

A DETAILED GUIDE ON HONEYPOTS

WWW.HACKINGARTICLES.IN

Contents

Introduction	3
What are honeypots?	3
Working of honeypots	3
Types of Honeypots	4
Windows System	7
Android Honeypot	14
Linux Honeypot	24



Introduction

Honeypots are generally hardware or software that are deployed by the security departments of any organization to examine the threats that are possessed by the attackers. Honeypots usually act as baits for an organization to gather information on the attacker and alongside protect the real target system.



What are honeypots?

Honeypots are a type of Internet security resource that is used to entice cybercriminals to deceive them when they try to intrude into the network for any illegal use. These honeypots are generally set up to understand the activities of the attacker in the network so that the organisation can come up with stronger prevention methods against these intrusions. The honeypots do not carry any valuable data as they are faked proxies that help in logging the network traffic.

Working of honeypots

As an IT administrator, you would want to set up a honeypot system that might look like a genuine system to the outside world. The kind of data that honeypots generally capture:

- Keystrokes entered and typed by the attacker.
- The IP address of the attacker
- The usernames and different privileges used by the attackers
- The type of data that the attacker had accessed, deleted or that was altered.



Types of Honeypots

TYPES OF HONEYPOT

[Based on the design]

- Low-interaction Honeypots
- Medium-interaction Honeypots
- High-interaction Honeypots
- Pure Honeypots

@HackingArticles

Low-Interaction Honeypots:

They match a very limited number of services and applications that are present on the network or on the system. This type of honeypot can be used to keep track of UDP, TCP, and ICMP ports and services. Here we make use of fake databases, data, files, etc. as bait to trap attackers to understand the attacks that would happen in real-time. Examples of a few low-interaction tools are **Honeytrap**, **Specter**, **KFsensor**, etc.

Medium-Interaction Honeypots:

They are based on imitating real-time operating systems and have all the applications and services of a target network. They tend to capture more information as their purpose is to stall the attacker so that the organisation gets more time to respond appropriately to the threat. Examples of a few medium-interaction tools are **Cowrie, HoneyPy, etc.**

High-Interaction Honeypots:

They are genuine vulnerable software that is run on a real operating system with various applications that a production system would generally have. The information gathered using these honeypots is more resourceful, but they are difficult to maintain. An example of a high-interaction tool is the **honeynet**.

Pure Honeypots:



These honeypots usually imitate the actual production environment of an organization, which makes an attacker assume it to be a genuine one and invest more time exploiting it. Once the attacker tries to find the vulnerabilities, the organisation will be alerted, and hence any kind of attack can be prevented earlier.



Production Honeypots:

These honeypots are usually installed in the organization's actual production network. They also help in finding any internal vulnerabilities or attacks as they are present in the network internally.

Research Honeypots:

They are high-interaction honeypots, but they are set up with a focus of research in the areas of various governmental or military organisations to gain more knowledge about the behaviour of the attackers.





Malware Honeypots:

They are the kind of honeypots that are used to trap malware in a network. Their purpose is to attract the attacker or any malicious software and allow them to perform certain attacks that can be used to understand the pattern of the attack.

Email Honeypots:

These honeypots are hoax email addresses that are used to attract attackers across the internet. The emails that are received by any malicious actor can be monitored and examined and can be used to help the fall for phishing email scams.

Database Honeypots:

These honeypots pose as actual databases that are vulnerable in name and usually attract attacks like SQL injections. They are meant to lure the attackers into thinking that they might contain sensitive information like credit card details, which will let the organisation understand the pattern of the attacks they have performed.

Spider Honeypots:

These honeypots are installed with the purpose of trapping the various web crawlers and spiders that tend to steal important information from the web applications.

Spam Honeypots:

These honeypots consist of hoax email servers to attract spammers to exploit vulnerable email elements and give details about the activities performed by them.



Honeynets:

these are nothing but a network of honeypots which are installed in a virtual and isolated environment along with various servers to record the activities of the attackers and understand the potential threats.

Honeypots can be deployed in various environments. Today we will see the installation and working of honeypots in the Windows, Android, and Linux environments.

Windows System

Today we will be looking at the famous honeypot software called HoneyBOT. which can be downloaded **here**. Start Kali Linux as the attacker machine and your Windows system as the host machine.

