RR

# Phishing Analysis

A user has received a phishing email and forwarded it to the SOC. Can you investigate the email and attachment to collect useful artifacts?

Text Editor   Mozilla Thunderbird   URL2PNG   WHOis

| Points | Difficulty | Solves | OS |
|---|---|---|---|
| 10 | Easy | 14053 | Windows |

Phishing Email
7KB

Password
btlo

Download File

## First-Blood

Hataker 1687 days ago

## Created By

BTLO 1687 days ago

## Recent Solves

| | | |
|---|---|---|
| FS | Fadhli Hadi Surya | Today |
| ND | Nurul Aulia Dewi | Today |
| AA | aab abdullah | Today |
| HA | Hana | Today |
| BE | Budi Tri Effendi | Today |

## Scenario

Scenario

A user has received a phishing email and forwarded it to the SOC. Can you investigate the email and attachment to collect useful artifacts?

⚠ Found an issue with this challenge? Click here to report it!

## Challenge Submission

Who is the primary recipient of this email? *(1 points)*

Solved!

What is the subject of this email? *(1 points)*

Solved!

What is the date and time the email was sent? *(1 points)*

Solved!

What is the Originating IP? *(1 points)*

Solved!

Perform reverse DNS on this IP address, what is the resolved host? (whois.domaintools.com) *(1 points)*

Solved!

What is the name of the attached file? *(2 points)*

Solved!

What is the URL found inside the attachment? *(1 points)*

Solved!

What service is this webpage hosted on? *(1 points)*

Solved!

Using URL2PNG, what is the heading text on this page? (Doesn't matter if the page has been taken down!) *(1 points)*

Solved!