Social Engineering: Techniques that can bypass Intrusion Detection Systems

by Toby Miller

last updated Monday, June 19, 2000

Rel

Su
the
IDS
Lis
Se

Introduction

The purpose of this paper is to explain how Social Engineering can defeat Intrusion Detection (ID) Systems. As we now enter the 21st Century, the computer age and cyber warfare is in full swing. Companies and organizations are still not fully addressing or understanding the issue of Social Engineering. The concept of Social Engineering can cause destruction to networks and cost companies millions of dollars. This paper will try to bring to light exactly how Social Engineering exposes the vulnerabilities of Intrusion Detection Systems and what can be done to protect ourselves against these vulnerabilities.

Intrusion Detection Systems

Intrusion Detection systems are applications that provide early detection/warnings to systems administrators when their computer systems are being attacked by hackers. These systems are usually installed throughout a network in strategic places. Typically, most security administrators like to place Intrusion Detection Systems in front of a firewall and behind the firewall. Many companies and organizations also place these devices in front of any critical network (i.e. Human Resources, Finance). The logic behind the placement is simple - most administrators want to view the attacks that are coming at the firewall, and those attacks that move past the firewall.

Now that we have identified where an Intrusion Detection System would be installed lets take a look at how ID systems recognize attacks and how administrators are notified. ID systems are similar to anti-virus software in that both require a "signature" to identify what the attacks look like. According to the American Heritage College, a signature is a distinctive mark, characteristic, or sound indicating identity. In the Intrusion Detection world, a signature is a distinctive pattern or piece of code that identifies different attacks. An example of a signature is found in Figure 1. Using signatures to identify attacks are good but it does have its flaws. The biggest problem with this kind of detection is that it is dependent on a specific pattern being known. Therefore, if the Intrusion Detection System is not updated regularly, it will not identify recent attacks. Until Artificial Intelligence in Intrusion Detection Systems becomes more advanced, detecting these signatures will be a difficult task. The following is an example of an Intrusion Detection System signature[1].

```
xmas_schema = library_schema:new( 1, ["time", "ip", "integer", "ip",
                                         "integer", "string" ], scope() );

filter xmas ip ( )  {

     if (tcp.hdr){
       $dabyte = byte(ip.blob, 13);
       # if SFAURP are all set this is nothing but a malicious packet
       if (!($dabyte ^ 63 )){
         record system.time, ip.src, tcp.sport, ip.dest, tcp.dport, "UAPRSF"
           to xmas_recorder;
         return;
       }

     }
}
```

```
xmas_recorder=recorder( "bin/histogram packages/test/xmastree.cfg",
        "xmas_schema"  );
```

Figure 1: XMAS Tree IDS Signature

Figure 1 identifies the XMAS Tree scan. In the XMAS Tree scan, an attacker would send a packet that has the SYN, FIN, ACK, URG, PSH, RST flags set. According to RFC 793, this type of activity should not occur under normal situations. Therefore, an attack is in progress if a network is receiving these packets.

Social Engineering

Social Engineering is an attack method used by many attackers that takes advantage of trust and complacency at work. Humans by nature are very trusting and rarely question actions that are considered normal. Examples of Social Engineering are shown in Table 1.

Type	Description
Friendships	Exploits the trust relationship between friends.
E-mail	Forum used to exploit people's trust and spread certain types of attacks.
Dumpster Diving	Technique where attackers go through trash cans to obtain information.
Office Snooping	Great technique that requires snooping eyes and unlocked doors/cabinets.
Trust	Social Engineering exploits human trust.
Time	Attackers have this element on their side.

A recent example of Social Engineering is the "Love Bug" virus that raged havoc on many networks in May 2000. From a technical standpoint, this virus was not considered spectacular. Nevertheless, it did exploit our trust of the phrase "I love you", and showed the weakness of the Microsoft Outlook e-mail program.

Until the Love Bug virus was released, we trusted most e-mail that came to us that stated I love you, especially if it came from a trusted source. Why? - Because the phrase "I love you" is often used to express our feelings. When this virus came out, most people opened it for one of three reasons:

1. It came from a trusted source (i.e. co-worker, spouse),
2. Many people thought it was a joke (e-mail is great for distributing jokes), and
3. The person opens any, and all e-mail.

This virus exploited our trust and caused the billions of dollars to repair. Trusting was never so expensive.

Another forum that Social Engineering can expose is the Computer Conference (i.e. SANS, Defcon) Computer conferences are great for obtaining information. Most conferences stress openness, this within itself is not a bad idea but the problem occurs when people give too many details. Some of the information that attendee's and instructors give out could be used against them and their network(s). Information about network configuration, types of firewalls and Intrusion Detection systems were just a few items commonly shared.

Social Engineering vs. Intrusion Detection Systems

This area is interesting because there are a number of companies and organizations that overlook Social Engineering, giving them a false sense of security. Parameter devices are good for protecting resources from outside computer attacks, but there are very few resources to protect us against the human attack.

There are many ways that an attacker can take advantage of a business or individual using Social Engineering methods that will not be detected. The following is a list of methods an attacker can use against a business or an individual to obtain information. Information in this case could be more then just a password or IP address; it could be critical network design data, business plans or future marketing plans.

