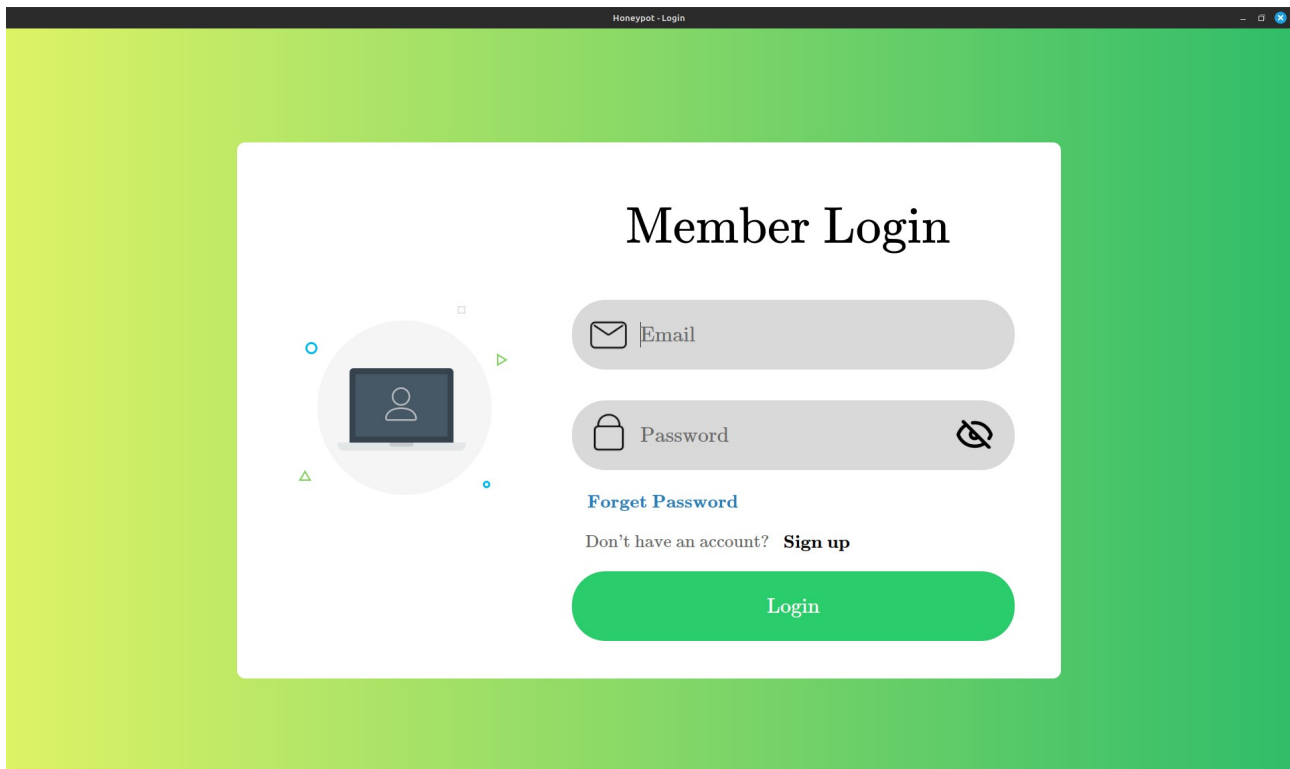


Honeypot Project Screenshots

Login Page:



The screenshot shows a web browser window titled "Honeypot - Login". The page has a green gradient background. In the center, there is a white card with the title "Member Login". To the left of the login fields is an illustration of a laptop with a user icon on its screen, surrounded by small blue and green geometric shapes. The login fields consist of an "Email" input field with an envelope icon and a "Password" input field with a lock icon and a toggle eye icon. Below the password field are links for "Forgot Password" and "Don't have an account? Sign up". At the bottom of the card is a large green "Login" button.

