Global Information Assurance Certification Paper

JARRAD LISMAN

GSEC v1.3

ADMINISTRATOR COMPLACENCY: A REAL THREAT TO NETWORK SECURITY

Abstract

In a world of fast paced technological expansion it is hard for people to keep up with network security. It is even harder to secure a network when the person involved has become lazy or has not received the proper training to enable them to perform their job effectively. Complacency in the network security industry can be cited as the cause of many major intrusions and hacking strikes. Administrators are forgetting to do simple tasks or they just cannot be bothered. And that is a major cause for concern in a world where information transfer over the Internet is a critical function. What's worse is the fact that many new IT security professionals are seriously lacking in training but are getting the work because of the low cost to companies.

So in this paper I will talk about security issues that I have discovered to be where network security professionals, in general, are below average. These are not the only areas that need to be addressed by professionals but are the ones that I find the most alarming and threatening. They include not being aware of how easy it is to hack in today's world, how threatening the technology boom is, IDS and how it is not perfect, log monitoring, upgrades and patches and the qualification level of some so called administrators.

Introduction

As a new member to the world of IT, I thought long and hard about what kind of network security issues I could write about for the GIAC accreditation. Being an electrical engineer by trade I can tell you how a computer works but when it comes to software I have little to no clue.

I began to research hacking in general and began to realise how easy it was to do and how easy it is to get information on the processes involved. It then occurred to me that if I didn't know it was that easy maybe there are others that don't realise how easy it is. Obviously there are and the problem is some of them are administrators, responsible for the security of complex networks.

The process of hacking in today's modern world is so much easier that people now devote their lives to preventing intrusions into network systems. Large companies employ specialised people to try and break their systems so that they can know where holes exist and further protect their data. But does it work? Will they find every hole? Of course not, where there is a will there is a way and if a hacker is determined to get into a system they will… eventually. The only sure way to prevent hackers from attacking your system is to disconnect that system from the wider world and that is only protecting from external hackers, what about the internal staff member who wishes to further their own career by spying for another company? Easy solution? Not likely. Fast data transfer now-a-days is relied on that heavily, that the difference of seconds can mean millions of dollars.

What administrators are forgetting to do is to step into the mind of the hacker. It is all well and good to set up this incredible firewall and then try to break it down and come back thinking you are invincible when you can't break it. But have you achieved anything? *Is* that system unbreakable will your firewall keep everyone out? It might for now but can you conceivably check every known exploit, do you know that there is a new exploit several weeks old that no one has heard of yet? Of course not.

With the Internet now being so large and widely accessible, with computer processor speeds and hard drive sizes growing at an astronomical rate, it becomes easier and easier to take control of and use someone's home computer to break into large corporate facilities.

Each system must be constantly monitored and administrators must keep up to date with patches or they are not sec uring their network. There is a mountain of work for administrators to do in their every day job and I don't believe that half of them realise what is actually involved and what knowledge and skills they will require to do the job. Then there is the proble m that another half of network administrators just do not know… anything.

Learning how to hack, how easy is it?

I'll start with the Google search engine. Within seconds I have done a search on how to hack and have received a staggering 2,130,000 results i n a whole 0.16 of a second. Unfortunately, as is expected with most basic searches the first few pages are junk, a few newspaper articles and other jargon. As I progress through the lists I come upon a site that at face value appears to be it, this is the one, this will tell me all I need to know… it is:

"How to become a hacker"

The opening sentence is:
"Looking for advice on how to learn to crack passwords, sabotage systems, mangle websites, write viruses, and plant Trojan horses? You came to the wrong p lace. I'm not that kind of hacker ."
So I have hit the wrong place, oh well, I have only been looking for two to three minutes. Let's continue looking.
Now I have just found a whole bunch of sites that are designed to help people to hack systems for an educational purpose… yeah right!

"UK Hacker and Phreaker's Guide"

"The alt.ph.uk group"

There were more and more sites including one with three large pdf files on how to crack windows 2000, but then I hit the ultimate, a whole site dedicated to hacking pages and what's more, it rated them from one to fifty! What is this glorious site?

