CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Intrusion Detection System

Honeypots

Video Summary

- Honeypots
- Honeypots Deployment
- HoneyNets
- Honey Drive
- HoneyFiles

Honeypots

The system is left intentionally vulnerable

- Default setting
- Missing patches
- Security misconfigurations
- Fake data is placed on the Honeypot

Honeypots

➢ **Honeypots designed to:**

- A **honeypot** is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate.

Honeypots

- **Honeypots designed to:**

  - Turn a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond

- **Filled with fake information that a legitimate user of the system wouldn't access**

- **Resource that has no production value**

  - Incoming communication is most likely a scan, or attack
  - Outbound communication suggests that the system has probably been compromised

- **Once intruders are within the network, admins can observe their behavior to figure out defenses**

Honeypots Deployment

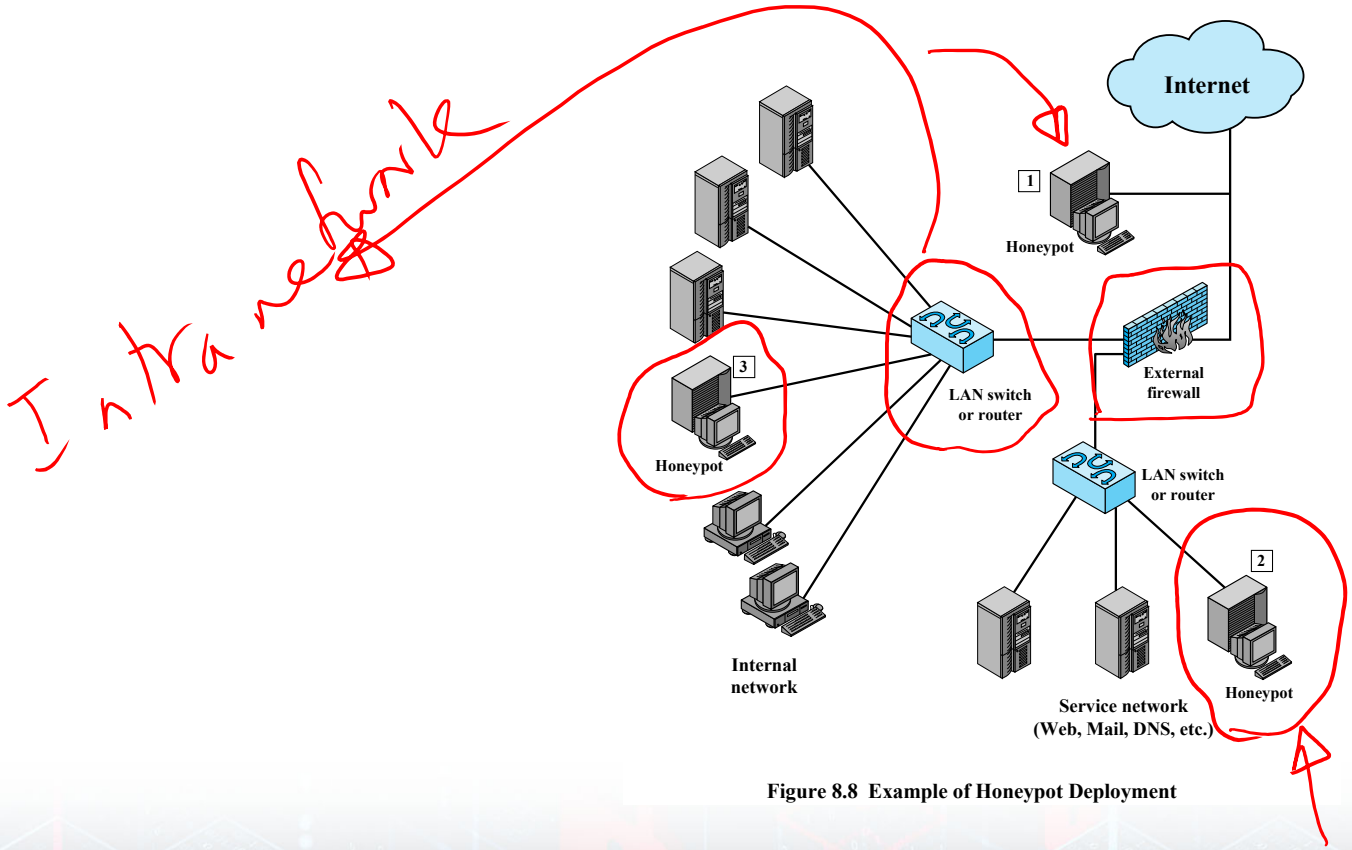
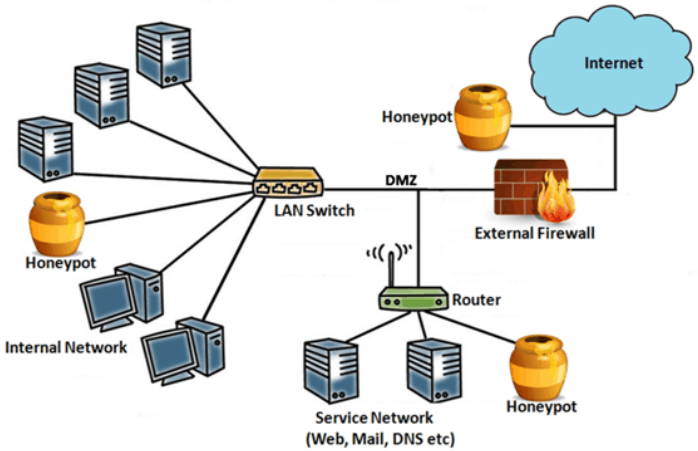


