



Introduction to Honeypots
By
Ahmed AL Mutairi

Introduction:

في هذا البحث سوف نتحدث عن احدى التقنيات المستخدمة في تحليل هجمات القرصنة وكذلك اصطبادهم وهي HoneyPOT وتتمحور التقنيه في عمل بينه مناسبه للمخترق بحيث توهمه انها ممكنة الاختراق بهدف تحفيز المهاجم للجھوم على النظام و مما لاشك فيه ان هناك انواع يتم على اساسها عمل هذه التجربه واطلاقها في الانترنت

Honeypot Types :

تنقسم انواع هذه التقنيه على اسس مختلفه وهي الاستخدام او طريقة عملها وسوف نقسمها على حسب طريقه عملها وذلك لان مايريد من هذه التقنيه هي النتيجه وللوصول الى النتيجه المراده وتخطي العقبات يجب معرفة طريقه عملها وعلى هذا الاساس سوف نستخدمه تنقسم التقنيه على المبدء الثاني الى ثلاث اقسام سنتطرق الي قسمين منها مع الامثله

1- Pure Honeypots :

في هذا النوع يكون النظام كامل ولا يحتاج الي اي اداة اضافيه ويكون عمله مراقبه وتسجيل تحركات المهاجم دون علمه

2- Low-interaction honeypots :

في هذا النوع يكون دقيق اكثر من النوع السابق بحيث يكون اختيارنا مقصور على خدمه معينه يكون اختيارنا لها لكثره الاختراق من خلالها مثلا في HTTP - FTP - SSH ..etc

-Tools :

قبل الانتقال الى الجانب العملي سأتطرق الي اهم الادوات التي ممكن استخدامها في هذان النوعان من هذه التقنيه

1- HoneyD :

في هذه الاداه يتم عمل انظمه وهميه كامله وشامله وتصنف من النوع Pure HoneyPots

2-HoneyBOT:

في هذه الاداه تشمل النوعين الاول والثاني بحيث يمكنك عمل على خدمه معينه ومراقبتها او على النظام كله وهي خاصه لانظمه الويندوز

3-Pentbox

هذه الاداه هي شامله لعدة خدمات تقدمها تم كتابتها بلغه Ruby ولكن مايهيها هي خاصه واحده من خلالها يمكننا مراقبه اي منفذ ومراقبه الطلبات المشبوهه التي تتم من خلاله

- Practical Part :

الآن سوف نتطرق الى الجانب العملي من هذا البحث وتم تركيب الادوات المذكوره مسبقا وفي كل مره تتم تشغيل هذه الادوات يتم اختبارها بعدة ادوات منها **Nmap and Nessus** للتمكن من معرفه قوة هذه الاداه وسوف نتطرق للجزء الاول من هذه العمليه مع الاداه **Pentbox**

```
PentBox 1.8
PentBox
----- Menu          ruby2.3.3 @ 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
Insert port to Open.
[ -> 80
Insert false message to show.
-> Hello Mr.hacker
```