Let us first do an nmap scan on the host machine when the honeypot is not installed.

nmap -sV 192.168.1.17

root@kali	:~# nn	ap -sV 192.168	3.1.17 🚽 🗕				root@kali:~# nmap -sV 192.168.1.17 🔫 🗕				
Starting	Nmap 7	7.91 (https://	<pre>nmap.org)</pre>	at 2020	-11-13 (07:19	EST				
Nmap scan	repor	t for 192.168.	1.17								
Host is u	ıp (0.0	0027s latency)).								
Not shown	: 996	closed ports									
PORT	STATE	SERVICE	VERSION								
135/tcp	open	msrpc	Microsoft N	Windows	RPC						
139/tcp	open	netbios-ssn	Microsoft N	Windows	netbios	-ssn					
445/tcp	open	microsoft-ds?									
3389/tcp open ms-wbt-server Microsoft Terminal Services											
MAC Address: 00:0C:29:54:91:59 (VMware)											
Service I	info: C)S: Windows; CF	PE: cpe:/o:r	microsof	t:windo	NS					

Now on your Windows system, install the HoneyBOT software and configure it. Click on "yes" to proceed.



😭 Н	oneyBO	Т						
File	View	Reports	Help					
				3	ه ال	8 🥖	2	
	Ports			Date	Time		Remote IP	Remote P
ł	HoneyB(TC Would	you like	to configure	HoneyBOT	×		
				Yes		No		

Check all the parameters that you want in your honeypot and click on Apply to proceed.

🍓 Options	Х
General Email Alert Exports Updates	
 Auto Start on Load Enable Sound Alert Capture Binaries Automatically Rotate Log 	
Enter the alias name that HoneyBOT will operate under. Server Name public08	
OK Cancel Apply	

To get email reports on your honeypot, add the recipient's email address and click on "Apply."



🍓 Options	×
General Email Alert Exports Updates	
Sends a daily summary to your email address. 'Autom Rotate Log' must be enabled to activate this feature.	atically
Send Email Alerts	
Email Server Enter your mail server address	
Server Port 25	
Recipient Address Enter your email address	
OK Cancel	Apply

If you want to save the honeypot logs in CSV format, you can use this setting.

🍓 Options	\times				
General Email Alert Exports Updates					
Exports your log files to CSV format. 'Automatically Rotate Log' must be enabled to activate this feature. Export Logs to CSV Uploads your log files to the central reporting server. 'Automatically Rotate Log' must be enabled to activate this feature.					
Upload Logs to Server					
Note: Log files are used to create aggregate reports of attack trends. No information that could identify the IP address of a HoneyBOT sensor is published in these reports.					
OK Cancel Apply					

On the attacker's machine, performs a nmap scan, and there you will see so many fake services that are open due to the presence of the honeypot in the system.



root@kali:	:∼# nma	ap 192.168.1.17 🔫——
Starting M	Vmap 7	.91 (https://nmap.org) at 2020-11-13 08:24 EST
Nmap scan	report	t for 192.168.1.17
Host is up	o (0.00	0084s latency).
Not shown	: 752 (closed ports
PORT 0	STATE	SERVICE
1/tcp	open	tcpmux
3/tcp	open	compressnet
4/tcp	open	unknown
6/tcp	open	unknown
7/tcp	open	echo
9/tcp	open	discard
13/tcn	open	davtime
17/tcn	onen	aotd
10/tcn	open	chargen
20/tcp	open	ftn-data
21/tcp	open	ftn
22/tcp	open	sch
22/tcp	open	telnet
25/tcp	open	cecilec
24/ CCP	open	smtp
23/tcp	open	den
27/tep	open	usp time
37/1Cp	open	
42/tcp	open	nameserver
43/LCP	open	
49/tcp	open	tacacs
53/tcp	open	domain
70/tcp	open	gopner
/9/tcp	open	tinger
80/tcp	open	nttp
81/tcp	open	nosts2-ns
82/tcp	open	xter
83/tcp	open	mit-ml-dev
84/tcp	open	ctf
85/tcp	open	mit-ml-dev
88/tcp	open	kerberos-sec
89/tcp	open	su-mit-tg
90/tcp	open	dnsix
99/tcp	open	metagram
100/tcp	open	newacct
106/tcp	open	pop3pw
109/tcp	open	pop2
110/tcp	open	pop3
111/tcp	open	rpcbind
113/tcp	open	ident
119/tcp	open	nntp
125/tcp	open	locus-map
135/tcp	open	msrpc



Let us try connecting via FTP from the attacker machine to the host machine.



