they are all wide-open for me to attack.

My intuition tells me that the most important information is likely protected using something like HTTPS. In searching the results of the scanner, it identifies a web server that is running a serious vulnerability in the popular OpenSSL cryptographic software library. The bug is a bounds check bug where a client can ask for (and receive) a large amount of a server's memory. The bug was found in 2014 and allows one to steal the names and passwords of users. It will be easy to compromise a machine that is vulnerable to:

E B H T E D E A L R

June 30

The forum server revealed Jeanine's user name. In attacking the vulnerable web server, I send hundreds of probes at it and set up a program to search the data returned for anything containing the string jmatthews. After several hours, it finally returns her user name and password. I log into the system as Jeanine and find myself with complete access to the main Erudite computer server.

I search Jeanine's e-mail and all of the files in her home directory. It is a trove of information. It appears that Serum D2 is a mind control serum. A person injected with the serum remains conscious, but is not in full control of their bodies. Instead, their behavior is modified from a remote computer simulation. From the map I had discovered earlier on Max's computer, I'm guessing the serum will be used to destroy the Abnegation. From Jeanine's recent messages, it appears that the serums have already been deployed so in order for me to stop this plan, I'll need to find and destroy the computers running them. I dig deeper and find messages detailing a high-security computer server room that is housed in a secret location on the Erudite campus. Its computers and internal network are ``air-gapped''. They can not be reached from the rest of the Erudite computers. If this is where simulations will be run from, I will need to somehow find a way to infiltrate the Erudite headquarters in order to obtain

A L I S P C Y H S C A S C E

I search for more details of this plan. It must be happening soon. Reading the most recent messages in Jeanine's Inbox, I find what I'm looking for. Launch time is set for Friday, July 10th at 3pm. I have less than 2 weeks to stop them.