بعد تشغيل الاداه ننتظر التحرك من المهاجم لكي نشاهد ماذا يمكنه عمله



Hello Mr.hacker

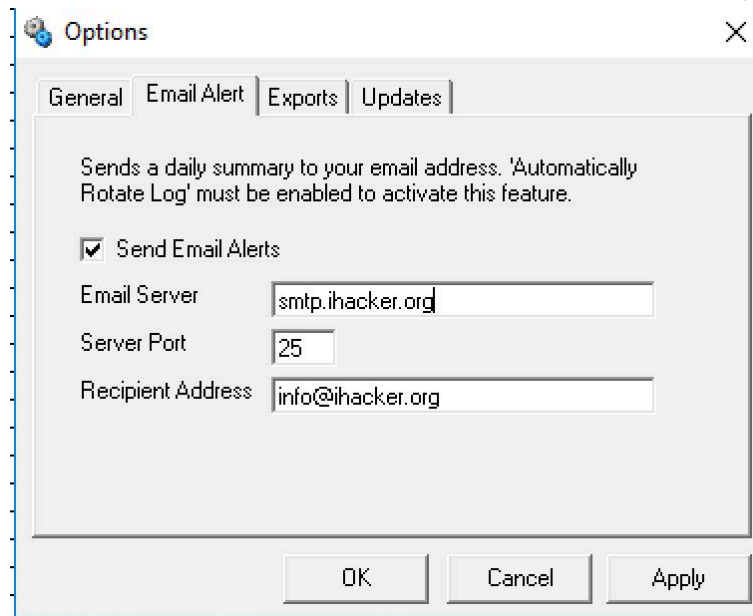
```
GET /index.php?id=asas%27%20union%20select HTTP/1.1
Host: 192.168.1.10:80
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----
INTRUSION ATTEMPT DETECTED! from 192.168.1.10:54054 (2017-06-23 17:37:52 -0400)
-----
GET / HTTP/1.1
Host: 192.168.1.10:80
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

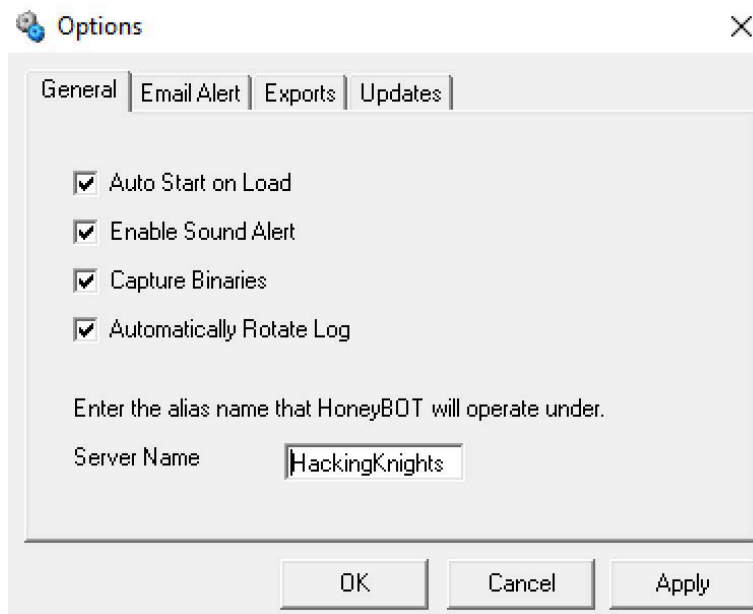
Practical Part #2 :

HoneyPOT On Windows في هذا الجزء سيختلف نوع التقنيه المستخدمه وتشمل النظام كله والاداه المستخدمه

بعد تثبيتنا للاداه نشغلها وننتظر الهجوم والجميل في هذه الاداه نستطيع ان نجعلها ترسل لنا عبر البريد الالكتروني في حال وجود هجوم وذلك عن طريق الاعدادات



وكذلك يمكننا التحكم بالخدمات التي نريد اظهارها او اسم النظام او اضافته جديده



Nessus بعد تواجد الهجوم نرى في البدايه ماهي النتائج من عمليه البحث عن الثغرات في مشروع

← Back to Testing HoneyPOT

Sev	Name	Family	Count
●	Microsoft Windows/Exchange SMTP DNS Lookup Overflow (88...	SMTP problems	1
●	Service Detection (HELP Request)	Service detection	2
●	NetBus 1.x Software Detection	Backdoors	1
●	Check Point FireWall-1 Identification	Firewalls	3
●	MS10-024: Vulnerabilities in Microsoft Exchange and Windows ...	SMTP problems	1
●	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	General	1
●	SSL Certificate Cannot Be Trusted	General	1
●	SSL Medium Strength Cipher Suites Supported	General	1

Host Details

IP: 157.140.2.27
 OS: Microsoft Windows 10
 Start: Today at 5:43 PM
 End: Today at 6:25 PM
 Elapsed: 42 minutes
 KB: [Download](#)

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

نرى ان هناك العديد من الثغرات المصاب بها النظام وذلك هو عمل الاداه خداع المهاجم والان نرى من النتائج من عمليه البحث عن طريق Nmap

