

1. Who Did What?

- a. Russ Beck – Chose and researched the Research Lab and Physical Attacks, created the report
- b. Matt Grimm – Chose and researched the Accounting section and Physical Attacks
- c. Matt Dinkel – Found the 7 steps, created the topography, researched Blind-Remote Attacks
- d. Chris Wisor – Researched the User-Level Attacks, created the report

2. Business Processes

1. Research Lab

The research laboratory mainly takes on the task of producing new glove designs and coatings and using computers to perform scientific calculations, exchange ideas and write reports. Following are the responsibilities of researchers at TwoHands:

- Develop new and innovative ways to improve the products and make them more appealing to customers
- Keep ahead of their competitors through the research and development of new or improved products

To help in their developments, researchers want to have easy access to the Internet, where they would be able to find beneficial information to aid them in their research. This would certainly enhance research techniques and help researchers to become more productive in their developments and in turn, making advancements to TwoHands Corporation. It is vital to TwoHands that a connection to the Internet be secure in order to protect its valuable intellectual property.

Each division of the research lab would be on its own network. This way, if a hacker breaks into one network, they would not have full access to all systems. The internet would be secured with a firewall and virus scanners. The research lab would need full access to the internet, so blocking sites would not be good for the company. With this in mind, we have to watch what they are downloading and looking at. We will also monitor what they save and what information is taken off of the computers. We do not want people to steal company secrets. We will also have keycard access to the lab, so that only those authorized have access.

2. Accounting

The accounting system at TwoHands Corporation became automated years ago. The accounting system is currently accessible via the LAN and the accounting system is stored on a server. The accounting business process is important to protect because it gives TwoHands crucial information on the amount of money the company has at the end of each day.

The accounting system works like any other. Information regarding inventory, accounts receivable, accounts payable, debits, credits, etc. are entered into the system as the

information changes. Each time an order is placed, the inventory is edited in the accounting system. The accounts receivable are also updated within the system. Each month, fixed and variable costs, such as lighting bills, rent, and equipment costs, are updated in the accounting system. Following are tasks performed using an accounting system:

- Accounts payable – bill paying
- Accounts receivable – billing for services
- General ledger to record transactions
- Payroll
- Financial Reporting
- Fixed asset reporting
- Inventory tracking

The accounting department is responsible for ensuring that all debts are paid to TwoHands creditors. The department also ensures that there is enough money at the end of each day to pay the employees. The accounting system also enables TwoHands to determine where it is losing money. It offers a variety of information that the business can use to continue to prosper.

The Accounting Department will need to use certain aspects of the internet to do their job. However, to prevent anything malicious from finding its way onto the computers, we will block any non-company website, and will approve certain other websites that might be needed.

3. Topology

Attached

4. Attacks

- a. Research Lab
 - i. Competitor trying to get a leg up
 1. Stealing ideas
 - ii. Thief trying to sell company secrets
- b. Accounting
 - i. Steal sensitive credit information
 - ii. Steal employee information

5. Competitor Trying to Get a Leg Up (Research Lab)

- a. The blind remote attack
 - i. A Hacker trying to beat the firewall and gain access to the company's systems, so that he can see what we are researching.
 1. Reconnaissance would most likely take place on the website. An attack would attempt to gather information on the company and its network. Often, websites include contact information such as email addresses. If they are not included, email addresses and phone

numbers of system admins can often be found using a free service such as WhoIs.net, which looks up the registration information of the domain name. This information could then be used for phishing attacks in an attempt to get a password. This would provide easy access to the network. Let us assume that a phishing attack fails. The attacker would then begin to directly probe the network for more information.