1) Friendships: One of the best ways to obtain information and access is through friendships. Once a friendship has been established, there is usually a "trust" between those individuals. This trust is what usually is exploited. This technique is great in obtaining information along with being stealthy to firewalls and Intrusion Detection Systems. Many friends share information with each other about different subjects, this includes work-related information. If an individual wanted to mount an attack against XYZ company and needed a great starting point where do think he/she might start? Probably with the companies employees. If the individual has friends already in the company they can begin using Social Engineering techniques to obtain critical information about the companies network, hiring practices and financial data. If the individual does not have a friends within the company he | she can develop some friendships. This type of Social Engineering happens quite frequently and unfortunately, people are not aware of this.

2) E-Mail: E-mail provides great opportunities for attackers to use social engineering. As stated earlier, each Intrusion Detection System and Anti-virus program requires signatures to capture malicious packets or mail. Because these signatures cannot be developed until the malicious packet/code has been discovered this gives the attacker time to do his/her work. How many times have you logged in at your ISP and there is an e-mail waiting for you claiming to be from the ISP's customer services division requesting your user name, password and credit card number? Could an IDS system or anti-virus system detect this? That would depend. If this happens all the time then the answer is yes. Otherwise, probably not. As technology advances, so will the type of virus we will be encountering. Social Engineering will become a critical part releasing and executing these viruses. The great thing about e-mail is that it only takes one person to open his/her e-mail to begin its circulation.

3) Dumpster Diving: Dumpster diving is a simple technique that requires no technical skills. All dumpster diving requires is the will to find the necessary information and dig through a trashcan or dumpster. Why would anyone want to dig through trash? Many people throw away valuable pieces of paper without thinking about the information on that piece of paper. A good example is credit card receipts. Many people will throw these away after they receive their statement and verify that everything is correct. The problem is that when a person throws away these receipts without shredding them, someone who is dumpster diving can get your credit card number and use it against you.

The same is true for network information. Many companies and organizations have policies on how to treat documents that are considered confidential or secret but how about the other documents? Company's phone books, IP addresses and server information are all documents that may not be considered classified but needs to be shredded because of the information they contain.

Dumpster Diving is another technique that can be used that neither a firewall nor an IDS system could detect but could certainly be considered an attack. The following are steps to prevent this type of attack:

- Lock your garbage containers,
- If you are unsure about the information shred it, and

- Implement policies that cover these types of situations.

4) Office Snooping: Office snooping and dirty desks can fall into a one package deal. If not controlled, both are vulnerabilities that can be detected. When people leave work at night some lock up their desk and offices, some do not. Because some people do not lock up before they leave, anyone could copy and steal information, put the original back and the victim would never know that he/she had been attacked. Have you ever had a co-worker that keeps a messy desk? If so, then this is also a big vulnerability. This can be used against you in the same fashion as office snooping except the attacker could take the original document and the victim will never know (he will probably think that he lost it and think nothing of it). Again this form of attack leaves no noticeable trail and neither a firewall nor an intrusion detection system would catch this attack.

5) Trust: Although this is not really a technique used, it does need to be covered. Trust along with negligence and ignorance; make Social engineering a great attack method. A lot of what Social Engineering is about deals with violating the trust we have for other people and even people positions. Until people are trained or we stop trusting so easily, we will always be vulnerable to this type of attack. A great example of exploiting the trust relationship is credit card companies calling to give a new card and new rate. How many times have the credit card companies questioned you about your social security number, mothers last name and average household income? How many times do you give this information to them? This is the kind trust that is easy to exploit. We often trust that the person calling us is from a legitimate company trying to sell us a credit card. How do know that it is not a person calling from home gathering social security numbers and personal information about selected individuals. Trust can cost us everything, so we need to be careful with whom we provide information to.

6) Time: Remember attackers have time on their side. They can take as much time necessary or as little time necessary to complete the attack. Defenders have very little time to react to these incidents so it is vital that we know what to do in these situations. In other words, an attacker can mount his attack over a six (6) month time period where as a security administrator only has seconds to defend his/her site. In this case the attacker has time on his/her side.

Preventing these attacks

A lot of these attacks can be stopped if people are aware of their surroundings. The following is a list of recommendations on how to prevent these attacks:

1) Training: Training is very important in preventing these types of attacks. When training people on social engineering explain to them scenarios, why this type of attacks happens and what they can do to prevent it from happening. Make training fun and educational for all. Training should occur every quarter to six months. The training should enforce the techniques that attackers use to accomplish the attacks versus what would happen to the individuals if these attacks occur. Another recommended technique is to reward employees if they catch a violation in progress. Rewards could be a certificate of appreciation, days off and/or cash rewards. Again, this depends on how much your information is worth to you.

2) Policies: As with all of security, an organization that has good policies and is able to carry out these policies will be less likely attacked. An organization that does not have policies or has trouble enforcing policies will have a difficult time recovering from these attacks. Need I say more?

3) Awareness: With all of the attention given to "Hackers" and their technical knowledge many companies and individuals often forget that social engineering types of attacks often occur and therefore these same companies gear their security efforts towards the technical side only. The security community needs to make people aware that these attacks are out there and show them how to reduce the risk of being attacked from all sides.

Conclusion

Social Engineering is a great tool that many attackers will use to evade Intrusion Detection Systems and many other computer programs that are designed to catch attackers. I hope that this paper brought to light the importance of Social Engineering and how it can impact our business world.

References

[1] L0pht.com http://www.l0pht.com/NFR/

Toby Miller is currently employed by a major Internet security firm based in California. Toby holds a B.S in Computer Information Systems . Toby is a GIAC Certified Intrusion Analyst and a Microsoft Certified Professional. In his seven years in the computer field he has worked in many area such as Firewalls, Unix administration, NT Administration and some mainframe work.