

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Icarus: A Prototype Honeyfarm System

Kevin Zhijie Chen

The HoneyNet Project

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

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

1 Honeyfarm

2 Key Modules

3 Statistics

4 Case Study

Honeypots and Honeynets

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

HoneyNet

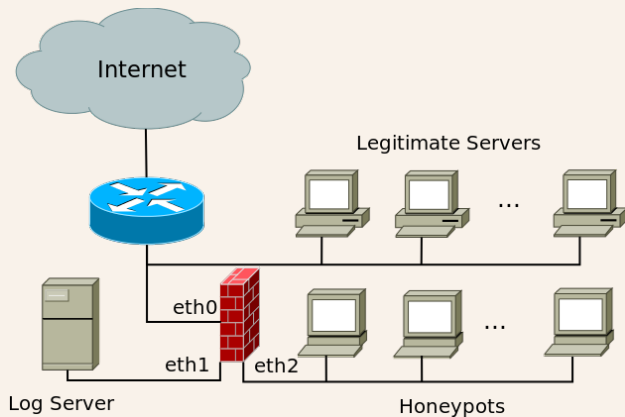


Figure: Topology of a HoneyNet

Honeypots and Honeynets

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Honeynet



Figure: “Matrix” Distributed Honeynet in CNCERT/CC

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Honeyfarm

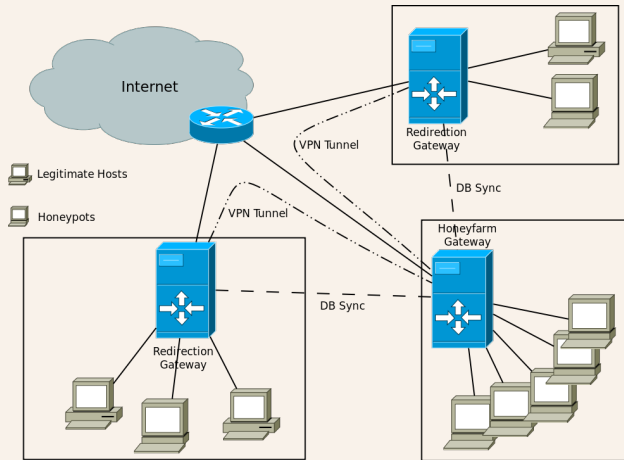


Figure: Topology of a Honeyfarm

Attack Scenarios

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

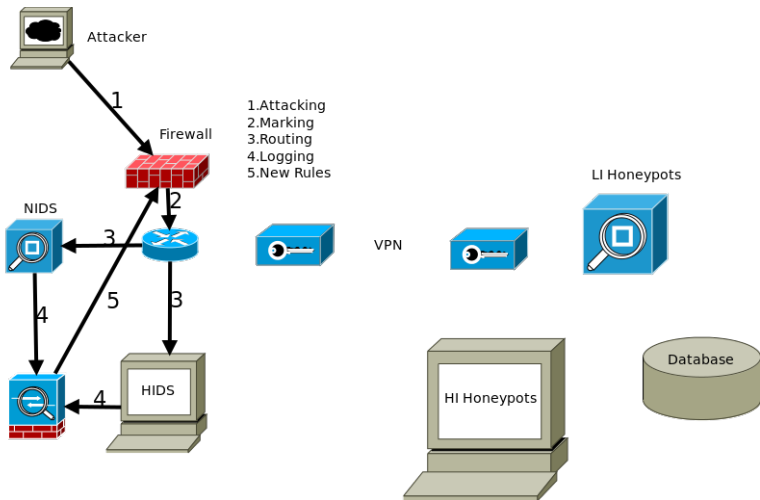


Figure: First Attack from Unknown Source

Honeyfarm

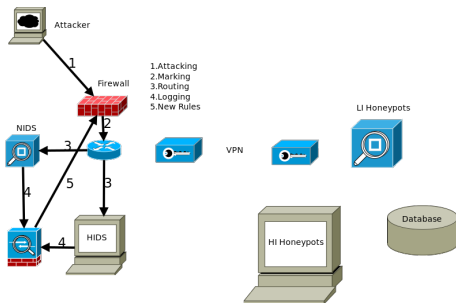
Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study



2 Traffic Redirection

- Packets Marking
- Policy based Routing
- VPN Tunneling
- Building network in the honeyfarm the same as real the production network

Honeyfarm

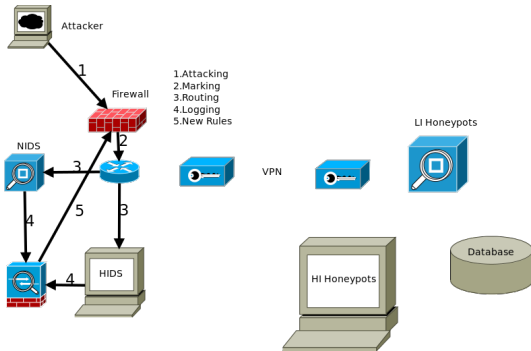
Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study



4,5. Log Correlation

- Semantic Reconstruction of VMs
- Correlating the logs from HIDS and the ones from NIDS

Attack Scenarios

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

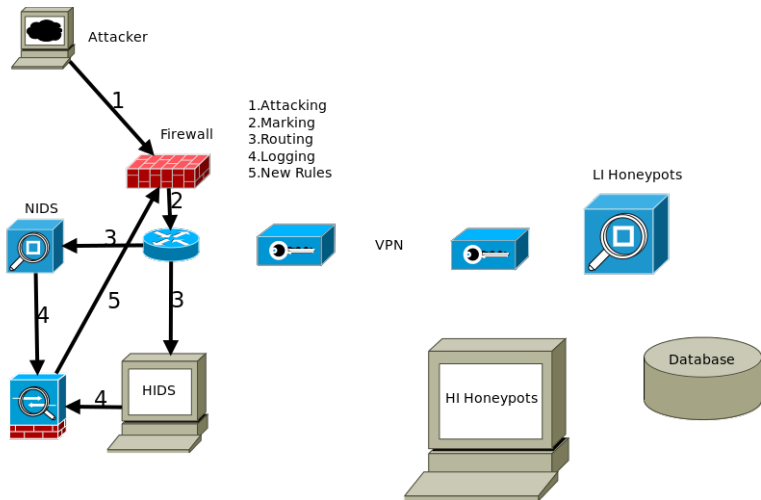


Figure: First Attack from Unknown Source

Attack Scenarios

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

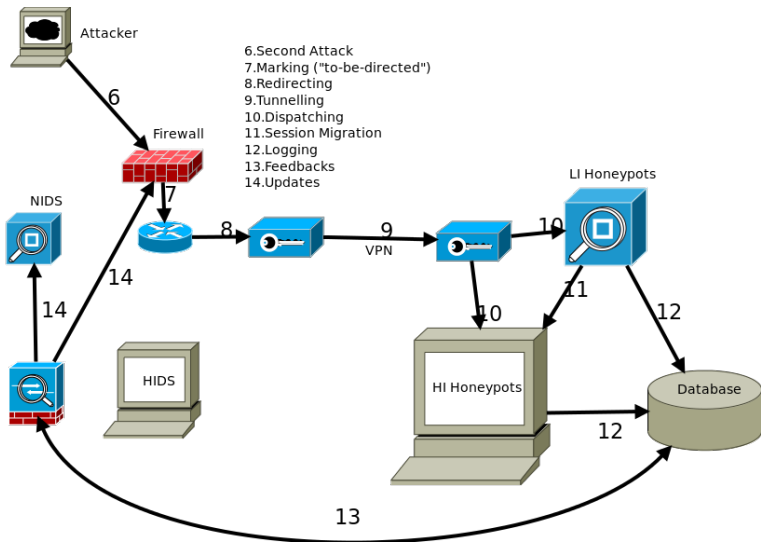


Figure: Non-business Traffic / Traffic from Known Attackers

Honeyfarm

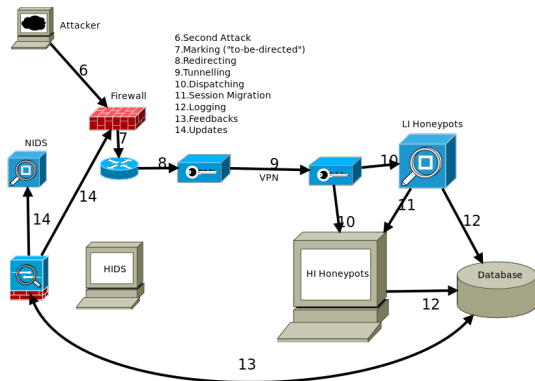
Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study



11. Session Migration

- Use low-interaction HPs (nepenthes) to handle traffics in the honeyfarm first
- If they can't handle, pass it to the high interaction honeypots

Attack Scenarios

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

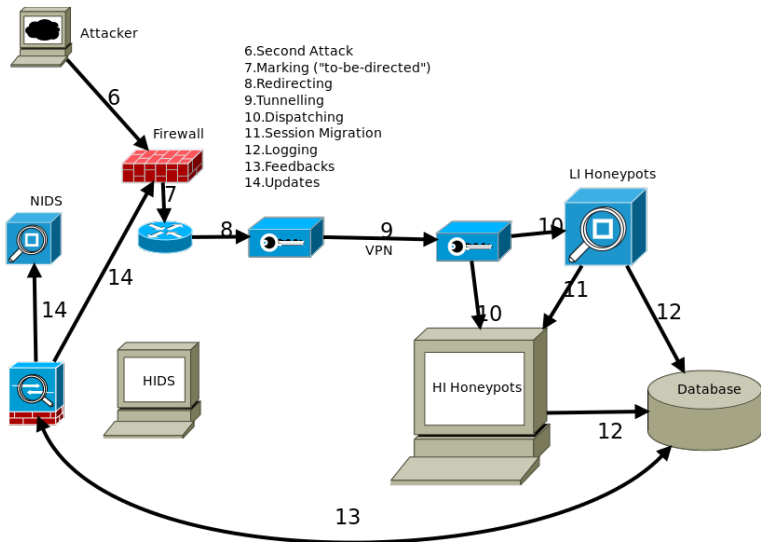


Figure: Non-business Traffic / Traffic from Known Attackers

Honeyfarm

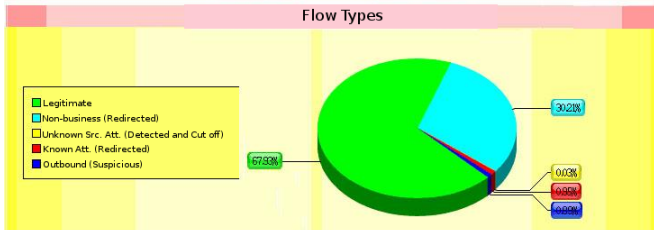
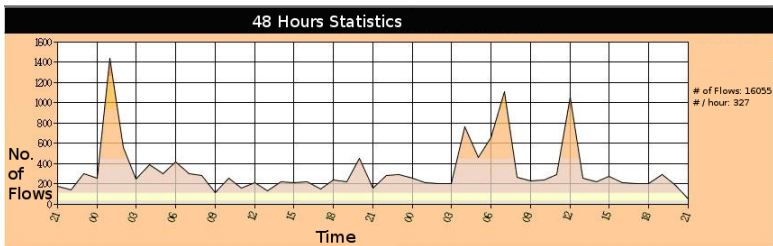
Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study



Honeyfarm

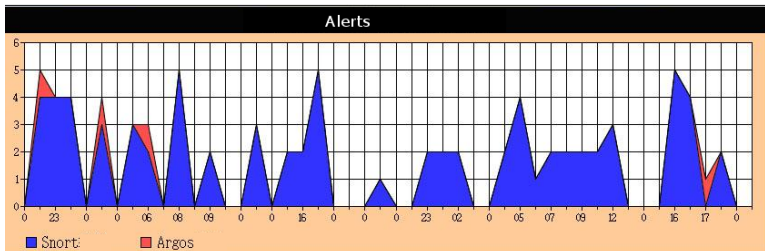
Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study



Known Attackers

59.100.177.181	59.100.177.167
总计: 2	

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

```
msf exploit(ms03_026_dcom) > exploit
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:59.██████████1[135] ..
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:59.██████████1[135] ...
[*] Sending exploit ...
[*] The DCERPC service did not reply to our request
[*] Exploit completed, but no session was created.
msf exploit(ms03_026_dcom) > █
```

Figure: Exploiting

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Event ID	Attack Time	Type	Platform	Log File
1163975089	2008-10-30 15:30:16	4	0	./argos.csi.1163975089
1663860249	2008-10-30 14:35:11	4	0	./argos.csi.1663860249
1931652305	2008-10-30 14:34:59	4	0	./argos.csi.1931652305
617164656	2008-10-17 16:10:51	4	0	./argos.csi.617164656
542534383	2008-10-16 17:21:32	4	0	./argos.csi.542534383
1316718064	2008-10-15 12:25:49	4	0	./argos.csi.1316718064
1761203658	2008-10-14 16:42:54	5	0	./argos.csi.1761203658
750621350	2008-10-10 17:54:42	0	0	./argos.csi.750621350
1112393033	2008-10-10 17:54:16	0	0	./argos.csi.1112393033
1804760512	2008-10-10 15:17:38	4	0	./argos.csi.1804760512
789331151	2008-10-07 15:08:22	0	0	./argos.csi.789331151
1518721670	2008-10-07 15:07:42	4	0	./argos.csi.1518721670