As you see, a log has been generated of the attacker's IP and the port that he was connected to.



😭 HoneyBOT - Log_20201113.b	in						_	
File View Reports Help								
) 🗞 🖌) 🕺 🥖	2					
	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
🖻 Remotes	11/13/2020	5:31:10 AM	192.168.1.9	48000	192.168.1.17	21	TCP	41
4- <mark>192.168.1.9</mark>	11/13/2020	5:32:03 AM	192.168.1.9	48006	192.168.1.17	21	TCP	41

Here you can see a detailed report on the connection that was created by the attacker.

😭 Packet Log (ftp)					_	\times
Connection Details:	Packet His	tory				
Date: 11/13/2020 COMPUTE: GFS Time: 5:32:03 AM Millisecond: 671 Time Zone: -8:00 Source IP: 192.168.1.9 Source Port: 48006 Server IP: 192.168.1.17 Server Port: 21 (ftp) Protocol: TCP Bytes Sent: 41 Bytes Received: 0	Time 5:32:03 AM 5:32:03 AM	Direction RX TX	Bytes 0 41	Data SYN 220 PUBLIC08 FTP Service (Version 5.0).		2
Packet Data:						-
View as 💿 text						
⊖ hex						
<< < > >>						

Similarly, an SSH connection was initiated on port 22 from another operating system.



Command Prompt

Connection-specif Link-local IPv6 A IPv4 Address Subnet Mask Default Gateway . Refault Configuration Category:	ic DNS Suffix . : address : fe80::a : 192.168 : 255.255 : 192.168	a100:b097:1971:cfb4%17 3.1.3 5.255.0 3.1.1 ? ×
- Session	Basic options for your PuTTY se	ession
Logging	Specify the destination you want to conne	22:4832%20
	Host Name (or IP address)	Port
Keyboard	192.168.1.17	22
Bell	Connection type:	
	ORaw OTelnet ORlogin ● SSI	H O Serial
	Load, save or delete a stored session Saved Sessions	
Colours	Default Settings	Load
Data		Save
Proxy Telnet		Delete
Riogin		
terial	Close window on exit: Always Never Only on c	clean exit
About Help	Open	Cancel

Now you can see that a log for the same has been generated for the connection created on port 22.





Android Honeypot

The honeypots can also be installed on Android phones using the Google Play store. Here we have downloaded the Hostage honeypot.







On switching on the application, it looks safe.







Now let us check the IP address of your android device and let's proceed.







Let's turn on the attacker's system and let's conduct an nmap scan on the IP address of the android device.

```
root@kali:~# nmap 192.168.1.14 _____
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-13 08:47 EST
Nmap scan report for 192.168.1.14
Host is up (0.0025s latency). ______
Not shown: 995 closed ports
PORT STATE SERVICE
1025/tcp open NFS-or-IIS
2222/tcp open EtherNetIP-1
3306/tcp open mysql
8080/tcp open bttp proxy
```

An alert will be generated on the android device when the nmap scan is connected.







A log will be created and we will see the IP of the attacker system and the ports that were attacked.



7:23 🎐	傘 と	*	V&WiFi2
< <	<unknown s<="" th=""><th>sid></th><th></th></unknown>	sid>	
CONVERS	ATION		
RECEIVED	from 192.168.1 11/13/20 at 7: CREATED	.9:577 <u>82 to 19</u> 17 PM TEXT	92.168.1.14:1025
RECEIVED	from 192.168.1 11/13/20 at 7: CLOSED	.9:577 <u>82 to 19</u> 17 PM TEXT	92.168.1.14:1025 HEX
RECEIVED	from 192.168.1 11/13/20 at 7: CLOSED	.9:577 <u>82 to 19</u> 17 PM TEXT	92.168.1.14:1025 HEX
RECEIVED	from 192.168.1 11/13/20 at 7: CLOSED	.9:577 <u>82 to 19</u> 17 PM TEXT	92.168.1.14:1025
RECEIVED	from 192.168.1 11/13/20 at 7: CLOSED	.9:57782 to 19 17 PM TEXT	92.168.1.14:1025 HEX
RECEIVED	from 192.168.1 11/13/20 at 7: CLOSED	.9:57782 to 19 17 PM TEXT	92.168.1.14:1025 HEX
RECEIVED	from 192.168.1 11/13/20 at 7: CLOSED	.9:57782 to 19 17 PM TEXT	92.168.1.14:1025
			Û
	\bigtriangledown	0	0