```

Not shown: 721 closed ports
PORT      STATE    SERVICE          VERSION
1/tcp     open    tcpmux?
| auth-owners: ERROR: Script execution failed (use -d to debug)
3/tcp     open    compressnet?
| auth-owners: ERROR: Script execution failed (use -d to debug)
4/tcp     open    unknown
| auth-owners: ERROR: Script execution failed (use -d to debug)
6/tcp     open    unknown
| auth-owners: ERROR: Script execution failed (use -d to debug)
7/tcp     open    reverse-ssl     SSL/TLS ClientHello
| auth-owners: ERROR: Script execution failed (use -d to debug)
| fingerprint-strings:
|_  DNSVersionBindReq:
|_  version
|_  bind
|_  GetRequest:
|_  GET / HTTP/1.0
|_  HTTPOptions:
|_  OPTIONS / HTTP/1.0
|_  RTSPRequest:
|_  OPTIONS / RTSP/1.0
9/tcp     open    discard?
| auth-owners: ERROR: Script execution failed (use -d to debug)
13/tcp    open    daytime         Microsoft Windows International daytime
| auth-owners: ERROR: Script execution failed (use -d to debug)
17/tcp    open    chargen
| auth-owners: ERROR: Script execution failed (use -d to debug)
19/tcp    open    chargen
| auth-owners: ERROR: Script execution failed (use -d to debug)
20/tcp    open    ftp-data?
| auth-owners: ERROR: Script execution failed (use -d to debug)
21/tcp    open    ftp             Microsoft ftpd
| auth-owners: ERROR: Script execution failed (use -d to debug)
|_  ftp-bounce: no banner
22/tcp    open    ssh?
| auth-owners: ERROR: Script execution failed (use -d to debug)
23/tcp    open    telnet          Microsoft Windows 2000 telnetd
| auth-owners: ERROR: Script execution failed (use -d to debug)
24/tcp    open    priv-mail?
| auth-owners: ERROR: Script execution failed (use -d to debug)
25/tcp    open    smtp            Microsoft ESMTP 6.0.3790.0
| auth-owners: ERROR: Script execution failed (use -d to debug)
|_  smtp-commands: Couldn't establish connection on port 25
    
```

الآن سوف انتقل بكم الى البيانات التي تم الوصول اليها من خلال الهجمات التي تمت على النظام

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
6/23/2017	11:26:48 AM	54.175.125.231	42838	158.69.134.77	50505	TCP	0
6/23/2017	11:26:48 AM	54.175.125.231	9224	158.69.134.77	3195	TCP	0
6/23/2017	11:26:48 AM	54.175.125.231	52180	158.69.134.77	2064	TCP	0
6/23/2017	11:26:49 AM	54.175.125.231	45624	158.69.134.77	280	TCP	0
6/23/2017	11:26:49 AM	54.175.125.231	8314	158.69.134.77	3168	TCP	0
6/23/2017	11:26:49 AM	54.175.125.231	37998	158.69.134.77	217	TCP	0
6/23/2017	11:26:49 AM	54.175.125.231	30788	158.69.134.77	1511	TCP	0
6/23/2017	11:26:49 AM	54.175.125.231	47402	158.69.134.77	371	TCP	0
6/23/2017	11:26:50 AM	54.175.125.231	56848	158.69.134.77	3531	TCP	0
6/23/2017	11:26:50 AM	54.175.125.231	33736	158.69.134.77	205	TCP	0
6/23/2017	11:26:50 AM	54.175.125.231	57136	158.69.134.77	140	TCP	0

نلاحظ عدد المهاجمين على الخادم ولعرض تفاصيل اكثر عن نوع البيانات المرسل او العمليات المستخدمة يمكن الضغط على احد الاعمده الظاهره في الشاشة على اليمين

★ Packet Log (ircserv)

Connection Details:

Date: 6/23/2017
 Time: 10:47:58 AM
 Millisecond: 453
 Time Zone: -7:00
 Source IP: 54.175.125.231
 Source Port: 37182
 Server IP: 158.69.134.77
 Server Port: 2401 (ircserv)
 Protocol: TCP

Bytes Sent: 0
 Bytes Received: 1040

Packet History

Time	Direction	Bytes	Data
10:47:58 AM	RX	0	SYN
10:47:58 AM	RX	1040	NESSUS
10:48:03 AM	TX	0	FIN

احدى الطلبات المرسله من مشروع Nessus

Packet Data:

View as text

hex



NESSUS

root

للتقنيه هذه يوجد العديد من الادوات المفيده سوف اطرحها باختصار وكيفية عملها

1- SSHesame

ميزة هذه الاداه هي تكوين بروتوكول SSH وهمي دون كلمه مرور ويتم تسجيل جميع تحركاته داخل النظام

2- Honey Pot Pi

هذه الاداه يتم تحويل Raspberry Pi الى Honeypots

الخاتمه

اتمنى من الله اني وفقت في هذا العمل

Links:

<https://github.com/free5ty1e/honeypotpi>

<http://www.atomicsoftwaresolutions.com/>

<https://github.com/jaksi/sshesame>

<https://github.com/royaflash/pentbox>

<http://www.honeyd.org/>

[https://en.wikipedia.org/wiki/Honeypot_\(computing\)](https://en.wikipedia.org/wiki/Honeypot_(computing))

<https://wiki.archlinux.org/index.php/honeyd>