Marshall Eddy

CS332-002

Vincent Skimmer

1 February 2017

TCP/IP Uses for a Penetration Tester

Good knowledge of networking and network protocols. Being able to list the OSI model does not qualify as knowing networking and network protocols. You must know TCP in and out. Not just that it stands for Transmission Control Protocol, but actually know that structure of the packet, know what’s in it, know how it works in detail. A good place to start is TCP/IP Illustrated by W. Richard Stevens (either edition works). Know the difference between TCP and UDP. Understand routing, be able to in detail describe how a packet gets from one place to another. Know how DNS works, and know it in detail. Understand ARP, how it’s used, why it’s used. Understand DHCP. What’s the process for getting an automatic IP address? What happens when you plug in? What type of traffic does your NIC generate when it’s plugged in and tries to get an automatically assigned address? Is it layer 2 traffic? Layer 3 traffic?

If you don’t understand the things in the previous paragraph, then you can’t possibly understand how an ARP Spoof or a MiTM attack actually works. In short how can you violate or manipulate a process, if you don’t even know how the process works, or worse, you don’t even know the process exists! Which brings me to the next point. In general, you should be curious as to how things work. I’ve evaluated some awesome products in the last 10 years, and honestly, after I see it work, the first thing that comes to my mind is “how does it work”.

Spoofing involves creation of TCP/IP packets using somebody else's Internet addresses and then sending the same to the targeted computer making it believe that it came from a trusted source. It is the act of using one machine to impersonate another. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. The destination machine only uses that source IP address when it responds back to the source. This technique is used in internal and external penetration testing to access computers that have been instructed to only reply to specific computers. This can result in sensitive information be released to unauthorized systems. IP spoofing is also an integral part of many network attacks that do not need to see responses (blind spoofing).

References

[SOURCES]