Member Login

Email

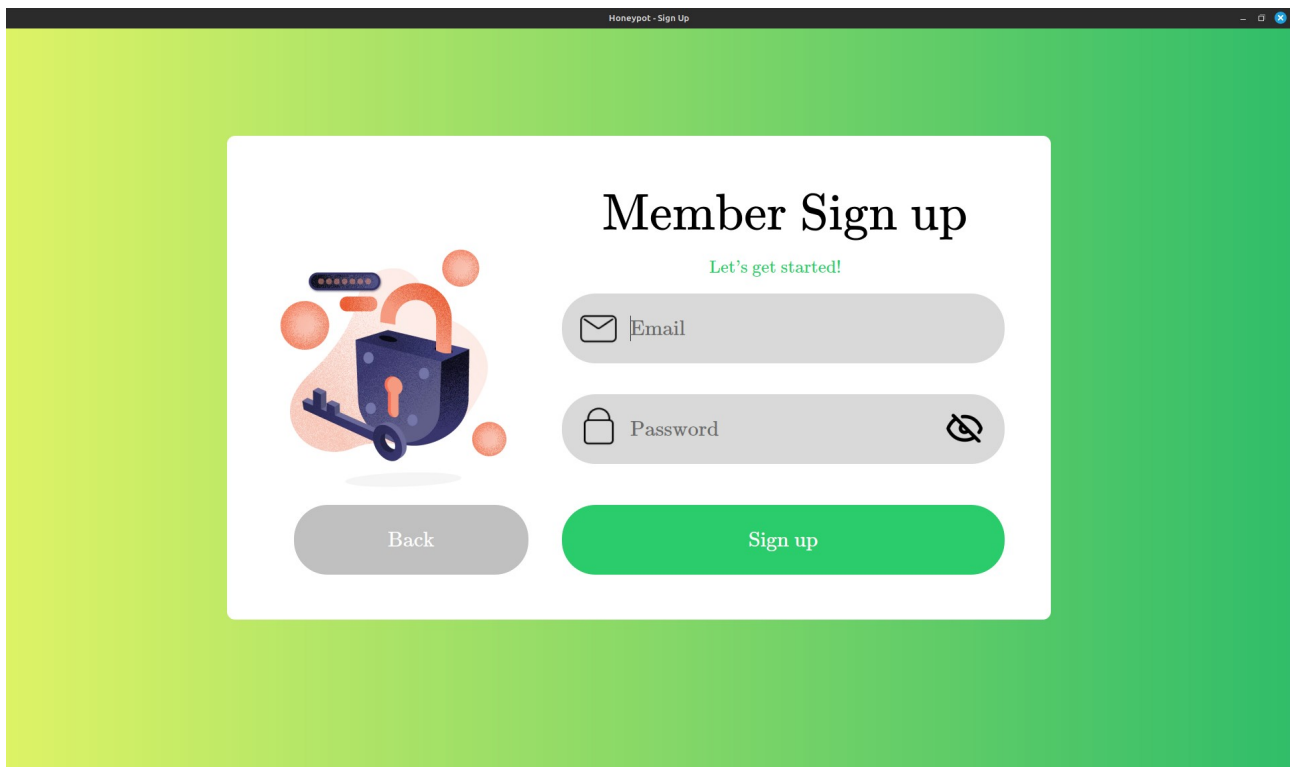
Password

[Forgot Password](#)

Don't have an account? [Sign up](#)

Login

Sign Up Page:



The screenshot shows a web browser window titled "Honeypot - Sign Up". The page has a green gradient background. In the center, there is a white card with the title "Member Sign up". To the left of the sign-up fields is an illustration of a blue padlock with an orange keyhole, surrounded by orange and red geometric shapes. Above the sign-up fields is the text "Let's get started!". The sign-up fields consist of an "Email" input field with an envelope icon and a "Password" input field with a lock icon and a toggle eye icon. Below the password field are buttons for "Back" and "Sign up".

Member Sign up

Let's get started!

Email

Password


[Back](#) [Sign up](#)

Reset Password Page:

Honeypot - Reset Password Page

Reset Password

Please ensure the email address is correct. A password reset code will be sent to this address.

 Email

Cancel **Continue**

Honeypot - Reset Password Page

Reset Password


Please enter the code sent to [REDACTED] to reset your password.


9 0 4 5 1 3


Cancel **Back** **Verify**


Honeypot - Reset Password Page

Reset Password

 Password



 Confirm Password




Cancel

Back

Reset Password

Welcoming Page:

Honeypot

 Honeypot

Welcome

Dashboard

Network Monitor

Firewall Management

File Integrity

Remote Shell

File Security

IP Investigator

Capture Evidence


Logout

Welcome

Welcome to Honeypot panel,
Are you ready to explore cyber war threats?

Get Started!

