Global Information Assurance Certification Paper

Information Security Reconnaissance: Journey to Mordor[1]
(a.k.a. Know your Enemy)
Fred Hill
December 7, 2000

Are you 31337[2]? Do Hax0rs Ph33r j00? Can crackers access your K3wl pHil3z and steal your warez? Do you understand their mindset or even their jargon? Do you know where in both physical and cyber space the crackers and hackers lurk? Do you know where they get their "tools of the trade?" Are you dealing with a script kiddie or an elite cracker? How can you tell? Did you know that there are resources out there to "mentor" wannabe hackers along with pages that list all of the default passwords for commercial firewalls and routers?

This paper takes a look at some of those resources. Resources that not only help answer (or at least translate) the questions posed above, but also help us understand the mindsets of the individuals and groups who are pinging the ports of your firewalls. Crackers are successful because they are highly creative, think "outside the box," and don't play by the rules[3]. But don't ever be fooled into thinking that they don't know the rules. Many times it is their intense, in-depth understanding of the "rules" that allow them to penetrate your best defenses.

Here's a sample of the cracker mindset in applying the "rules" they do understand. Crackers know that finding a firewall means that there may be something of value behind it. Which begs the question "How do I find firewalls?" One cracker resource answers in the following manner:

"…
First, try to traceroute, from a UNIX-machine, to the machine you want to check. If the trace-route dies (hangs on the same routerhop forever...), it's probably because of a firewall. You could actually see if it is, by first seeing if a traceroute with ICMP-packets (such as a Windows tracert) goes through. If it does, it's definitely a firewall, or at least a filter of some sort. If it still does not get through, there MIGHT be a firewall OR the router is down for some unknown reason.

In that case, you try with a sort of special traceroute... Now, if your traceroute dies because of a filter, it's because the probes are coming from a port that the filter doesn't like. What you do then is that you try to mask your probes as something legitimate, like DNS-packets.

Now, the portnumber is incremented for each probe, and for each routerhop traceroute sends out 3 probes. What you want to achieve is for the portnumber to reach 53 exactly at the filter, so it thinks that the packets are DNS-packets.

The formula is: (target_port - (number_of_hops * num_of_probes)) – 1. So, let's say our traceroute died at the 8th routerhop, you would have to do a (53 - (8 * 3)) - 1 = 28

traceroute -p28 targethost …"[4]

(Are you thinking, "So what…so they found my firewall…I'm still safe?" If so read "Are Firewalls Enough?"[5] in the SANS Information Reading Room at http://www.sans.org .)

As the above example demonstrates, crackers have access to the same technical specifications, and security and vulnerability alerts that you do…they just react to them a little differently and with a lot more diligence, knowing that most vulnerabilities go unheeded for a long time[6].

To be a better information security professional, one must attempt to understand the hacker mindset by doing some information security reconnaissance. To really know your enemy, you must undertake a journey to Mordor…the land of shadows…the land of the cracker. (Note: Mordor was the "land of the shadow world" in J.R.R. Tolkien's classic trilogy titled "The Lord of the Rings.")

My personal journey along the road of information security began with a trip to the DefCon 7.0[7] Hacker conference in July of 1999. I was amazed. I thought I had flown to Las Vegas, Nevada. Instead I had landed at the portal to a parallel universe. Here there were sessions on hacking operating systems, hacking passwords, and hacking people (social engineering) along with presentations on how to steal someone else's identity (including a discussion of the "legitimate" reasons for changing your identity) and a highly animated stage production by the Cult of the Dead Cow (creators of the infamous BackOrifice) announcing the release of BO2K!

While the underlying theme was basically "hack the planet," there were also sessions on IPv6, TCP/IP, cryptography, cyber forensics, and defense measures. The vendor booths offered fake ID cards (e.g. driver's licenses for any state in the US), lock picking demonstrations, telephone equipment of questionable origin, books and magazines on hacking, and various incantations of UNIX open source OS's. Conference events included "Spot the Fed," "Hacker Death Match," "Capture the Flag (LAN style)," and the 'Black and White Ball." The general attire ran the gamut from your standard black Goth style to white robes with multi colored Mohawk hairstyles, however the majority wore cut offs, jeans, and shorts (July in Las Vegas is HOT!)

I left DefCon 7.0 with the feeling that no system is ever really secure. For me it was a brief glance into the world of the cracker and a glimmer of insight into the cracker mentality. To gain more insight I began exploring the various online resources for computer security and hackers. Below are two charts detailing some of the sites and events that I've encountered on my journey to Mordor. Far from being exhaustive lists, they are at least a first step toward information security reconnaissance.

Warning and disclaimer: Most of these sites will trigger the alarms of many firewall and content filtering systems (probably with good reason). Use discretion when accessing. Use even more (read: extreme) caution if you download anything from these sites.

Internet hacker related resources are:

URL	Description
http://www.insecure.org/	Great source for tools (nmap, crack, etc.), news, and stuff.
http://www.nmrc.org/	Even more hardcore stuff
http://packetstorm.securify.com/index.shtml	"An online security library." Great source for almost anything security related.
http://www.2600.com/	The original hacker and phone phreak site.
http://phrack.infonexus.com/	The current hackers site
http://www.hackernews.com/	Commercial version of a hacker info page.
http://freshmeat.net/	Not necessarily for hackers but great stuff for Linux
http://www.l0pht.com/	Security/hacker Power Tools for NT
http://www.tcpdump.org/	Indispensable tool for TCP sniffing
http://netgroup-serv.polito.it/winpcap/2.1beta.htm	Basically tcpdump for windows

Hacker Conferences:

URL	Description
http://www.defcon.org	A must see, must do event.
http://www.atlantacon.com/	"…a convention held April Fool's weekend in Atlanta for technology addicts, computer enthusiasts. Security professionals, hackers, gamers, and geeks hosted by a few masochistic individuals who fit somewhere into the above description."
http://www.rubi-con.org/	Basically DefCon in Detroit
http://www.h2k.net	H.O.P.E. – Hackers on Planet Earth (a 2600 Event)

---

[1] Tolkien, J.R.R. "The Lord of the Rings." (trilogy) 1955

[2]Author unknown. "Jargon File 4.2.0". 31 Jan. 2000 URL: http://www.science.uva.nl/~mes/jargon/ (5 Dec. 2000)

[3] Daintry, Duffy. "Meet the Hackers" Dec. 2000. URL: http://www.darwinmag.com/read/10100/hackers.html (5 Dec. 2000)

[4] Andersson, Marcus. "Newbie FAQ" Version 1.0. 08 Aug. 2000. URL: http://209.143.242.119/cgi-bin/cbmc/forums.cgi?faq=defined#newbie (1 Dec. 2000)

[5] Giannoulis, Peter. "Are Firewalls Enough?" September 11, 2000. URL: http://www.sans.org/infosecFAQ/firewalls_enough.htm. (6 Dec. 2000)

[6] Arbaugh, William A., Fithen,William L., and McHugh, John. "Windows of Vulnerability: A Case Study Analysis," Computer Vol. 33 pub 12 (Dec 2000) (http://computer.org) (4 Dec. 2000)

[7] alias Buster, Bronc. "Hackerz, Phreakerz and Fedz: Three Days of Fear and Loathing in Las Vegas" July 1999. URL: http://www.thesynthesis.com/tech/defcon/vii.html (4 Dec. 2000)