Aufspüren von Honeypots / Honeywalls

© Amir Alsbih
alsbiha@informatik.uni-freiburg.de

28.03.2006

Honeypots / Honeywalls – How to seek them out

Honeypots[1] werden verwendet um die Angriffe und Vorgehensweise von Hackern zu studieren.
Die Grundidee dabei, in einem Netzwerk einen oder mehrere spezielle Server (Honeypots) zu platzieren.
Da ein Angreifer; der nicht zwischen echten Servern/Diensten und Honeypots unterscheiden kann; routinemäßig alle Netzkomponenten auf Schwachstellen untersucht, wird dieser früher oder später, die von einem Honeypot angebotenen Dienste in Anspruch nehmen, dabei werden sämtliche Aktivitäten von dem Honeypot protokolliert.
Hackt er also diesen Honeypot können all seine Aktivitäten ausgewertet werden und daraus Schlussfolgerungen und Analysen erstellt werden.

Damit man einen Honeypot nicht zum weiterhacken in andere Netze oder Rechner verwenden kann, wird das Netz in dem sich die Honeypots befinden durch eine Honeywall[2](Transparente Brücke, die den Traffic zu und von den Honeypots überwacht) gesichert, die den Verkehr überwacht und dabei Angriffe nach aussen herausfiltert.

Genau hier setzt das Verfahren an, man schickt einfach einen Ping mit einem Datenpacket das einen Shellcode enthält; dafür kann man z.B. hping2[3] verwenden; an den Server und vergleicht das ausgehende ICMP Packet mit der Rückgabe des Servers (mittels Tcpdump[4] oder Ethereal[5]) .
Erhält man keine Antwort auf einen Ping mit Shellcode, oder ein verändertes Datenpacket, dann handelt es sich bei dem Server um einen Honeypot, der durch eine Honeywall gesichert wird.

Am besten man schickt zuvor einen Ping mit einem Packet ohne Shellcode um zu testen ob der Server überhaupt auf Pings reagiert.
Letztenendes kann man jedoch nach diesem Schema jeden Dienst zum testen auf eine Honeywall verwenden, der die gleichen Daten zurückliefern muss, wie die, die er bekamm.

Schickt man also ein ICMP Packet mit dem Datenpacket **Security** an den Honeypot, so sieht man dass man keinen Packetlost hat und mittels Etheral auch, dass es sich um den selben Inhalt handelt:

1 http://www.honeynet.org/
2 http://www.honeynet.org/tools/cdrom/
3 http://www.hping.org/
4 http://www.tcpdump.org/
5 http://www.ethereal.com/

© Amir Alsbih – alsbiha@informatik.uni-freiburg.de

```
#hping2 -1 -d 5 -E testpacket.txt -c 1 10.0.0.20
HPING 10.0.0.20 (eth0 10.0.0.20): icmp mode set, 28 headers + 5 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=10.0.0.20 ttl=64 id=3471 icmp_seq=0 rtt=1.2 ms

--- 10.0.0.20 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.2/1.2 ms
```

Sendet man nun hingegen ein Packet mit einem **Shellcode**, so bekommt man entweder keine Antwort oder aber ein Datenpacket dessen Inhalt sich geändert hat:

```
#hping2 -1 -d 45 -E shellcode.txt -c 1 10.0.0.20
HPING 10.0.0.20 (eth0 10.0.0.20): icmp mode set, 28 headers + 45 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!

--- 10.0.0.20 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Getest wurde dieses Verfahren mit der Honeywall RO-1.0.hw-189.

Ich danke Herrn Marcello Bellini vom Max-Planck-Institut für auslaendisches und internationales Strafrecht, für seine Unterstützung. Herr Bellini stellte mir freundlicherweise ein Netzwerk mit Honeywall und Honeypots zur Verfügung.

Honeypots / Honeywalls – How to seek them out

To study the proceedings and attacks from hackers, Honeypots are used.
The idea thereby is, to put one or more special servers (Honeypots[6]) in a network . An aggressor; who cannot differentiate between genuine server/services and honeypots; sooner or later will be taken up the services offered by a Honeypot by his search for a safety gap.
All his activities on the honeypot are loged thereby.
So if an hacker, hacks into an Honeypot all his activities could evaluated and from it consequences and proceedings will be concluded.

Thus that one who hacked in a honeypot not uses it to hack other systems, the network that contains the honeypot, is secured by a Honeywall[7] (transparente bridge, which supervises the traffic to and from the Honeypots), that filters outward-attacks.

The procedure sets exactly here, one simply sends a Ping with a datapacket that contains a shellcode with e.g. hping2[8] to the server and compares the outgoing ICMP packet with the one returns by the server (with tcpdump[9] or ethereal[10]).
If the server does not send an answer to a ping that contains a shellcode, or changed the responsed datapacket (shellcode), then the server is protected with a honeywall.

The best proceeding is, sending a ping with a packet without a shellcode to test if the server response to pings. If he does, sending a packet with a shellcode, if then there comes no response or a modified packet, then it is a network protected by a honeywall.

Sending an ICMP packet that contains the word e.g. **Security** to a Honeypot will result in no packet loss. And ethereal will show that the response packet contains the same that we have send:

```
#hping2 -1 -d 5 -E testpacket.txt -c 1 10.0.0.20
HPING 10.0.0.20 (eth0 10.0.0.20): icmp mode set, 28 headers + 5 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=10.0.0.20 ttl=64 id=3471 icmp_seq=0 rtt=1.2 ms

--- 10.0.0.20 hping statistic ---
```

6 http://www.honeynet.org/
7 http://www.honeynet.org/tools/cdrom/
8 http://www.hping.org/
9 http://www.tcpdump.org/
10 http://www.ethereal.com/

```
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.2/1.2 ms
```

But if we now sending a packet that contains a **shellcode**, so we will get no response or we will get a packet that contains a different content:

```
#hping2 -1 -d 45 -E shellcode.txt -c 1 10.0.0.20
HPING 10.0.0.20 (eth0 10.0.0.20): icmp mode set, 28 headers + 45 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!

--- 10.0.0.20 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

This has been tested on the Honeywall RO-1.0.hw-189.

I thank Mr. Marcello Bellini from the Max-Planck-Institut for foreign and international criminal law, for his support.
Mr. Bellini kindly provides me a network with a Honeywall and Honeypots for my testings.