Dashboard Page:

Honeypot

Welcome

Dashboard

Network Monitor

Firewall Management

File Integrity

Remote Shell

File Security

IP Investigator

Capture Evidence

Logout

Dashboard

Connections:

Detected TCP traffic to 35.174.127.31:443 from 192.168.8.198

Detected TCP traffic to 35.174.127.31:443 from 192.168.8.198

Detected TCP traffic to 192.168.8.198:42640 from 35.174.127.31

Detected TCP traffic to 35.174.127.31:443 from 192.168.8.198

Detected TCP traffic to 192.168.8.198:42640 from 35.174.127.31

Detected TCP traffic to 34.237.73.95:443 from 192.168.8.198

Detected TCP traffic to 34.237.73.95:443 from 192.168.8.198

Detected TCP traffic to 192.168.8.198:45508 from 34.237.73.95

Detected TCP traffic to 192.168.8.198:45508 from 34.237.73.95

Detected TCP traffic to 192.168.8.198:45508 from 34.237.73.95

Detected TCP traffic to 34.237.73.95:443 from 192.168.8.198

Unique Detected Traffic:

{'Detected TCP traffic to 34.237.73.95 from 192.168.8.198',

'Detected UDP traffic to 192.168.8.1 from 192.168.8.198',

'Detected TCP traffic to 34.215.93.114 from 192.168.8.198',

'Detected TCP traffic to 13.69.109.131 from 192.168.8.198',

'Detected TCP traffic to 35.174.127.31 from 192.168.8.198'}

Protocol Type:

TCP Connections: 22, UDP Connections: 6


Opened Ports (Port number, Number of times):

[(443, 12), (45508, 5), (42640, 3), (53, 3), (56950, 1), (45760, 1), (49660, 1), (35748, 1), (35492, 1)]

Top Attacking IPs (IP Address, Attempts):

[(('192.168.8.198', 13), ('35.174.127.31', 5), ('34.237.73.95', 5), ('192.168.8.1', 3), ('13.69.109.131', 1), ('34.215.93.114', 1))]

Network Monitor:

Honeypot

Welcome

Dashboard

Network Monitor

Firewall Management

File Integrity

Remote Shell


File Security

IP Investigator

Capture Evidence

Logout

Network Monitor

Interface: wlp43s0Duration: 1

frame.number,frame.time,eth.src,eth.dst,ip.src,ip.dst,tcp.srcport,tcp.dstport,udp.srcport,udp.dstport,frame.len

1,Jun 3, 2025 16:54:50.062153646 +03,,,,,443,51105,109

2,Jun 3, 2025 16:54:50.062153904 +03,,,,,52

3,Jun 3, 2025 16:54:50.069265981 +03,,,,,443,51105,1514


4,Jun 3, 2025 16:54:50.083063669 +03,,,,,51105,443,101

5,Jun 3, 2025 16:54:50.062153646 +03,,,,,443,51105,109

6,Jun 3, 2025 16:54:50.062153904 +03,,,,,52

7,Jun 3, 2025 16:54:50.069265981 +03,,,,,443,51105,1514

8,Jun 3, 2025 16:54:50.083063669 +03,,,,,51105,443,101

Download

Firewall Management:

The screenshot shows the Honeypot Firewall Management interface. On the left is a sidebar with navigation links: Welcome, Dashboard, Network Monitor, Firewall Management (highlighted), File Integrity, Remote Shell, File Security, IP Investigator, and Capture Evidence. At the bottom of the sidebar is a Logout button. The main area is titled 'Firewall Management' in green. Below the title, there's a 'Status:' section with three buttons: 'Enable' (green), 'Disable', and 'Reload'. To the right of the status buttons is a refresh icon. Below this is a 'Current Rules:' section. It contains a table with three columns: 'To', 'Action', and 'From'. The table lists two rules: [1] 22/tcp, DENY OUT, Anywhere (out) # Block SSH; and [2] 22/tcp (v6), DENY OUT, Anywhere (v6) (out) # Block SSH. At the bottom right of the main area are two buttons: 'Add' (green) and 'Delete' (red).

To	Action	From
[1] 22/tcp	DENY OUT	Anywhere (out) # Block SSH
[2] 22/tcp (v6)	DENY OUT	Anywhere (v6) (out) # Block SSH

Add Rule:

The screenshot shows the 'Add a Firewall Rule' dialog. It has a title bar 'Honeypot - Add Rule'. The dialog contains several input fields: 'Name:' with the value 'Block SSH'; 'Source:' with the value 'any'; 'Destination:' with the value 'any'; 'Policy:' with a dropdown menu showing 'Deny'; 'Direction:' with a dropdown menu showing 'Out'; 'Protocol:' with a dropdown menu showing 'TCP'; and 'Port:' with the value '22'. At the bottom are two buttons: 'Close' (red) and 'Add' (green).

Delete Rule:

The screenshot shows the 'Delete a Firewall Rule' dialog. It has a title bar 'Honeypot - Delete Rule'. The dialog contains a text input field with the placeholder text 'Enter the number of the rule: *' and 'Number within the square brackets []'. At the bottom are two buttons: 'Close' (red) and 'Delete' (green).