2. Probing the network entails exploring the network directly in an attempt to find security flaws. A detailed map of the network could be attained remotely using a program such as NMap, which can be downloaded for free on the internet. NMap can remotely map out the entire network. Its search includes for each IP address on the network the operating system and any open ports (among other things). A little research on the internet can easily reveal known vulnerabilities for machines which are not properly secured.
3. Obtaining a toehold is gaining access to a machine within the network. Once the vulnerabilities are known, a program such as Metasploit (also free), which keeps a database of known exploits and executes them effortlessly for the operator, could be used to gain access to a machine on the network. Let us assume that the accounting database server was vulnerable and the attacker was able to execute a bind-shell payload in the system. This gives them a command line prompt for the compromised system and access to the entire accounting database.
4. At this point, the attacker is normally impeded by the access control measures of the network. Most accounts should be restricted from important files. However, since TwoHands does not use access control at this time, the attack already has access to all files in the network and can skip the advancement step. We will highly recommend adding access control later, as it can stop a hacker at this point.
5. The attacker, to avoid being tracked, will remove anything that could be used to trace him at this point. Normally, this would involve deleting intrusion detection logs; however, TwoHands does not utilize intrusion detection software, so this is not necessary. They may, however, want to delete various system logs which show their actions while executing the bind-shell payload. They are also likely to replace the system binary code with a malicious one which will not log their future actions using the shell which they have created.
6. Now the hacker will establish a permanent “backdoor” so that they can easily monitor and return to the system at will. A program such as Backdoor.Winshell.50 is known to do this. This specific

program would probably be picked up by a virus scanner, but TwoHands does not utilize one, and therefore will most likely not detect it. They are also likely to install a stealth tool to allow them further ability to fake access to the system logs and other information that may reveal their presence in the system. Trojan.Stealther.B is known to serve this purpose, and again would be picked up if TwoHands implemented virus software. Trojan.Stealther.B also includes a sniffer, so the attacker can keep their own logs of network traffic, giving them intimate knowledge of the company's network operation.

7. After sniffing the network, can gain valuable information, such as user names and passwords. Due to the lack of security, however, it would extremely simple for the attacker to spread from the accounting database throughout the entire system. By repeating some of the steps that they have already used, they can establish listening posts in all the machines on the network. They can access install a virus to take down the network, or steal valuable information without anyone ever knowing.

b. The user-level attack

- i. A Phishing attack sends emails to users in the Research Lab, to try and get them to click on the link, which then downloads a virus onto the computer. This virus then sends the Phisher information about what the user is doing.
 1. Recon: The attacker would search for domain names of the company so it would make it easier to gain access to employee information. The attacker could then get into the system to gain access to e-mail addresses. The attacker then can send out an e-mail to users, attempting to gain access to passwords so they can get access to the system.
 2. Probe: Once the attacker has a password to gain access to the system, they can start to detect weaknesses. In this case, since password protection is the only mechanism in place, total access would be granted with a password. In short, no other security systems exist.
 3. Toehold: Since no other security mechanisms are in place, once a password is obtained, total access is granted to all systems.
 4. Advancement: Because there are no security measures, advancement is not required because you already have a privileged account so you can access all files and data.
 5. Stealth: Nothing is in place to detect intrusions, and since you entered through a normal route and didn't break in so to speak, there is no need to cover your tracks.
 6. Listening Point: Installing sniffing programs or stealth programs aren't necessary at this point because there are no tools in place to stop an intruder.

