TCP/IP Skills Required for Security Analysts

Don Parker 2004-05-17

Breaking into the network security industry, and finding a job as a computer security analyst can often be a daunting task. A great deal of us who work in the industry started down this path with nothing but an interest in computer security to begin with, and a desire to work in a field that we love. The question of how does one seek employment in this job sector, and more importantly what skills does one really need to have is a question I have been asked many, many times. One of the wonderful parts about the online community is the spirit of sharing and helping one another. Bearing this in mind I will now attempt to give a far fuller explanation of what I believe to be core skills required in today's security professional. Within the confines of this article the skills that I personally believe one should have at a minimum will be listed, and reviewed briefly to give you an idea of what those skills are.

In this tightening labor market it is also beneficial to have some certifications as well. Quite often the certification process also helps to cement one's knowledge in a particular area. For example getting a CCNA will certainly help you solidify your skills in the setting up of and daily maintenance of a router. This is just one example, and there are many others. A great number of people question the value of certifications, and their actual impact on the hiring process. Answering this question is beyond the scope of this article, and would be highly subjective at best anyhow. What is difficult to argue though is the fact that many company's are now openly advertising their jobs with a demand for some certification or other now. Knowing this it would seem apparent that getting one would certainly help in getting hired by a company. However, having the skills required to actually do the job, certification or not, may be another question altogether.

TCP/IP skills

The skills I am going to list are in no particular order of importance. Typical for people employed as security analysts, we will cover TCP/IP, IDS, IDS data output management, firewalls, routers, programming, and operating systems. That being said there is one area of knowledge that serves as the foundation, which all others skills are built upon: TCP/IP. This abbreviation stands for transmission control protocol, and internet protocol. There is more to the TCP/IP protocol suite then the aforementioned two though. Were it simply a matter of knowing and understanding two protocols it would indeed be a simple task. One has to know a great many other protocols such as ICMP and ARP amongst many others to gain a solid footing in this area of study. Gaining a deep or expert understanding of this subject is critical, and cannot be overemphasized.

Why is understanding TCP/IP so very important, you may ask? Computers themselves speak to each other across a network through the use of packets. In essence the base unit of communications in the world of computer networks is the packet. Packets themselves are most commonly built using the TCP/IP stack, which is part of the computer's operating system. Each operating system has some unique values coded into its implementation of the TCP/IP stack. This is how OS fingerprinting works, by studying these unique values such as MSS and MTU among others. It has been said before that to recognize the abnormal you must first understand what is normal. This is why we need to understand what a normal TCP/IP packet looks like and how TCP/IP itself sets up communications between computers.

By looking at actual packets which are sniffed off the wire using a packet capturing utility such as tcpdump or its win32 equivalent windump we can study what is normal behavior. We will see how when we double click on our web browser that there is a syn packet sent out and that a syn/ack packet comes back to us in turn. This is followed by an ack packet and it in turn is followed by a series of psh/ack packets which are used to exchange data back and forth between you and whatever server your homepage is set too.

It is through this study of basic TCP/IP concepts that you will be able to effectively troubleshoot computer network problems and diagnose possible anomalous behavior on your network. To elaborate further you will need to understand what the protocol ICMP is and what purpose it serves. From a security perspective these protocols are very important to understand. A great deal of hacking seen today involves buffer overflows and the bending or protocols.

You cannot be content to simply understand on a conceptual level what these protocols are. During an investigation you may be required to look at a possible case of ARP poisoning. To understand what it is that may or may not be going on you will first have to understand what ARP is and what role it plays on computer networks. Please note that I have not mentioned actual application layer protocols such as HTTP or SMTP yet. These protocols themselves are also very important to understand. They not only follow a set way to communicate, but also have a series of messages which are used to communicate certain conditions. For example; the ubiquitous 404 error message often seen while surfing the web.

The last part of TCP/IP that I will cover before going on to another skill is the actual study of packet metrics themselves. I mentioned above certain values that are used to identify operating systems. Values such as maximum segment size, and maximum transmission unit are but a few TCP/IP metrics that are normally always seen in packets. One will need to understand what each of these values means, and what is its purpose. Once you begin to study these values you will begin to see they are relationships between certain values such as say the window size and the maximum segment size. Being comfortable in looking at all these values and truly understanding what they all mean is very important. No more so is being able to decipher what all those hex values mean in a packet. Having the ability and skills to do this will allow you to analyze packets themselves for possible malicious content. No matter how clever the exploit developer is they still have to send that exploit to your computer via a packet and or packets. So as we can see gaining a very good understanding of TCP/IP is very much key to any network security professional.

Learning Intrusion Detection Systems (IDS)

Another central skill in the arsenal of a security professional is the administration, and upkeep of an intrusion detection system. This technology has slowly matured to a point where it is now pretty much indispensable. With the possible exception of a home user who only does the occasional surfing and sending of emails, most every computer, and certainly every corporate network, has computers offering various services. Having the best firewall ruleset in place will not do a thing for you to safeguard these services for they still have to be able to communicate. (application layer filtering being an exception) Shutting down access to port 80 simply is not possible if you are running a web server for your company's web presence.