Linux Honeypot

We can install a honeypot on a Linux machine as well. Here we have demonstrated using Pentox, which can be easily installed on Ubuntu.

wget http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz tar -zxvf pentbox-1.8.tar.gz

root@ubuntu:~# wget http://downloads.sourceforge.net 2020-11-14 11:01:16 http://downloads.sourcefor Resolving downloads.sourceforge.net (downloads.sour Connecting to downloads.sourceforge.net (downloads HTTP request sent, awaiting response 302 Found Location: https://excellmedia.dl.sourceforge.net/pi 2020-11-14 11:01:16 https://excellmedia.dl.sour Resolving excellmedia.dl.sourceforge.net (excellmed Connecting to excellmedia.dl.sourceforge.net (excellmed HTTP request sent, awaiting response 200 OK Length: 1550930 (1.5M) [application/x-gzip] Saving to: 'pentbox-1.8.tar.gz'	et/project/pentbox18realised/pentbox-1.8.tar.gz rge.net/project/pentbox18realised/pentbox-1.8.tar.gz rceforge.net) 216.105.38.13 sourceforge.net) 216.105.38.13 :80 connected. roject/pentbox18realised/pentbox-1.8.tar.gz [following] urceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz jia.dl.sourceforge.net) 202.153.32.19 Llmedia.dl.sourceforge.net) 202.153.32.19 :443 connected.
pentbox-1.8.tar.gz	100%[
2020-11-14 11:01:22 (2.90 MB/s) - 'pentbox-1.8.tar	.gz' saved [1550930/1550930]
<pre>root@ubuntu:~# tar -zxvf pentbox-1.8.tar.gz pentbox-1.8/lib/racket/racket/l2/.svn/text-base/lub pentbox-1.8/lib/racket/racket/l2/.svn/text-base/lub pentbox-1.8/lib/racket/racket/l2/.svn/text-base/vtp pentbox-1.8/lib/racket/racket/l2/.svn/text-base/mti pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eig pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eig pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eig pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eig pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eig pentbox-1.8/lib/racket/racket/l2/.svn/text-base/eig pentbox-1.8/lib/racket/racket/l2/.svn/prop-base/llb</pre>	rb.svn-base an.rb.svn-base ap.rb.svn-base o.rb.svn-base sc.rb.svn-base ghtotwodotthree.rb.svn-base mernet.rb.svn-base rb.svn-base an.rb.svn-base

Once it is installed, let us start using the pentbox. Select the network tools and honeypot from the menu to install the honeypot. Go along with the manual configuration to install it according to your preferences for a honeypot.

./pentbox.rb



root@ubuntu:~/pentbox-1.8# ./pentbox.rb
PenTBox 1.8
Menu ruby2.7.0 @ x86_64-linux-gnu
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit
-> 2
1- Net DoS Tester 2- TCP port scanner 3- Honeypot 4- Fuzzer 5- DNS and host gathering 6- MAC address geolocation (samy.pl)
0- Back
-> 3
// Honeypot //
You must run PenTBox with root privileges.
Select option.
1- Fast Auto Configuration 2- Manual Configuration [Advanced Users, more options]
-> 2



Now you can open the fake port according to your preference and insert a fake message. You can also provide the option to save the log and save the name of the log. You can see that the honeypot is activated on the required port, and similarly, you can manually activate honeypots for other ports.



Turn on the attacker's machine, and scan the host machine using nmap. The results of the open ports and services are displayed below.



Here, the attacker machine is trying to connect with the host machine using telnet.



telnet 192.168.1.108

```
root@kali:~# telnet 192.168.1.108 
Trying 192.168.1.108 ...
Connected to 192.168.1.108.
Escape character is '^]'.
Join Ignite TechnologiesConnection closed by foreign host.
root@kali:~#
```

For every attempt of intrusion that is made, it gets alerted and a log is created where the attacker's IP and port are recorded.







JOIN OUR TRAINING PROGRAMS



in 😱

www.ignitetechnologies.in