"Blackcode.com"

This site has everything, downloads, information, its own top 50 hacking sites. What else could a new hacker want?

So now I kno w where to look, lets have a look at what there is for me to get and how much I get told about how to start on my hacking career.

Starting with The Newbies Area, I click on the link and what do I find? A whole page dedicated to Unix hacking tools, we hav e root kits, Nukerz, Spoofing, Security for your own system, Sniffing, Cloaking, Scanners, Crackers and other Miscellaneous tools that do a combination of the above in one fell swoop. Each of these general areas has around ten to fifteen tools each. What b etter place to start as a hacker. Of course there is a disclaimer at the top of the page warning that these tools are for "educational purposes only" but who really expects that every visitor to this site will use these tools for education? I guarantee tha t some young people will enter the site

and use these programs for malicious reasons, fully understanding (or not) the consequences of what they are about to do.
Ok, now I have all my tools for hacking a Unix system, all I need to do now is find a place that I want to hack in to and go for it. Given that I am new I will probably start small. I'll find some small company that has a weak security system, as they cannot afford a top of the line administrator and all the relevant tools, and I'll practice on their system.
A few weeks later I have become relatively adept at hacking small systems as I have so much spare time on my hands that I spend every spare moment on the internet. As I become more and more skilled in hacking I begin to target bigger and bigger networks, till I am so good that cracking someone's system becomes like second nature to me and by this stage I am so proud of myself that I will not stop. Having no real motivation other than to just cause havoc I will continue till someone is smart or good enough to catch me.
Now a year or so later I have become, if I was dedicated enough, an experienced and worthwhile hacker, more than likely good enough to begin writing my own code and my own hacking tools.
If it takes one person just over a year to bec ome well versed in the art of hacking and there are approximately six billion people in the world, it doesn't take a genius to work out that with the current rate of internet expansion, that there are potentially millions upon millions of hackers out there and their numbers are growing increasingly with the new generation of computer literate children with free and fast access to the internet.
For example, the fifteen year old Vice Miskovic of Croatia hacked into U.S. Army computers, just to see if he could do it.

> *I used some of the hacking programs available on the Internet, adjusted them, and, with a bit of luck, managed to break into the computer system of the Anderson Air Force Base in Guam," Miskovic said this week.*
>
> *"It was a challenge," he said, smil ing. "I was curious to see whether I could do it or not."*[1]

What is worse it took U.S. Army administrators a whole month to detect and put an end to the boy's mischief. If a more experienced hacker, say sixteen years old, had gotten into the system, what is to stop them erasing their tracks and placing backdoor's or getting classified documents? One month is a long time to have access to such a system.
It is easy to hack systems, the tools are just there and the documentation on how to use it is also there with it. Administrators are getting smug and forgetting to think like the enemy. Some are not taking into account that there are millions of young people who are ready and willing and have the resources to hack systems. It may sound like paranoia but it is how an administrator must think in order to beat the children of tomorrow. It must be acknowledged that there are constant malicious attacks occurring on lots of systems by hackers who have learnt their techniques off of the World Wide Web.

[1] Vukic, Croat Teen: I hacked into army

Technology? Won't that help me?

This brings me to the next problem with network security that administrators are failing to see; the fact that technology is changing at a phenomenal rate that it is impossible for one person to know everything there is to know about net work security without dedicating their life to constant study. It is here that administrators are forgetting that new exploits are being found all the time and it is often months before they are known to the wider world. That gives hackers several months t o be in and out of a system or crash it as they wish. Administrators cannot believe that they have built a secure system, there is no such thing. It may be secure against known threats, and even then you can bypass the detection systems, but there are alwa ys unknown threats that have the ability to do as much damage as the known ones.