This point is the point where the IDS begins to earn its keep, and where one has to be able to update and write rules if your system allows it, as well as interpret the IDS output. The output

of an IDS system are packets, which are logged once they are seen to match a specific signature, one which is part of that system's signature table. We are now once again coming back to TCP/IP for it will now be up to us to interpret what is going on with the packet that tripped this signature. You will have to look at those packets and interpret not only what is in the ASCII content portion but also interpret the hex values of the packet. In addition you will need to analyze the usual metrics such as the window size and TCP sequence numbers among others to make sure all is as it should be.

One of the problems though is that the IDS can produce an enormous amount of data that requires checking. A majority of these at first will probably be false positives -- these are alarms which are false but triggered anyway because they met some part of the signature. You cannot prove this is the case though till you have thoroughly checked the packet itself. It is well worth the effort to take the time to fine tune your IDS signatures, and take an inventory of services being offered on your network. This will help minimize the amount of false positives. For example there is no sense in having FTP signatures if you don't offer FTP services on your network, and by extension any other signatures enabled which don't apply to your network. Some IDS will let you write your own signatures, and this is a definite advantage. To take advantage of this though you will need to learn how to write them, and leverage your knowledge of TCP/IP to make the filter as effective as possible. Being able to write custom signatures for your computer network is a very useful ability. Many networks have certain quirks, and others have certain restrictions in place for employees using it. The ability to write customized ones is not a skill you should ignore.

The problem remains though that you still need to manage a massive volume of data. You can minimize this ocean of packets needing analysis by using bpf (Berkely Packet Filters) and bitmask filters. Having a knowledge of these two means of distilling information will allow you to quickly focus on the packets of interest. Once again though we are drawn back to knowledge of TCP/IP itself and how packets are put together to fully realize the potential of bpf and bitmask filters. There is simply no way of escaping TCP/IP and the requirement for a firm grounding in it as we can see. For example, say you have just had all of your company's web servers scanned. You wish to see if there was any exploit code pushed across to them. What you could do is use the scanning IP address and your company's subnet as a bpf filter to isolate the traffic. Furthermore you would tack on a bitmask which would show you only psh/acks which is were a payload would be. Having a means of filtering information that we want from a file that might have been 20MB to begin with, down to a manageable 50KB or so is not only an enormous savings in time, but also keeps the analyst from being worn down. That will also keep them fresh so that they do indeed see the truly hostile traffic, and don't become desensitized by a never-ending stream of packets to check.

Firewalls and routers

Most every network nowadays also has a firewall in place as well as routers to manage the traffic. I mention the two in the same breath for they both have similarities in the way they are managed. You should never obviously go with the default setting of either one of these appliances. Much as with an IDS you need to tweak the settings of these to suit the needs of your environment. For example if you bought a high end firewall which has anti DDoS technology such as handling connection attempts before handing them off to the internal network, you would want that enabled. What that means is you have to go and play with your new firewall at work and see what options it has, and how you should go about implementing

them. Firewalls largely though are fairly straightforward, and simple to configure. A rule of thumb is to deny all traffic, and then only explicitly allow the passing of traffic based on the organization's requirements.

What can be more difficult and intricate is the setting up of a router, and the writing of its ACL. Knowing how to properly configure such routing protocols like BGP, and OSPF if you have internal routers, can be quite tricky to set up correctly. Once the initial configuration is done though the router should only require minimal maintenance. The other tricky part of dealing with a router is the writing of ACLs to decide what is and is not allowed entry into your network. These rules have a syntax of their own which can be compared loosely to something like IPTables syntax. The placement and order of these rules is crucial to the security of your network so very careful attention is required when writing these. It is always best to have someone else look at your rules before you implement them. Having a second pair of eyes can save you from a potentially serious breach of your network due to a poorly written ACL.

Other skills

The last three skills that are important to have in your arsenal is the ability to at least read code, and ideally program a little bit. Being able to read code, and if necessary modify or debug programs and scripts is very important. You may land in a new job where you have inherited legacy scripts which need to be updated or fixed. Knowing how to debug code will also allow you to analyze, and study exploit code. Once you have it functional you can play with in a lab environment and see how it can affect your network assets. You should also have a very good grasp of the operating systems that are on your network as well. This will allow you to further tighten down the operating system itself to attack, and allow you to counter exploit code out there as well as any possible internal mischief. Finally, you should familiarize yourself with the concept of penetration testing, a term once known as ethical hacking. While the testing of vulnerabilities in systems, networks and applications can be a fine art in itself, there are many tools out there (such as Nessus) that security analysts can use to get a better understanding of the systems they are protecting.

Conclusion

As we can now see there are a great many skills required of the network security analyst if they are to be successful at their job. We have expanded on these skills to give some concrete examples, which will hopefully put them into context for you. The second part of this article will bring you through a simulated day in the life of a security analyst. You will see how all of these skills are actually used in what could very easily be a real life scenario. After having read the second part to this article what is needed and expected of you as a security professional should become clear.

Continue on to part two of this article series.

About the author

Don Parker is an Intrusion Detection Specialist who holds the GCIA certification. He works for Rigel Kent Security and Advisory Services as an instructor and also provides other computer security services of a highly specialized nature.

Comments or reprint requests can be sent to the editor.