Figure: HIDS Log

Attacks Exploiting MS03-026

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Host ID	1	Event ID	1163975089
Time:	2008-10-30 15:30:16	Platform:	0
Type:	4	Log File:	./argos.csi.1163975089
Registers:			
EAX	0x00000000	EBX	0x0057f8a8
ECX	0x00000002	EDX	0x00000000
EDI	0x004a5524	ESI	0x00096c08
ESP	0x0057f730	EBP	0x19eb10eb
EFALGS 0x00000202			
EIP	0x0018759f	原始 EIP	0x048ab724
查询前 60 秒, 后 90 秒的数据 <input type="button" value="查询"/>			

可疑内存块列表

Mem ID	物理地址	虚拟地址	大小	污染
1	0x048b7b54	0x00074b54	12	Yes
2	0x04939af8	0x0007daf8	8	Yes
3	0x04832c10	0x0007fc10	4	Yes
4	0x04832c20	0x0007fc20	8	Yes
5	0x04832c48	0x0007fc48	4	Yes
6	0x048818cc	0x000808cc	4	Yes
7	0x048818ec	0x000808ec	2	Yes
8	0x04881a00	0x00080a00	12	Yes
9	0x04881a14	0x00080a14	4	Yes
10	0x04881a2c	0x00080a2c	12	Yes
11	0x05250418	0x0008c418	556	Yes
12	0x052125a0	0x0008e5a0	1024	Yes
13	0x052363ee	0x000913ee	1	Yes
14	0x05236400	0x00091400	4	Yes

argos	2008-10-30 15:30:20	0215	46-> 58	31TCP	51437 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:19	0215	46-> 58	31TCP	47289 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:19	0215	46-> 58	31TCP	50846 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:18	0215	46-> 58	31TCP	33291 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:17	0215	46-> 58	31TCP	48048 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:17	0215	46-> 58	31TCP	48553 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:16	0215	46-> 58	31TCP	58971 74	1	4444	54	1	unknownRST	
argos	2008-10-30 15:30:15	6215	46-> 58	31TCP	51050 2784	8	135	666	5	unknownFIN	
argos	2008-10-30 15:30:15	0215	46-> 58	31TCP	53175 74	1	4444	54	1	unknownRST	

NIDSAlert List

ID	Time	Source IP:Port	Destination IP:Port	Proto	Alert Type	Pcap Downl
16838	8690	2008-10-30 15:30:16	2 651050	59	1135	6 None

Attacks Exploiting MS03-026

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

ms03026_dcom_port_135.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression...

No.	Time	Source	Destination	Protocol	Info
2	1225351815.994007	181	21	TCP	epmap > 51050 [S...
5	1225351816.030317	181	21	DCERPC	Bind_ack: call_id...
9	1225351816.158449	181	21	TCP	epmap > 51050 [A...
11	1225351821.254536	181	21	TCP	epmap > 51050 [A...
12	1225351821.256926	181	21	TCP	epmap > 51050 [F...
1	1225351815.991583	246	59	TCP	51050 > epmap [S...
3	1225351815.997886	246	59	TCP	51050 > epmap [A...
4	1225351816.019562	246	59	DCERPC	Bind: call_id: 0...
6	1225351816.033953	246	59	TCP	51050 > epmap [A...
7	1225351816.155065	246	59	TCP	[TCP segment of a...
8	1225351816.155120	246	59	DCERPC	Request: call_id...
10	1225351821.251771	246	59	TCP	51050 > epmap [F...
13	1225351821.259687	246	59	TCP	51050 > epmap [A...

> Frame 2 (78 bytes on wire, 78 bytes captured)

> Ethernet II, Src: RealtekU_12:34:56 (52:54:00:12:34:56), Dst: LanmerE1_06:89:e1 (00:90:0b:06:89:e1)

> Internet Protocol...

Figure: Pcap File

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

action	acti
Successful: iptables -t mangle -A ATTACKERS -s 219.██████████.46 -m conntrack --ctstate NEW -j MARK --set-mark 101	
Successful: iptables -t mangle -A ATTACKERS -s 219.██████████.46 -m mark ! --mark 0x65 -m mark ! --mark 0x66 -j MARK --and-mark 0x60	

Figure: Redirection Rule

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Questions?

Honeyfarm

Kevin ZC

Honeyfarm

Key Modules

Statistics

Case Study

Thank you!