It is not unusual now a days to find a Gigahertz speed machine with 150 Gig of hard drive space, half a Gig of RAM and a high -speed connection to the internet in someone's lou nge room. With this type of power in the hands of the average Joe, how hard is it going to be for them to perform operations that require lots of computing power? Not very, they may have to leave the machine running over night working on the problem, but h ow long is that in the big scheme of things? So they watch a movie one night instead of hacking computers, big deal. And what if 150 Gigs of hard drive space is not enough? Easy, I just find some small company that is easy to hack, or even more likely with permanent connections to the net, I find someone with their home PC connected to the net which also runs at similar spec as my own PC and high-jack some of their resources.

How do you protect against someone who has the combined computing power of one to two hundred home PC's all with high speed connections to the net all slaved to do their bidding? It is not like you will be able to get every home user to implement their own security policies and network monitoring. Apart from being too expensive for the average home user, it requires years of experience just to know what needs to be done and the average user does not even have the skills or knowledge to even know where to start. The average user, without having experience in the IT world or a personal interest in the working of computers will not stand a chance and even if they did have some knowledge, unless they were a computer genius they still probably wouldn't stand a chance

So you now have some sixteen -year-old computer boffin, with several hundred computers backing them up, trying to bust through a "high -tech" network. What chance has this hacker got? A fairly good one with that much processing power, storage space, a will to break something and no moral dilemmas. Without significant monetary backing , there is no way a system administrator can compete with that. Their network is now susceptible to attacks and passwords become easier to brute force open.

Are administrators thinking about this? There is a reason that cryptographic algorithms are written to last 150 years, because with technology expansion it will only take 15 years. These people will get excited about the newest gigahertz range of Pentiums but will forget what it means to their network they are trying to secure. They must realise that in the end every advance in technology is a new threat to their system.

OK we are now aware of who and what we are dealing with, a youngish computer nerd with an unlimited amount of processing power behind them. So how do we prevent this person or persons at tacking our system?

Are intrusion detection systems all they are cracked up to be?

"But I have an intrusion detection system, I can tell if someone has entered my network" I hear people cry. Well that is good, it is one of many steps that are needed to help detect and prevent unwanted people entering you system. The problem is I decided to look at intrusion detection methods, briefly and in no amount of detail, in order to see how easy it would be for someone to detect an intrusion, even if they could not prevent it.

So back to the trusty search engine and I type in "network security".

Four links down the page I find what looks like an informative site and not just one that is designed and made by some intrusion detection software company trying to plug their own gear.

"The Network Security Library"

On the left hand side there is a menu bar that has a link to their intrusion detection area. Clicking on this I find a page where there are lists of papers that can be read. Scrolling down these I am faced wi th titles as follows:

> Intrusion Detection
>
> Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Events.
>
> Investigating an Attempted Intrusion
>
> Intrusion Detection within a Secured Network
>
> Insertion, Evasion, and Denial of Ser vice: Eluding Network Intrusion Detection
>
> 50 Ways to Defeat Your Intrusion Detection System

Hang on… 50 ways to defeat your intrusion detection system?!?! What is this? Looking back there is another paper on eluding network intrusion detection.

So what is the point in performing network intrusion detection if it is only going to be bypassed by some clown who is twenty years your junior and has stumbled upon a site that tells them how to beat intrusion detection, a crucial part of a network protection system. Well before we get too carried away let's look at how this is performed and see what these hackers will be doing to avoid your network monitoring.

Upon opening the page, 50 ways to defeat your intrusion detection system, I read the introductions and find out that the article, written by Fred Cohen has interesting background information:

> *From a standpoint of the network security manager, it is often difficult to tell the wheat from the chaff when selecting products or deciding on capabilities. The current situation in intrusion detection is that very*

few managers know how to make a proper decision and vendors seem to be taking advantage of this knowledge vacuum to make sales.

I have heard many claims and a wide range of prices for these systems, but the plain truth is that most current intrusion detection technologies and systems available to the average buyer are poor at best. This seems to me to be a case where the emperor has no clothes. Since exposing naked emperors is one of my goals in life, I thoug ht it might be useful to provide decision -makers with some ammunition to use in evaluating candidate systems. While I hope my playful tone is understood, the issues underlying these examples are serious and these examples are only the tip of the iceberg. [2]

The article then goes on to explain some very, very easy ways to defeat the common IDS system, from simply adding a few bogus lines of code that don't do anything but change the look of an attack to changing the language the attack was published in so that the IDS will not recognise it. In short IDS systems are comparing attacks against a set of guidelines so that if you modify the attack to perform the same job but not be recognised as the original form of the attack, it will not be detected by the IDS system.

Intrusion detection systems, for example Snort, use a set of rules that when matched to specific data incoming on the network will flag an alert. This alert is then placed in a log file that can be checked later. By itself this will not prevent an at tacker having access to the system and for an experienced hacker this log file can be altered to remove all trace of their incursion. These log files when looked at are a multitude of entries that go on and on and on and each entry is similar to the last. An administrator would have to spend hours of their time sifting through each file to determine if an actual attack has been launched or if it is just harmless traffic. So now a tool such as SnortSnarf is added to the process which allows an administrator to view these logs as a nice web page or alternatively data bases such as MySQL are used. This is all well and good if the hacker has not removed evidence of their intrusion. But the fact still remains that these attacks may have occurred hours earlier tha n when the log file is looked at.

So now we add response rules to the IDS so that, for example, if a specific IP address makes a number of failed logon attempts within a given time frame, their IP will be banned from accessing the system or something simil ar. Good, we now have a set of rules that if matched can prevent and will log attacks on a system, until a new exploit is released.

Although a powerful tool, intrusion detection software is literally only software and as such, can only detect behaviour th at it decides fits within a set of parameters. The computer systems that it monitors are sufficiently complex such that it is impossible to describe every possible attack although, to counter this, attack signatures are provided to keep systems up to date and it must be said that, by using the same logic, it will guard against some attacks that have not yet been used.

[2] Cohen, 50 ways to defeat your In trusion Detection System

Administrator complacency is the protected network's biggest long - term enemy.[3]

Here we have seen that an IDS is not all it is cracked up to be and that it is itself susceptible to neglect. If administrators neglect it then it will not be up to date and cannot perform its given task of helping to prevent and log known attacks on a system. Administrators cannot become complacent in this, it is important that the IDS is constantly checked and revised and monitored correctly.

The log files.

Log files are an administrator's best friend, these files will record everything that happens to a system. They may not be easy to read, they may be large and cumbersome but they are important, they are the keys to providing good system security. Without these little gems of information, an administrator is virtually flying blind, they have no way of knowing what is happening on their system as they cannot see and react to everything at the one time.

I have found that Linux based systems have a multitude of log files that are nicely split into different areas so that the average human can read them and know what each relates to. In the /var/log directory is a lo g file called messages, which will log all events that deal with the kernel. There is also a file called secure, which logs activities such as logons, logon attempts and security related issues.

Why do these files exist? So that a system administrator know s what is going on. Monitoring these files will provide an insight into the who's and what's of a system and the why's of what is going on. Administrators often ignore these files and forget to check for recent activity that could be malicious and damaging to the systems continued operation.

There is no little GUI tool around that will ensure that administrators read their log files, there is no piece of code that will patch the logs into the brain of these people. If they do nothing else, administrators *must* check these files several times a day. There is no point in making a 'secure' system if you do not read these files. These are the final line of defence, computers are stupid, they do not think outside of the box, they have a set of rules that they will stick to and will ignore everything else. A computer cannot tell suspicious from good unless you tell it, a computer does not know what bad is and what bad does. Administrators must know what is going on, they must know how to make the computer smarter. I f not, another, smarter person will break into their system and will be free to do whatever they like. Log files are a guide to this. If a serious intrusion occurs, they are the trail to follow when determining what went on, it is the log files that will h elp you prevent it from happening again.

System administrators must stop disregarding the logs and start paying attention to what is going on in their system. It is their clue to the internals of their system and what is happening behind the scenes. Withou t this administrators will never know exactly what is happening on their network behind the scenes, behind what they can visibly see on the screen.

Upgrades? Patches?

"Virtually every report of a hack attack that I read says, 'The hackers used a known exploit for which a security patch was released,' notes Wired's Delio." [4]

---

[3] Grosse, Internet Security Systems: RealSecure

This one is easy, there are that many news groups and web sites out their that finding the patches, being aware of the patches, knowing about the security holes is a simple matter of putting your name on a list and reading the incoming mail. Many administrators do not have the will to go out of their way and monitor what is going on in the world.
It is here that administrators are not being pro -active enough, in that they are not getting the updates to fix holes in their systems. Without these patches the holes exist for some script kiddie to exploit on the network. It requires a small amount of work but the rewards are huge and in the long run will save the administrator time and the company money.

The drive, the knowledge.

System administrators now days seem to be more and more careless with their work and seem to take their jobs for granted. Training as a system administrator is now becoming easier and easier to come by, resulting in less professional and less dedicated people being employed for the job. Also due to the economics of hiring a less experienced person, these administrators with less knowledge and less drive are being churned out at a dime a dozen and consequently are infi ltrating into the IT world where they can end up doing more damage than good.
There are constant reminders of administrators having qualifications that are not up to scratch, including the example given in an article called Screwdrivers & Degrees at Radsoft.com. It is mentioned here, that many administrators now days do not even know what a hidden file is thus causing a demise in the standard of computer network security. With exploits being found faster and faster, too fast for people to keep up with, the standard of system administrator skills must get higher and higher to cope. Companies are looking for cheap alternatives, which may in the long run lead to many thousands of lost dollars, as the cheap alternative was not good enough to stop or find an intrusion.
To demonstrate this point I will go back to my university years where I lived on campus with a thousand other young adults. At this particular institution we each had a T1 line into our rooms and were charged 12 cents per megabyte of downloaded data .
In the last year of university some people that I knew discovered a new and wonderful program called Direct Connect. The best way to describe DC is like Napsta but with files and CD images. Now DC didn't connect on a standard port and hence was not recognised by the billing program that was tracking our data transfers. Upon discovering that they were not being charged for these downloads, like most young uni students, they abused the fact and began to download hundreds of gigabytes of software within a ma tter of days.
After a while they ran out of interesting programs to download and only used it occasionally. This went on until three months later an e -mail was sent to all of the students on campus saying that it had been discovered that students were usin g a program that used an un-tracked port, but the problem had been rectified and that people could be charged from now on. The mail also stated that a debt recovery would not be implemented to recover the costs already incurred.
Looking back at this, about four or five of my friends downloaded around 200 gigabytes of data. This alone totals a whopping $24 000 of downloads. Add to this the fact that they probably were not the only ones and you can see that in just three months

[4] Rudich, Network Lockdowns

potentially hundreds of thousands of dollars could have been lost by the IT administrators at the university.
Over three months it should have been obvious that an unusual amount of data was being transferred over the Internet connection and it should have been acted upon sooner. If the IT cell had been monitoring the system they should have immediately been able to tell that the abuse of an open port was occurring. In a situation where there would be more aggressive hackers this may have led to a situation where in a corporate institution, millions of dollars in revenue could have been lost and permanent damage to the equipment may have been caused.
It does not take hackers long to exploit a hole in a system and three months is way to much time for just a simple thing such as excessive data transfer to be noticed. If this had been a hacker not a downloader would they have been detected?
It can be seen with this, that the skill level of system those administrators, was just not good enough to deal with this. Again this problem is related to not monitoring logs etc but not monitoring logs can be attributed to having a poor background in the administrative area or shear laziness. IT people are now less skilled than what they used to be in a world where they need to have greater skills as there are more and more complex threats out there.

