

Re: Honeypot detection and countermeasures

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-06/0128.html>

From: Henry O. Farad (*lrcrypto_at_red4est.com*)

Date: 06/24/03

Date: Tue, 24 Jun 2003 12:19:58 -0700

To: pen-test@securityfocus.com

I've seen some interesting stuff on this thread. On the premise that the best way to get an answer on the internet is to post the wrong answer, I'll try to summarize what I think I've seen people say.

1) On pen-testing and honeypots:

This is the question I asked, rather than the one that I meant to ask. In many cases, the customer will say "Don't bother attacking these systems, they are honeypots". In this case the pen tester will end up testing the security of the "production machines" without wasting time on the honeypots. However, this will not test the system as a whole, since the honeypots are part of the complete security scenario.

2) Low hanging fruit is suspicious:

This is getting in to what Lance referred to as his tiered strategy. A system that is easy to break into will be more tempting to a less experienced intruder, and more suspicious to an experienced intruder. If a system is easier to break into, there should be a plausible reason. For example, maybe it's patches are a couple of weeks out of date. One may want to apply security patches to the honeypots last, but do eventually apply them. Unless, of course, you are using it as bait for the careless intruder, or are trying to distract from your "real" honeypot.

Question: what plausible reasons might there be for a less secure system on the net? Are machines that people just "forgot about" all that common?

3) Professionals won't do a portscan once they are inside a network.

While it is common for machines exposed to the outside to be portscanned, portscans on the internal network tend to raise alarms. Therefore, if a machine does not get any traffic, the professional either may not see it, or will be suspicious of it. There would have to be a plausible reason for a company to invest

SecurityFocus Penetration: Re: Honeypot detection and countermeasures

in a machine that doesn't appear to be used. Perhaps it is used for testing new revisions of the website, but lies fallow when not being used for such.

Question: Do people often share an IP address between a production machine and a honeypot when the production machine is not in use. For example test machines.

4) Many honeypots have easily detected signatures

Dave Aitel gave some specifics for VMWare (though there are other reasons for having a VMWare machine than just a honeypot). John Lampe mentioned that other systems have signatures (Mantrap). Unfortunately when I tried to google for more information on this subject, it pretty much just pointed me to this thread.

However, it seems that while it is possible to detect a lot of these honeypots, many pentesters, and we may assume intruders, don't check for them.

Question: Do you ever get caught by honeypots? Either get busted in the middle of a pen-test, or have the customer tell you after the fact that you were caught?

5) What about using a honeypot as an intrusion resource?

Sure it's a honeypot, but it may be configured to be more vulnerable. Do you ever use a honeypot that you find as an attack point for other systems?

What about using it as a distraction? Do some noisy attacks to and from the honeypots, while simultaneously, you quietly attack another system?

I think that this is long enough for now. I greatly appreciate all of the thoughtful discussion I've seen on this subject.

Larry

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team? Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Visit us at: www.coresecurity.com/promos/sf_ept1
or call 617-399-6980