File Integrity:

The screenshot shows the Honeypot File Integrity interface. On the left is a sidebar with a 'Honeypot' logo and a list of navigation items: Welcome, Dashboard, Network Monitor, Firewall Management, File Integrity (highlighted), Remote Shell, File Security, IP Investigator, and Capture Evidence. At the bottom of the sidebar is a 'Logout' button. The main area has a title 'File Integrity' in green. Below the title is a 'Path:' label followed by a text input field containing '/home/user/file.txt'. A yellow warning icon is next to a note: 'Note: To check file integrity, this feature must be used before any changes made to file.' At the bottom right of the main area are two green buttons: 'Check' and 'Add'.

Remote Shell:

The screenshot shows the Honeypot Remote Shell interface. The sidebar is identical to the File Integrity interface, with 'Remote Shell' highlighted. The main area has a title 'Remote Shell' in green. Below the title is a 'Command:' label followed by a text input field containing 'cd Desktop ; cat test.py'. To the right of the input field is a green status indicator. Below the command field is an 'Output:' label followed by a large text area containing the following Python code:


```
# rpc_client.py
import xmlrpc.client

class RPC_Client:
    def __init__(self):
        self.proxy = None
        self.server_url = None

    def connect_to_server(self, server_url="http://192.168.8.212:8000"):
        """Attempts to connect to the RPC server and returns the connection status."""
        self.server_url = server_url
        try:
            self.proxy = xmlrpc.client.ServerProxy(self.server_url)
            print(f'Connected to RPC Server at {self.server_url}')
            return self.proxy, True
        except ConnectionRefusedError as e:
```

At the bottom right of the main area are three buttons: 'Connect to SSH Server' (green), 'Close connection' (red), and 'Send' (gray).

File Security:

HoneyPot

Home

Dashboard

Network Monitor

Firewall Management

File Integrity

Remote Shell

File Security

IP Investigator

Capture Evidence

Logout

File Security

Path: Upload Attributes

☒ Append Only ?

☐ Undeletable ?

☐ No Tail-merging ?

☒ No Atime Updates ?

☐ No Dump ?

☒ Immutable ?

☐ Compressed ?

☐ Don't Compress ?

☐ Journaled Data ?

☐ Secure Deletion ?

☐ Synchronous Updates ?

Apply Attributes

IP Investigator:

HoneyPot

Home

Dashboard

Network Monitor

Firewall Management

File Integrity

Remote Shell

File Security

IP Investigator

Capture Evidence

Logout

IP Investigator

Search:

IP Address: 8.8.8.8
Public IP: True
IP Version: 4
Whitelisted: True
Abuse Confidence Score: 0
Country Name: United States
Usage Type: Content Delivery Network
ISP: Google LLC
Domain: google.com
Hostnames: ['dns.google']
Tor Exit Node: False
Total Reports: 262
Distinct Users Reporting: 59
Last Reported At: 2025-06-03T14:04:03+00:00

Search

Report an IP Address

Report IP Address:

Honeypot - Report IP

IP Address * (ex. 8.8.8.8)

192.168.8.100

Categories * (at least one is required)

☐ DNS Compromise ?

☒ DDoS Attack ?

☐ Email Spam ?

☒ Brute-Force ?

☐ DNS Poisoning ?

☐ Open Proxy ?

☒ Port Scan ?

☐ Bad Web Bot ?

☐ Fraud Orders ?

☐ Web Spam ?

☐ Spoofing ?

☐ Exploited Host ?

☐ Web App Attack ?

☐ FTP Brute-Force ?

☐ Fraud VoIP ?

☐ Hacking ?

☐ SSH ?

☐ Ping of Death ?

☐ Blog Spam ?

☐ SQL Injection ?

☐ IoT Targeted ?

☐ Phishing ?

☐ VPN IP ?


Comment

Comment (server log snippets, abuse details, etc)

Close

Report IP Address

Capture Evidence:

 Honeypot

Home

Dashboard

Network Monitor

Firewall Management

File Integrity

Remote Shell

File Security

IP Investigator

Capture Evidence

Logout

Capture Evidence

Company Name or Client Name:

King Khalid University

Generate Evidence File



Honeypot Report

Incident Response: Honeypot Data To Analysis

Creation Date: 2025-06-03

Prepared for:
King Khalid University

Prepared by:
Honeypot Team

BRIEF CONTENTS

Chapter 1: System Information:

Chapter 2: Disk and Storage:

Chapter 3: Network Information:

Chapter 4: Process Management:

Chapter 5: User Specific Information:

Chapter 6: Logging: