Дәріс №8: Honeypot технологиясы

Honeypot технологиясы - бұл зерттеу немесе шабуыл жасау болып табылатын қауіпсіздік ресурсы. Honeypot қаншалықты құрылымдалған болса да, ресурстарды шабуылдаушы зерттеп, шабуылдап, қолдануы керек дегенді білдіреді. Ресурстың қандай екендігі маңызды емес: имитациялық қызмет немесе толыққанды операциялық жүйе. Ең бастысы, ресурстардың жұмыс істеу мағынасы оған шабуыл жасау болып табылады.

Honeypot - бұл қауіпсіздік құралы, оның мәні сканерлеуге, шабуылдарға және хакерлерге бейімділігінде. Honeypot міндеті - шабуылдау және сізге бұл туралы айту.

Honeypot түрлері:

- бөлінген серверде орнатылған Honeypot оны нақты рөлге мүмкіндігінше жақындатуға мүмкіндік береді, оның рөлі - деректер сервері, қосымша сервері, прокси-сервер;

- эмуляцияланған Honeypot – шабуылдан соң тез қалпына келеді, сонымен қатар ОЖ-мен шектеледі. Оны VMware немесе Honeyd көмегімен жасауға болады.

Honeypot міндеттері:

- шабуылдың басталуын анықтау, ақпарат жинау;
- Сізге хакердің әрекеттері туралы ақпарат беру;
- Хакердің өзін анықтау.

Web-ке арналған Pentbox бағдарламасын қолданамыз.

```
gulzinat@gulzinat-VirtualBox:~$ sudo apt-get install wget
[sudo] password for gulzinat:
```

```
gulzinat@gulzinat-VirtualBox:~$ sudo apt-get install ruby
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fonts-lato javascript-common libjs-jquery libruby2.7 rake ruby-minitest
  ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmlrpc ruby2.7
  rubygems-integration
Suggested packages:
```

```
gulzinat@gulzinat-VirtualBox:~$ wget http://downloads.sourceforge.net/project/p
entbox18realised/pentbox-1.8.tar.gz
```

```
gulzinat@gulzinat-VirtualBox:~$ tar xvfz pentbox-1.8.tar.gz
```

```
pentbox-1.8/other/
pentbox-1.8/
gulzinat@gulzinat-VirtualBox:~$ ls
 Desktop                          msfinstall           Public
 Documents                        Music                snap
 Downloads                        pentbox-1.8          Templates
'download?use_mirror=netcologne'  pentbox-1.8.tar.gz   TEST
'download?use_mirror=netcologne.1' Pictures            Videos
gulzinat@gulzinat-VirtualBox:~$ cd pentbox-1.8/
gulzinat@gulzinat-VirtualBox:~/pentbox-1.8$ ls
changelog.txt  lib    pb_update.rb  readme.txt  tools
COPYING.txt    other  pentbox.rb    todo.txt
gulzinat@gulzinat-VirtualBox:~/pentbox-1.8$ ./pentbox.rb

 PenTBox 1.8

    ____            _____ ____
   |  _ \ ___ _ _|_   _| __ )  _____  __
   | |_) / _ \ '_ \| | |  _ \ / _ \ \/ /
   |  __/  __/ | | | | | |_) | (_) >  <
   |_|   \___|_| |_|_| |____/ \___/_/\_\

--------- Menu          ruby2.7.0 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web
```

```
   -> 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.
```

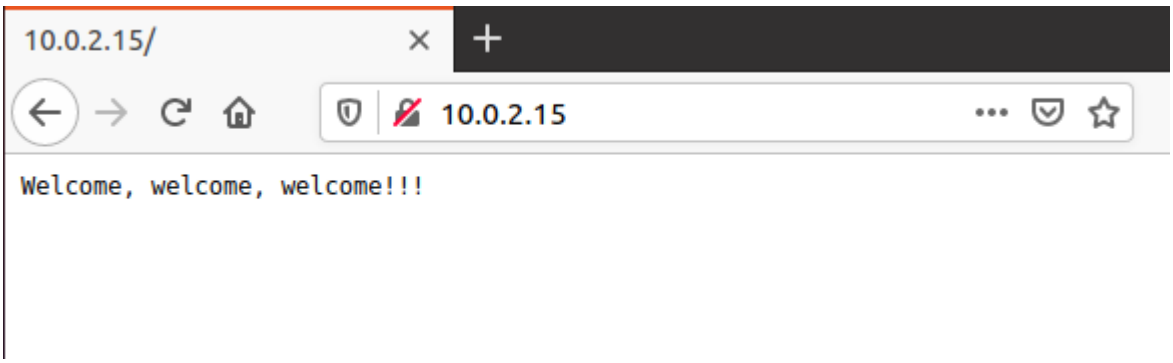
```
   -> ^Z
[1]+  Stopped                 ./pentbox.rb
gulzinat@gulzinat-VirtualBox:~/pentbox-1.8$ sudo ./pentbox.rb
[sudo] password for gulzinat:

 PenTBox 1.8

        __
       U00U|.'@@@@@@`.
       |__|(@@@@@@@@@@)
            (@@@@@@@@)
            `YY~~~~YY'
             ||    ||

--------- 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]
```

```
   -> ^Z
[2]+  Stopped                 sudo ./pentbox.rb
gulzinat@gulzinat-VirtualBox:~/pentbox-1.8$ sudo su
root@gulzinat-VirtualBox:/home/gulzinat/pentbox-1.8# ./pentbox.rb

 PenTBox 1.8
                                      .::!!!!!!!:.
  .!!!!!:.                        .:!!!!!!!!!!!!
  ~~~~!!!!!!.                 .:!!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$   $$$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$   4$$$$$*
      ^$$$B  $$$$      $$$$$$$$$$$   d$$R*
        **$bd$$$$      '*$$$$$$$$$$o+#
             ****          *******

--------- Menu          ruby2.7.0 @ x86_64-linux-gnu

1- Cryptography tools

2- Network tools

3- Web

4- Ip grabber
```

```
   -> 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.
```

```
   -> 2

 Insert port to Open.

   -> 80

 Insert false message to show.

   -> Welcome, welcome, welcome!!!

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   ->

 Activate beep() sound when intrusion?

 (y/n)   -> n

  HONEYPOT ACTIVATED ON PORT 80 (2020-11-06 06:37:52 +0600)
```



```
  INTRUSION ATTEMPT DETECTED! from 10.0.2.15:41248 (2020-11-06 06:41:12 +0600)
 ----------------------------
GET / HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Fir
efox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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 10.0.2.15:41254 (2020-11-06 06:41:16 +0600)
 ----------------------------
GET /favicon.ico HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Fir
efox/82.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://10.0.2.15/
```

Өзіндік жұмыс:

1) Мақаламен танысу - https://zen.yandex.ru/media/securitylab.ru/tehnologiia-honeypot-chast-1-naznachenie-honeypot-5addad9a9b403cf606151d82

2) Тәжірибе жасау – а) https://www.youtube.com/watch?v=0WUaI2pNiPI ; б) https://www.youtube.com/watch?v=Leogp9RJEWw