7. Takeover: Now that they have total access to the entire system, the attacker can begin to spread the malicious program throughout the system, unfazed.
- c. The physical attack
 - i. A thief trying to beat the keycard scanners either by stealing a card, or by creating a fake to get sensitive files.
 1. Reconnaissance – A spy from the ThreeFeet Company chooses an employee of our company he believes can be exploited. The spy has been hired by the Research Lab, therefore, he can observe all day.
 2. Probe – Probing in this scenario would only include trying to guess the employee's password or asking him to leave something up for the spy to look at.
 3. Gaining a Toehold – Apart from the information he already has available to, the spy can use the window the employee leaves his computer open to steal his research as well.
 4. Advancement – Now, he can explore the company files at the expense of the exploited employee. The spy ups the account to admin and pokes around.
 5. Stealth – As long as the spy gets off of the computer before the employee gets back, he will have nothing to worry about.
 6. Listening Post – Since he works in the same area, he is a physical listening post. He could still install a keylogger, or set up a camera on his desk to record his neighbor.
 7. Takeover – Now that he has everything in place, the spy can grab all the information he needs, and quit the job. He has stolen enough to be substantial, but has not been discovered.
- 6. Thief Trying to Sell Our Company's Ideas (Research Lab)**
- a. The blind remote attack
 - i. The thief obtains individual access to a computer, copies the files and sells them.
 1. Recon: The attacker would search for commonly use web applications used by then company that he could attack.
 2. Probe: Once the attacker finds a program, and an exploit, he will be able to test and see if he can get in and which method to use.
 3. Toehold: If he finds a hole in the system, because of our lack of security measures, he will get in quite easily and have access to a lot of important information.
 4. Advancement: Because there are no security measures, advancement is not required because you already have a privileged account so you can access all files and data.
 5. Stealth: Nothing is in place to detect intrusions, and since you entered through a normal route and didn't break in so to speak, there is no need to cover your tracks.

6. Listening Point: In case the company does decide to install security systems, the attacker installs a Trojan to send back information remotely. This way he doesn't have to continuously hack in.
 7. Takeover: Now that he is in, the attacker can do whatever he wants at his own will, and ruin the company's good name.
- b. The user-level attack
- i. The thief could call an employee pretending to be with IT, saying he needs the user name and password. Then use that information to obtain company secrets.
 1. Recon: Go to the company's website and obtain a phone number for a desk of an employee. Then call said employee and pose as an IT employee and get the password.
 2. Probe: Since there are no tools in place to prevent an attack, outside of password protection which has been compromised, the attacker doesn't have to worry about any intrusion detection or anything.
 3. Toehold: Now that the attacker has obtained a password, total access to a network and system files is gained.
 4. Advancement: Because all user accounts are on the same level, there is no need to gain administrative rights since the attacker theoretically already has them.
 5. Stealth: Seeing as currently there are no security tools, the attacker isn't required to disguise itself.
 6. Listening Point: Installing programs to detect other activity isn't required since the company isn't actively stopping intruders.
 7. Takeover: No security is in place so access is easily gained to every system on the network and secrets can be stolen no problem at all.
- c. The physical attack
- i. Befriend an employee and use him to gain access to the system and obtain sensitive files.
 1. Reconnaissance – the thief chooses an employee he thinks he can trick and begins to observe him. If he sees a trend, such as leaving his door unlocked, leaves his computer unlocked, or has his passwords on a sticky note on the desk, the thief will begin to formulate a plot.
 2. Probe – If he sees no obvious flaws of the employee, the thief will begin to test him. The thief might test a neighbor employee to see if that employee will give the thief access, or test out the strength of the door.
 3. Gaining a Toehold – Now, the thief has discovered a weakness, the employee lets the door unlocked when he leaves for lunch and on some occasions does not lock the computer. Now, the thief can access all the files on his computer, and all files in his filing cabinet, exposing company secrets he could profit from.

4. Advancement – Now the thief has had a taste of what he can do, he'll look to advance further. This time, he will make the user account an administrator. Now he has more access and digs deeper into files on the computer to see if any hidden folders are present. He also looks in the mail and rechecks the files for anything new.
5. Stealth – Because of the nature of this attack, nothing actually has to be taken. However, if he copies a file onto a thumb drive, some security systems will log the information and be able to catch him, or a neighbor employee will notice something is up and corner him.
6. Listening Post – If the thief has time, he could install a hidden camera, or computer software that gives him more information. Perhaps he hides a Trojan horse in a way a firewall won't catch it, allowing him to have remote access.
7. Takeover – The thief now owns the employee he is attacking. Every aspect of his job can be stolen and sold. If he is smart, the thief would stop stealing after a few months in case his methods are discovered, but at that point, the damage has been done.