Figure 8.8 Example of Honeypot Deployment

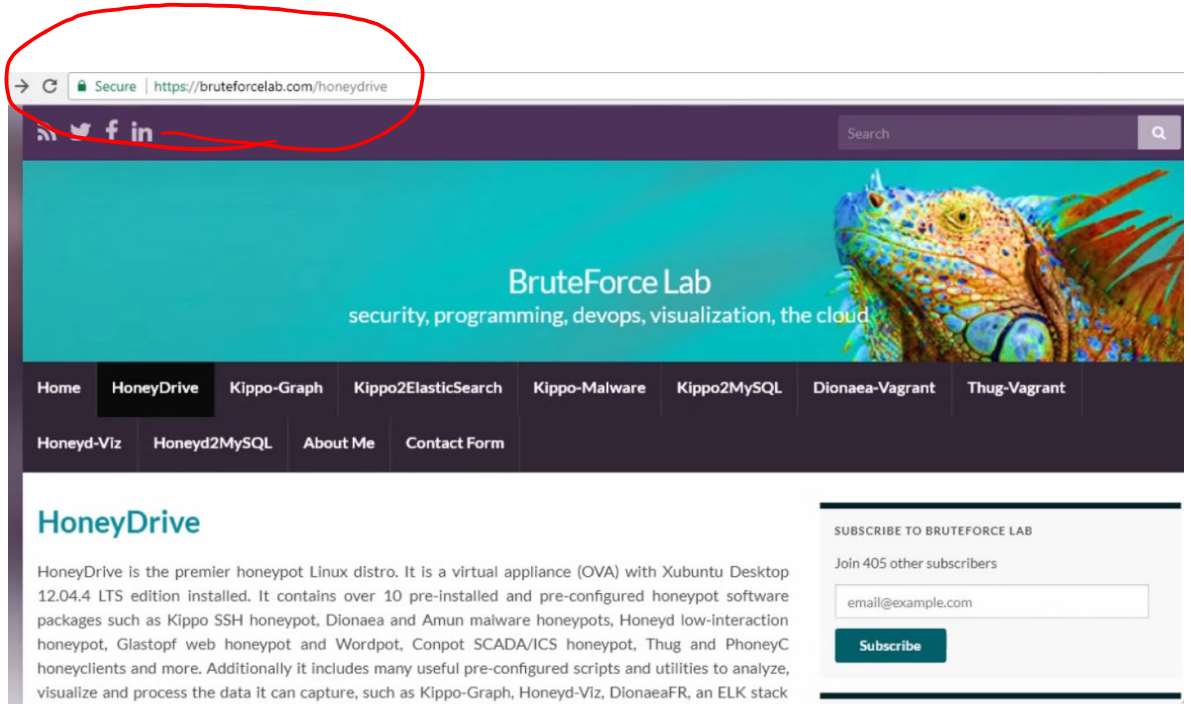
HoneyNets



- Two or more honeypots on the same network
- Groups dissimilar honeypots together (windows server + Linux server)
- IDS honeynet configurations can send notifications to security admin
- Must be deployed on an isolated network (virtual network on a cloud computing environment)