Conclusion

Administrator complacency is becoming more and more, wide spread. It has come to the extent that even system administrators themselves can be counted as a security hole. Administrators are forgetting that it is becoming easier and easier to hack and with the new generation of computer literate children and script kiddies, that hacking attempts are going to escalate. It is here that IT people must remember who it is they are dealing with, in general, young people who are bored, with nothing better to do and no moral obligation or no understanding of the consequences of what they do.
The problem of hacking being easy is then compounded by the fact that technology is growing and spreading, bringing the Internet to those that did not have it and to those places or countries where the hacking laws are not as strict as elsewhere in the world. This technology boom is not only bringing access to the net to these people but is also supplying very high tech, very fast machines with a big pipe to the net, to the average person. They can then use this processing power to break stuff that they never would have been able to, just a few short years ago.
This technology then swings the other way in that administrators begin to think that their machines are fast enough and that their software is good enough and they begin to rely too heavily on their system. Administrators then forget that security is required in depth and that an IDS by itself is just not good enough, there are ways around them and they will soon become antiquated if not constantly checked and revised. To aid in this constant watch, logs were created. These logs when monitored closely will give details about any intrusion that defeated the IDS or any attempted intrusion so that a counter measure can be constructed or devised. People are forgetting the logs and become happy in the knowledge that they have a firewall and an IDS. If they checked the logs I am sure that they would get a surprise in that their "protected" system is not as secure as they thought.
It is not only the logs that administrators are becoming complacent about, they forget to check for upgrades and patches. No one knows if a piece of software is totally secure, you will never be able to prove something is secure only that it is insecure. Because of this fact, software developers release patches so that any holes that come to light in their programs can be fixed. Again, it can not be stressed enough that the

system will never be secure b ut you can begin to narrow down the security holes to make it harder for intruders. It is mental block in the minds of administrators now days that they find it hard to accept that they do not have an unbreakable system.

The main problem, I feel, with admi nistrators today is that they do not know how to use a computer. They may have done their course or degree, but none of it ever sank in and now they are being paid low rates by companies thinking they are getting a network administrator when instead they a re getting some goose who likes to think they know about computers. It is becoming an ever -larger problem that network administrators do not know about computers to the extent that is needed to monitor traffic and fight intruders.

Administrator complacency exists on several levels. There is the person who knows what to do, but is lazy or has not realised what the outside world is actually like and then there is the administrator who is under trained and has no ambition to extend themselves off of their own back. Combining these two kinds of complacent administrator together you get, probably, the largest security problem in modern computing. Without the administrators awareness there is no possible way of any other problem getting fixed.

A complacent adminis trator enhances all other security issues and magnifies their potential damage.

REFERENCES

Robson, Gary. "How To Become A Hacker". Dec 1998.
URL: http://www.robson.org/gary/writing/b_ecomeahacker.html (13 Mar 2002)

Gandalf. "UK Hackers and Phreakers' Guide".
URL: http://www.exegesis.uklinux.net/gandalf/index.htm (13 Mar 2002)

Davis, James. "alt.ph.uk Group". 2001.
URL: http://alt.ph.uk.com/faq.html (13 Mar 2002)

Blackcode.com. "Blackcode Top 50".
URL: http://www.blackcode.com/top50/ (13 Mar 2002)

Vukic, Snjezana. "Croat T een: I Hacked Into Army".
URL: http://www.infowar.com/hacker/hackr.html -ssi (13 Mar 2002)

Cohen, Fred. "50 Ways to Defeat Your Intrusion Detection System".
URL: http://secinf.net/info/ids/9712.html (13 Mar 2002)

Grosse, Paul. "Internet Security Systems: RealSecure". Jun 2000.
URL: http://ourworld.compuserve.com/homepa_ges/pagrosse/j03f.htm (13 Mar 2002)

Rudich, Joe. "Network Lockdowns". Aug 2001.
URL: http://www.computeruser.com/articles/2008,2,2,2,0801,01.html (13 Mar 2002)

Radsoft.com. "Screwdrivers & Degrees". Feb 2001.
URL: http://www.radsoft.net/resources/rants/20010201,00.html (14 Mar 2002)