7. Steal Sensitive Credit Information (Accounting)

- a. The blind remote attack
 - i. The attacker would find a vulnerability in software used by the company (either web based or hard drive based) and exploit it, gaining all the information plugged into the software
 1. Recon: The attacker would do some research on what software the company uses. Either by searching the web, looking at pictures of the company, or taking educated guesses.
 2. Probe: If he finds a program he knows we use, finding an exploit will be the easy part. Now, he can test his attack because we have no firewall.
 3. Toehold: Now that he knows the attack works, he can get in and see what he can do.
 4. Advancement: Because there are no security measures, advancement is not required because you already have a privileged account so you can access all files and data.
 5. Stealth: As long as he makes sure no one can see what he's doing while he's inside, the attacker need not worry about stealth, we can't see him anyway.
 6. Listening Point: Now, he can install a backdoor on the software so that if he wants more information, he just calls upon this virus and gets it.
 7. Takeover: Now he can either be satisfied and move on, or try the same methods to another program and begin to take over our vulnerable system.
- b. The user-level attack

- i. Send an email to an employee with a basic attachment called Accounting Numbers, etc. When the employee opens it, a Trojan is installed that relays the information to the attacker.
 1. Recon: The attacker would research which accounting software the company uses. Then they would look for any known vulnerabilities, and whether or not they could exploit them effectively.
 2. Probe: Once that hack is obtained and the exploit is perfected, it's time to use it. System access is gained to the accounting software. The attacker can now use and modify the software that stores all the financial information with ease.
 3. Toehold: Once the attacker is in the system, they can install a keystroke logging program and have the information sent back to their PC.
 4. Advancement: The attacker then can proceed to access more PCs and install the keystroke logging on the entire network and gain access to all the financial information.
 5. Stealth: The PCs do not have any anti-virus programs, so the keystroke logging program wouldn't be detected in any way.
 6. Listening Point: Since the program wouldn't be detected and removed, there's no need to install programs to prevent it from being traced.
 7. Takeover: Once the program is spread throughout the entire company, all financial information would be compromised and exploited.
- c. The physical attack
 - i. Pose as a janitor, enter the offices of the accounting employees and take files or other information left lying around.
 1. Reconnaissance – The thief could choose to use a fake identity and pose as an employee himself to gather information on possible targets. Under the ruse of mistaken identity (say a janitor) the thief can keep a watch on office workings from inside. (possibilities include security systems set in place to limit access to certain areas, guards that keep a close eye on specific areas, late night workers, etc.) Once identified the 'janitor' has his information for where to strike.
 2. Probe – once any weakness is detected they are tested by the 'janitor' to see what is left exposed by employee's (employee not securing his/her work station, leaving confidential documents exposed, not shredding sensitive documents/ leaving them in the trash, not locking areas off limits to cleaning staff, etc). Testing the system for weakness is the primary idea here.
 3. Toehold - being a 'janitor' the thief could have unfettered access to workstations after hours, making stealing information incredibly easy. The 'janitor' could find a problematic employee that improperly secures his workstation nightly and work from there.

4. Advancement – being part of the cleaning staff would probably allow access to just about any part of the office, save for the highest offices or most secure locations. Moving from one station to the next cleaning desks and bumping loose files into his cart as he goes, searching garbage cans for sensitive materials, etc.
5. Stealth – operating under the guise of a ‘janitor’ the thief is able to remain practically invisible on the suspect radar if the right people are duped by it. Again having unfettered access to virtually every workstation within the company during nightly hours would make stealing anything just lying around very simple. Storing anything suspicious inside garbage carts and bags to remove from the building.
6. Listening Post – the janitor thief would be able to return to just about anywhere he wants on a nightly/daily basis to gain access to anything he wants if he has the proper ID, information, keys, tools, etc.. Essentially this job IS a listening post.
7. Takeover – upon discovery of specific information left unsecured the janitor thief would be able to return time and time again to that area to gain privileged material. Taking out the real documents and replacing them with false ones is a very realistic option. Moving from one site to another with no obstacles or barricades blocking his way.