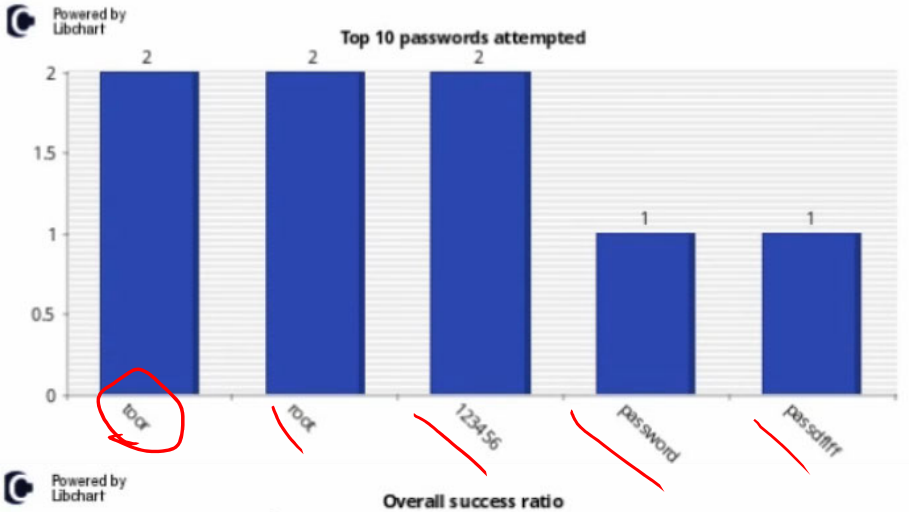
Honey Drive

- Free license
- Free Download (Virtual Machine)



Honey Drive

- Easy ssh (user root and password 1-6)
- Honey Drive keeps the log of the system so you can see who tried to access your Honeypot and their activities



Honey Drive

- Also Honey Drive gives you the option to playback the intruder activities

Replay input by attackers captured by the honeypot system

The following table displays a list of all the logs recorded by Kippo.

ID	Timstamp	Size	Play the log
1	2018-01-23 18:01:59	10.88kb	Play
2	2018-01-23 18:01:52	10.88kb	Play
3	2018-01-23 18:01:50	10.88kb	Play
4	2018-01-23 18:01:48	10.88kb	Play
5	2018-01-23 17:47:00	12.98kb	Play

IP: 192.168.0.7 on 2018-01-23 17:46:50

Playing 6362f5180065 11e8b7 c000c29a8ec81

```
root@svr03:~# ls
root@svr03:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:4c:a8:ab:32:f4
          inet addr:10.98.55.4  Bcast:10.98.55.255  Mask:255.255.255.0
          inet6 addr: fe80::21f:c6ac:fd44:24d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84045991 errors:0 dropped:0 overruns:0 frame:0
          TX packets:103776307 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:50588302699 (47.1 GiB)  TX bytes:97318807157 (90.6 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:308297 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308297 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:355278106 (338.8 MiB)  TX bytes:355278106 (338.8 MiB)
root@svr03:~# cd /etc
root@svr03:/etc# clear
^C
root@svr03:/etc# ls
shadow-                 bindresvport.blacklist
```

HoneyFiles

- Honeyfiles emulate legitimate documents with realistic, enticing names and possibly content.
- These documents should not be accessed by legitimate users of a system, but rather act as trap for intruders exploring a system.
- Any access of Honeyfiles is assumed to be suspicious.
- Appropriate generation, placement, and monitoring of Honeyfiles is an area of current research.

Video Summary

- Honeypots
- Honeypots Deployment
- HoneyNets
- Honey Drive
- HoneyFiles