



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1

Roll No.: 16010121045

Experiment No. 3

Title: Honeypot with KF sensor.

Objective: Honeypot with KF sensor.

CO	Outcome
CO5	Interpret legal and ethical issues in security

Books/ Journals/ Websites referred:

1. <http://www.keyfocus.net/kfsensor/>
2. <http://www.keyfocus.net/kfsensor/help/>
3. <https://www.youtube.com/watch?v=HvuIYE7UMHs>
4. <https://www.youtube.com/watch?v=nBqzBjGgJFw>
5. <https://www.youtube.com/watch?v=O3H1LH-V7nk>

Abstract:

A honeypot is a security mechanism designed to deceive attackers, gather information about their tactics, and protect real systems from their malicious activities. This concept involves deploying decoy systems or services that appear legitimate but are actually isolated and monitored, allowing security professionals to study attackers' behavior without risking the integrity of operational networks.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Related Theory:

Types of honeypots:

Honeypots can be categorized into several types based on their deployment and purpose. High-interaction honeypots fully emulate real systems and interact extensively with attackers, while low-interaction honeypots simulate only specific services or protocols with limited interaction. Additionally, there are research honeypots used for academic or research purposes, and production honeypots deployed within operational networks for security monitoring.

- 1. Honeypots and evasion techniques:** Attackers may employ various evasion techniques to identify and avoid honeypots, such as fingerprinting, timing-based analysis, and protocol-specific evasion. Security practitioners must continuously update honeypot configurations and monitoring techniques to mitigate these evasion attempts effectively.
- 2. Honeypot applications:** Honeypots serve multiple purposes in cybersecurity, including detecting and analyzing new threats, capturing malware samples, studying attacker tactics and techniques, and diverting attackers' attention away from critical systems. They can also aid in forensic investigations by providing valuable insights into attack methodologies and identifying compromised systems.

List of tools used as honeypots:

- 1. Kippo:** A medium-interaction SSH honeypot designed to capture and log SSH brute force attacks and shell interaction.
- 2. Dionaea:** A high-interaction honeypot focused on capturing malware samples and analyzing exploit attempts targeting network services like SMB, FTP, and HTTP.
- 3. Cowrie:** A SSH and Telnet honeypot designed to emulate vulnerable Linux systems and capture attacker activity.
- 4. Honeyd:** A low-interaction honeypot capable of emulating multiple IP addresses, operating systems, and network services to deceive attackers.
- 5. Glastopf:** A web application honeypot that emulates vulnerable web applications to lure and capture attackers attempting to exploit web vulnerabilities.

These tools provide security professionals with versatile options for deploying honeypots tailored to specific environments and objectives, enabling proactive threat detection and intelligence gathering in cybersecurity operations.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Implementation Details:

KFSensor Professional - Evaluation Trial

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description	Received	Sig. Message
32	12-04-2024 11:58:01.587	0.000	UDP	138	NBT Datagram ...	16detb415-7	NBT DGRAM Packet: id:42092 Typ...		
31	12-04-2024 11:57:09.662	0.000	UDP	138	NBT Datagram ...	16detb513-06	NBT DGRAM Packet: id:36199 Typ...		
30	12-04-2024 11:56:50.788	0.000	UDP	138	NBT Datagram ...	16detb415-17	NBT DGRAM Packet: id:44775 Typ...		
29	12-04-2024 11:56:47.056	0.000	UDP	138	NBT Datagram ...	16detb513-17	NBT DGRAM Packet: id:64423 Typ...		
28	12-04-2024 11:56:37.338	0.000	UDP	138	NBT Datagram ...	16detb415-14	NBT DGRAM Packet: id:40217 Typ...		
27	12-04-2024 11:56:23.759	0.000	UDP	138	NBT Datagram ...	16detb513-1	NBT DGRAM Packet: id:64629 Typ...		
26	12-04-2024 11:56:18.388	0.000	UDP	138	NBT Datagram ...	16detb415-52F2FAB	NBT DGRAM Packet: id:40130 Typ...		
25	12-04-2024 11:56:15.558	0.000	UDP	138	NBT Datagram ...	16detb407-08	NBT DGRAM Packet: id:43109 Typ...		
24	12-04-2024 11:56:12.257	0.000	UDP	138	NBT Datagram ...	16detb510-32	NBT DGRAM Packet: id:43110 Typ...		
23	12-04-2024 11:55:58.910	0.000	UDP	138	NBT Datagram ...	16detb513-12	NBT DGRAM Packet: id:65455 Typ...		
22	12-04-2024 11:55:05.496	0.000	UDP	138	NBT Datagram ...	16detb510-15	NBT DGRAM Packet: id:40552 Typ...		
21	12-04-2024 11:54:57.000	0.000	UDP	138	NBT Datagram ...	16detc10-U0246	NBT DGRAM Packet: id:46808 Typ...		
20	12-04-2024 11:54:55.747	0.000	UDP	138	NBT Datagram ...	16detb513-8	NBT DGRAM Packet: id:45867 Typ...		
19	12-04-2024 11:54:31.278	0.000	UDP	138	NBT Datagram ...	16detb513-04	NBT DGRAM Packet: id:63043 Typ...		
18	12-04-2024 11:54:21.149	0.000	UDP	138	NBT Datagram ...	16detb514-23	NBT DGRAM Packet: id:46069 Typ...		
17	12-04-2024 11:54:18.760	0.000	UDP	138	NBT Datagram ...	16detb513-4	NBT DGRAM Packet: id:40559 Typ...		
16	12-04-2024 11:54:09.760	0.000	UDP	138	NBT Datagram ...	16detb415-2	NBT DGRAM Packet: id:65599 Typ...		
15	12-04-2024 11:53:27.463	0.000	UDP	138	NBT Datagram ...	16detb513-12	NBT DGRAM Packet: id:60581 Typ...		
14	12-04-2024 11:53:12.257	0.000	UDP	138	NBT Datagram ...	16detb415-16	NBT DGRAM Packet: id:56982 Typ...		
13	12-04-2024 11:53:01.920	0.000	UDP	138	NBT Datagram ...	16detb510-14	NBT DGRAM Packet: id:65447 Typ...		
12	12-04-2024 11:52:51.399	0.000	UDP	138	NBT Datagram ...	16detb418-2	NBT DGRAM Packet: id:45883 Typ...		
11	12-04-2024 11:52:49.930	0.000	UDP	138	NBT Datagram ...	16detb510-23	NBT DGRAM Packet: id:46749 Typ...		
10	12-04-2024 11:52:40.000	0.000	UDP	138	NBT Datagram ...	16detb510-0	NBT DGRAM Packet: id:65233 Typ...		
9	12-04-2024 11:52:23.402	0.000	UDP	138	NBT Datagram ...	16detb417-02	NBT DGRAM Packet: id:51165 Typ...		
8	12-04-2024 11:52:20.338	0.000	UDP	138	NBT Datagram ...	16detb513-20	NBT DGRAM Packet: id:51325 Typ...		
7	12-04-2024 11:52:17.423	0.000	UDP	138	NBT Datagram ...	16detb513-05	NBT DGRAM Packet: id:49949 Typ...		
6	12-04-2024 11:52:07.861	0.000	UDP	138	NBT Datagram ...	16detb510-03	NBT DGRAM Packet: id:51996 Typ...		
5	12-04-2024 11:52:04.427	0.000	UDP	138	NBT Datagram ...	16detb415-15	NBT DGRAM Packet: id:59301 Typ...		
4	12-04-2024 11:51:59.030	0.000	UDP	138	NBT Datagram ...	16detb510-02	NBT DGRAM Packet: id:46830 Typ...		
3	12-04-2024 11:51:38.704	0.000	UDP	138	NBT Datagram ...	16detb510-13	NBT DGRAM Packet: id:34045 Typ...		
2	12-04-2024 11:51:25.074	0.000	UDP	138	NBT Datagram ...	16detb510-11	NBT DGRAM Packet: id:161008 Typ...		
1	12-04-2024 11:51:21.242	0.000	UDP	138	NBT Datagram ...	16detb416-23	NBT DGRAM Packet: id:44352 Typ...		

User Rights: Basic User [5] Server: Running Visitors: 32 Events: 32/32

KFSensor Professional - Evaluation Trial

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description	Received	Sig. Message
32	12-04-2024 11:58:01.587	0.000	UDP	138	NBT Datagram ...	16detb415-7	NBT DGRAM Packet: id:42092 Typ...		
31	12-04-2024 11:57:09.662	0.000	UDP	138	NBT Datagram ...	16detb513-06	NBT DGRAM Packet: id:36199 Typ...		
30	12-04-2024 11:56:50.788	0.000	UDP	138	NBT Datagram ...	16detb415-17	NBT DGRAM Packet: id:44775 Typ...		
29	12-04-2024 11:56:47.056	0.000	UDP	138	NBT Datagram ...	16detb513-17	NBT DGRAM Packet: id:64423 Typ...		
28	12-04-2024 11:56:37.338	0.000	UDP	138	NBT Datagram ...	16detb415-14	NBT DGRAM Packet: id:40217 Typ...		
27	12-04-2024 11:56:23.759	0.000	UDP	138	NBT Datagram ...	16detb415-1	NBT DGRAM Packet: id:64629 Typ...		
26	12-04-2024 11:56:18.388	0.000	UDP	138	NBT Datagram ...	16detb513-52F2FAB	NBT DGRAM Packet: id:40130 Typ...		
25	12-04-2024 11:56:15.558	0.000	UDP	138	NBT Datagram ...	16detb407-08	NBT DGRAM Packet: id:43109 Typ...		
24	12-04-2024 11:55:32.428	0.000	UDP	138	NBT Datagram ...	16detb510A-1	NBT DGRAM Packet: id:46808 Typ...		
23	12-04-2024 11:55:26.910	0.000	UDP	138	NBT Datagram ...	16detb513-12	NBT DGRAM Packet: id:46749 Typ...		
22	12-04-2024 11:55:05.406	0.000	UDP	138	NBT Datagram ...	16detb510B-1	NBT DGRAM Packet: id:46750 Typ...		
21	12-04-2024 11:54:57.000	0.000	UDP	138	NBT Datagram ...	16detb407-16	NBT DGRAM Packet: id:59301 Typ...		
20	12-04-2024 11:54:55.747	0.000	UDP	138	NBT Datagram ...	16detb415-8	NBT DGRAM Packet: id:46830 Typ...		
19	12-04-2024 11:54:31.278	0.000	UDP	138	NBT Datagram ...	16detb513-14	NBT DGRAM Packet: id:40217 Typ...		
18	12-04-2024 11:54:21.149	0.000	UDP	138	NBT Datagram ...	16detb514-23	NBT DGRAM Packet: id:46069 Typ...		
17	12-04-2024 11:54:18.760	0.000	UDP	138	NBT Datagram ...	16detb415-2	NBT DGRAM Packet: id:40559 Typ...		
16	12-04-2024 11:53:49.760	0.000	UDP	138	NBT Datagram ...	16detb513-20	NBT DGRAM Packet: id:46378 Typ...		
15	12-04-2024 11:53:27.463	0.000	UDP	138	NBT Datagram ...	16detb415-1	NBT DGRAM Packet: id:65341 Typ...		
14	12-04-2024 11:53:12.257	0.000	UDP	138	NBT Datagram ...	16detb415-16	NBT DGRAM Packet: id:44775 Typ...		
13	12-04-2024 11:53:01.920	0.000	UDP	138	NBT Datagram ...	16detb510B-1	NBT DGRAM Packet: id:46830 Typ...		
12	12-04-2024 11:52:51.399	0.000	UDP	138	NBT Datagram ...	16detb418-2	NBT DGRAM Packet: id:45883 Typ...		
11	12-04-2024 11:52:30.930	0.000	UDP	138	NBT Datagram ...	16detb510A-2	NBT DGRAM Packet: id:46749 Typ...		
10	12-04-2024 11:52:25.402	0.000	UDP	138	NBT Datagram ...	16detb417-02	NBT DGRAM Packet: id:51165 Typ...		
9	12-04-2024 11:52:20.338	0.000	UDP	138	NBT Datagram ...	16detb513-20	NBT DGRAM Packet: id:46378 Typ...		
8	12-04-2024 11:52:17.423	0.000	UDP	138	NBT Datagram ...	16detb513-05	NBT DGRAM Packet: id:43109 Typ...		
7	12-04-2024 11:52:17.423	0.000	UDP	138	NBT Datagram ...	16detb407-08	NBT DGRAM Packet: id:46750 Typ...		
6	12-04-2024 11:52:07.861	0.000	UDP	138	NBT Datagram ...	16detb510A-1	NBT DGRAM Packet: id:46808 Typ...		
5	12-04-2024 11:52:04.427	0.000	UDP	138	NBT Datagram ...	16detb415-15	NBT DGRAM Packet: id:40217 Typ...		
4	12-04-2024 11:51:58.928	0.000	UDP	138	NBT Datagram ...	16detb510B-0	NBT DGRAM Packet: id:46749 Typ...		
3	12-04-2024 11:51:38.704	0.000	UDP	138	NBT Datagram ...	16detb415-5	NBT DGRAM Packet: id:45883 Typ...		
2	12-04-2024 11:51:25.074	0.000	UDP	138	NBT Datagram ...	16detb510A-1	NBT DGRAM Packet: id:46378 Typ...		
1	12-04-2024 11:51:21.242	0.000	UDP	138	NBT Datagram ...	16detb416-23	NBT DGRAM Packet: id:44352 Typ...		

Event - 25

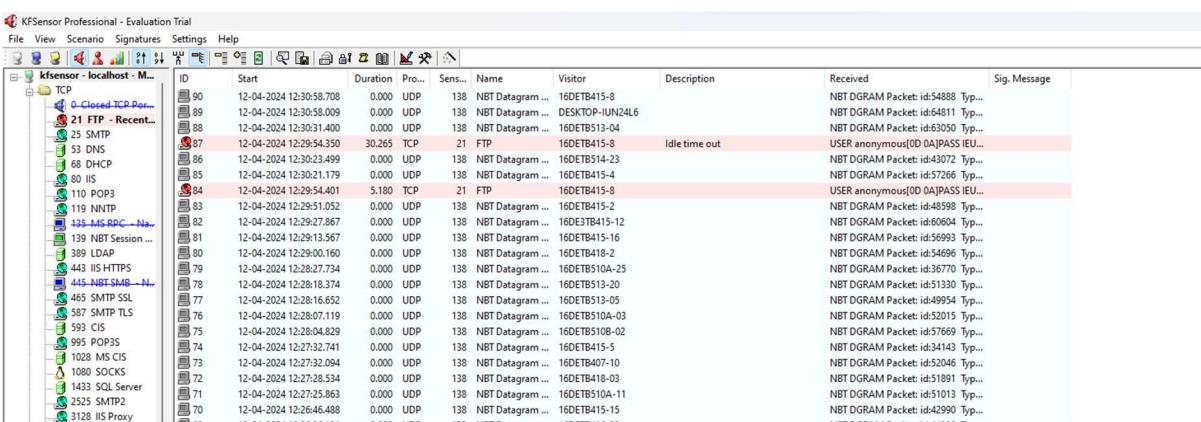
Sensor ID:	kfsensor
Event ID:	25
Start Time:	12-04-2024 11:56:15.558
Type:	Connection
End Time:	12-04-2024 11:56:15.558
Severity:	Low
Description:	
Closed By:	Visitor
Limit Exceeded:	
Received:	170 Bytes
Response:	0 Bytes
Visitor IP:	172.17.20.193
Port:	138
Domain:	16DET8407-08
Sensor Name:	NBT Datagram Service
IP:	
Port:	138
Bound:	
Protocol:	UDP
Action:	SimStdServer
Sim Server:	

Create Visitor Rule



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Name	Value
Sensor	kfsensor
Last status	12-04-2024 11:58:58.647
Status	Active
Running since	12-04-2024 11:50:47.649
Last restart	12-04-2024 11:51:05.711
Running for	8 minutes and 11 seconds
Scenario last up...	01-01-2016 05:30:00.000
Machine Name	16DETB415-8
DNS Name	16DETB415-8
Windows version	10.0.22621
Free disk space	28.994 gb
KFSensor version	5.8.0
Total Events	34
TCP Events	0
UDP Events	34
ICMP numEvents	0
Windows Events	0
Other Events	0





Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

NBT DGRAM Packet: id:64811 Type: EU...										
Event - 84										
Sensor ID: kfsensor Event ID: 84										
Start Time: 12-04-2024 12:29:54.401 Severity: High										
Description:										
Visitor IP: 172.17.20.68 Port: 52985										
Domain: 160ETB415-8										
Sensor Name: FTP										
Protocol: TCP Port: 21										
Signature:										
Message:										
Request Data - 66 Bytes										
USER anonymous PASS IEUser@ opts utf8 on syst site help PWD										
NBT DGRAM Packet: id:43120 Type: EU...										
Next Previous Close Help										

ID	Start	Duration	Proto...	Sens...	Name	Visitor	Description	Received	Sig. Message
89	12-04-2024 12:30:58.009	0.000	UDP	138	NBT Datagram ... DESKTOP-IUN24L6	160ETB415-8	Event - 93	USER anonymous[0D 0A]PASS IEU...	NBT DGRAM Packet: id:43120 Typ...
88	12-04-2024 12:30:51.400	0.000	UDP	138	NBT Datagram ... 160ETB513-04	160ETB415-8		NBT DGRAM Packet: id:43120 Typ...	NBT DGRAM Packet: id:65476 Typ...
87	12-04-2024 12:29:54.350	30.265	TCP	21	FTP	160ETB415-8		NBT DGRAM Packet: id:43120 Typ...	NBT DGRAM Packet: id:54888 Typ...
86	12-04-2024 12:30:23.499	0.000	UDP	138	NBT Datagram ... 160ETB510A-22	160ETB415-4			
85	12-04-2024 12:31:33.552	0.000	UDP	138	NBT Datagram ... 160ETB510A-12	160ETB415-4			
84	12-04-2024 12:29:54.401	5.180	TCP	21	FTP	160ETB415-8			
83	12-04-2024 12:29:51.052	0.000	UDP	138	NBT Datagram ... 160ETB510A-1	160ETB415-2			
82	12-04-2024 12:29:27.867	0.000	UDP	138	NBT Datagram ... 160ETB415-1	160ETB415-1			
81	12-04-2024 12:29:13.567	0.000	UDP	138	NBT Datagram ... 160ETB415-16	160ETB415-16			
80	12-04-2024 12:29:00.160	0.000	UDP	138	NBT Datagram ... 160ETB418-2	160ETB415-2			
79	12-04-2024 12:28:27.734	0.000	UDP	138	NBT Datagram ... 160ETB510A-1	160ETB415-2			
78	12-04-2024 12:28:18.374	0.000	UDP	138	NBT Datagram ... 160ETB513-20	160ETB415-2			
77	12-04-2024 12:28:16.652	0.000	UDP	138	NBT Datagram ... 160ETB513-05	160ETB415-3			
76	12-04-2024 12:28:07.119	0.000	UDP	138	NBT Datagram ... 160ETB510A-1	160ETB415-1			
75	12-04-2024 12:28:04.829	0.000	UDP	138	NBT Datagram ... 160ETB510B-1	160ETB415-5			
74	12-04-2024 12:27:32.741	0.000	UDP	138	NBT Datagram ... 160ETB415-5	160ETB415-5			
73	12-04-2024 12:27:32.094	0.000	UDP	138	NBT Datagram ... 160ETB407-10	160ETB415-4			
72	12-04-2024 12:27:28.534	0.000	UDP	138	NBT Datagram ... 160ETB418-03	160ETB415-4			
71	12-04-2024 12:27:25.863	0.000	UDP	138	NBT Datagram ... 160ETB510A-1	160ETB415-1			
70	12-04-2024 12:26:46.488	0.000	UDP	138	NBT Datagram ... 160ETB415-15	160ETB415-15			
69	12-04-2024 12:26:36.131	0.000	UDP	138	NBT Datagram ... 160ETB415-2	160ETB415-2			
68	12-04-2024 12:26:33.790	0.000	UDP	138	NBT Datagram ... 160ETB407-04	160ETB415-2			
67	12-04-2024 12:26:31.520	0.000	UDP	138	NBT Datagram ... 160ETB417-6	160ETB415-6			
66	12-04-2024 12:25:49.579	0.000	UDP	138	NBT Datagram ... 160ETB415-11	160ETB415-11			
65	12-04-2024 12:24:53.239	0.000	UDP	138	NBT Datagram ... 160ETB417-3	160ETB417-3			
64	12-04-2024 12:24:15.892	0.000	UDP	138	NBT Datagram ... 160ETB513-07	160ETB513-07			
63	12-04-2024 12:24:11.543	0.000	UDP	138	NBT Datagram ... 160ETB415-3	160ETB415-3			
62	12-04-2024 12:24:01.093	0.000	UDP	161	SNMP ... 160ETB415-2	160ETB415-2			
61	12-04-2024 12:24:00.086	0.000	UDP	161	SNMP ... 160ETB415-2	160ETB415-2			
60	12-04-2024 12:23:59.069	0.000	UDP	161	SNMP ... 160ETB415-2	160ETB415-2			
59	12-04-2024 12:23:30.004	0.000	UDP	138	NBT Datagram ... 160ETB410-09	160ETB415-2			
58	12-04-2024 12:23:24.884	0.000	UDP	138	NBT Datagram ... 160ETB407-15	160ETB415-2			
57	12-04-2024 12:22:56.174	0.000	UDP	138	NBT Datagram ... 160ETB419-2	160ETB415-2			
56	12-04-2024 12:22:25.389	0.000	UDP	138	NBT Datagram ... 160ETB417-02	160ETB417-02			
55	12-04-2024 12:22:14.672	0.000	UDP	138	NBT Datagram ... 160ETB407-02	160ETB407-02			
54	12-04-2024 12:22:01.238	0.000	UDP	138	NBT Datagram ... 160ETB415-7	160ETB415-7			
53	12-04-2024 12:21:32.954	0.000	UDP	138	NBT Datagram ... 160ETB407-08	160ETB407-08			
52	12-04-2024 12:21:10.727	0.000	UDP	138	NBT Datagram ... 160ETB513-06	160ETB513-06			

F FileZilla

File Edit View Transfer Server Bookmarks Help

Host: 172.17.20.68 Username: Vatsal Password: ***** Port: Quickconnect

Status: Insecure server, it does not support FTP over TLS.

Command: USER Vatsal

Response: 331 Password required for Vatsal.

Command: PASS *****

Response: 530 User cannot log in.

Error: Critical error: Could not connect to server



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Name	Value
Sensor	kfsensor
D	
D-Closed TCP Port	
21 TCP - Recent...	
25 SMTP	
53 DNS	
68 DHCP	
80 IIS	
110 POP3	
119 NNTP	
135 MS-RPC - Na...	
139 NBT Session ...	
389 LDAP	
443 IIS HTTPS	
445-NBT-SMB - N...	
455 SMTP SSL	
587 SMTP TLS	
593 CIS	
995 POP3S	
1028 MS CIS	
1080 SOCKS	
1433 SQL Server	
2525 SMTP2	
3128 IIS Proxy	
3389-Terminal-Service	
5000 MS Util Plug...	
5357 Web Service...	
5358 Web Service...	
8008 IIS Proxy	
8080 IIS Proxy	
UDP	
D-Closed UDP Port	
42 WINS UDP	
53 DNS UDP	
67 DHCP	
68-DHCP Client...	
88 Kerberos	
137 NBT Name Se...	
138 NBT Datagram...	
161 SNMP - Re...	
389 LDAP	
500-IPSec-Nativ...	
1026 MS Messen...	



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Postlab questions:

1. Differences and similarities between honeypot and firewall.

Differences:

- Purpose: A firewall is primarily designed to prevent unauthorized access to or from a private network, whereas a honeypot is designed to lure attackers and gather information about their tactics, techniques, and procedures (TTPs).
- Functionality: Firewalls analyze and control incoming and outgoing network traffic based on predetermined security rules, while honeypots passively monitor and attract malicious activity without actively blocking or allowing traffic.
- Deployment: Firewalls are typically deployed at network perimeters or within the network to regulate traffic flow, while honeypots are deployed within the network or in a DMZ (Demilitarized Zone) to deceive attackers and gather intelligence.

Similarities:

- Both aim to enhance network security by identifying and mitigating threats.
- Both can be part of a comprehensive cybersecurity strategy to protect network resources.

2. In a network architecture, what are the possible placements of honeypots in the design of the network?

Honeypots can be placed at various points within a network architecture, including:

- Inside the internal network: Deployed alongside legitimate assets to detect insider threats or lateral movement by attackers who have breached perimeter defenses.
- In a DMZ (Demilitarized Zone): Positioned between the internal network and external-facing services to attract and monitor attacks targeting publicly accessible systems, such as web servers or email servers.
- Outside the network perimeter: Placed in the Internet-facing zone to intercept and analyze incoming threats before they reach the internal network, providing early warning and intelligence gathering capabilities.

3. Discuss strengths and weaknesses of honeypots.

Strengths:

- Threat detection: Honeypots can detect previously unknown threats and zero-day attacks by attracting and monitoring malicious activity that might evade traditional security measures.
- Intelligence gathering: They provide valuable insights into attacker tactics, techniques, and procedures (TTPs), which can be used to improve security posture, develop better defenses, and enhance incident response.
- Deception: Honeypots deceive attackers by presenting enticing targets, diverting their attention from critical assets, and wasting their time and resources.

Weaknesses:

- Resource-intensive: Honeypots require dedicated resources for setup, maintenance, and monitoring, which can strain IT infrastructure and personnel resources.
- False positives: They may generate false alerts or attract benign activity that mimics malicious behavior, leading to unnecessary investigations or alarms.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

- Increased risk: Honeypots, if not properly configured and isolated, can pose a security risk by becoming compromised and used as launching pads for attacks against the rest of the network.