8. Steal Employee Information (Accounting)

- a. The blind remote attack
 - i. Find a computer level vulnerability and exploit it. Once the attacker has access to an individual computer, he can have access to the databases that user had access to.
 1. Recon: The attacker could look on our online servers for an employee database. Looking up domain names and searching at an advanced level could prove fruitful.
 2. Probe: Once the attacker finds what he believes to be a database, he can test to see how to get in and view the information.
 3. Toehold: Once he is in, simply copying and pasting the information will do just fine. Now he has all the information about every employee we hire.
 4. Advancement: Now that he already has all the information, advancing deeper into the system is pointless.
 5. Stealth: Because he will be in and out so quick, and we have to security, stealth should not be an issue to the attacker at all.
 6. Listening Point: Now he can install a program to send him updated databases whenever he wants them.
 7. Takeover: He has successfully taken over if he has a copy of our database, and a program to send him updates.
- b. The user-level attack
 - i. An attacker could send a general email – Hey, I need Bob’s employee number for a project we are working on over here in Finance. Joe the

Financial Officer told me to just shoot you an email. Thanks! – He would then be able to use Bob's information.

1. Recon: The attacker would need to find out what the company uses to store employee information.
2. Probe: Once they know that, they need to gain access to a PC that can directly access that database.
3. Toehold: Once they're in the database, it's a matter of finding critical information such as social security numbers, credit card numbers, bank accounts numbers, and anything that could be used for financial gain by the attacker.
4. Advancement: Since you already have total access to every financial record of every employee, advancement is not necessary.
5. Stealth: No tracking programs are in place, but the program probably has an access log built in, so deleting that would be about all the attacker would need to do.
6. Listening Point: Installing a program that looks for changes in the program and security would be ideal. That way the attacker always knows how to re-access the database and gain more information and cause more damage.
7. Takeover: Installing trackers on all the databases would be all that's necessary for the attacker to do.

c. The physical attack

- i. Wait until an employee leaves his desk, for lunch, etc. and see what he has left laying around. Did he lock his office, or his computer? What is on his desk?
 1. Reconnaissance – the thief selects and watches employee's habits, finding a weakness to exploit in one (possibilities include not securing his/her work station, leaving confidential documents exposed, not locking their office, etc). Once the vulnerability is identified the thief makes that employee their target.
 2. Probe - If no such vulnerability exists the thief may choose to probe the situation possibly forcing a vulnerability (breaking a lock, forging documents or memos calling the person from their desk, etc). Testing the system for weakness is the primary idea here.
 3. Gaining a Toehold – once the weakness is found the thief will try to gain entry into that area/system. As stated before the thief may force the vulnerability if none such exist. From here the thief has access to information left exposed and may be able to dig deeper to gain more confidential information if the toehold has been established properly.
 4. Advancement – upon establishing a toehold the thief would then look to advance the knowledge they can obtain from this person. If this employee is a low level user then the thief would look for any information within the workstation that could point to a more beneficial target. Probably searching the workstation or office for

any confidential information (UserID and passwords or memos) that would lead to further success.

5. Stealth – since this thief is operating on a physical level, stealing the information would be as simple as taking pictures or copying information down. No actual physical items need to be taken from the station, making concealment of the attack much simpler. Possible problems would be cameras or security guards, among other things like the employee returning unexpectedly or destruction/movement of belongings.
6. Listening Post – the thief may even go as far as to install some sort of tapping/listening device or keylog program within the employee's workstation to keep an eye out for any other information vital to their robbery. Always having a fall back plan to get back into a specific work station is essential. Having backdoors in getting more information is always a key to further success for the thief.
7. Takeover – now that the thief has nailed a single employee target to the wall they may choose to aim at other vulnerabilities within the office or network. Any information stored on said hacked employee's workstation is now a risk to everyone on the network. The thief could do the very same things to each of those targets, gaining more and more information along the way.