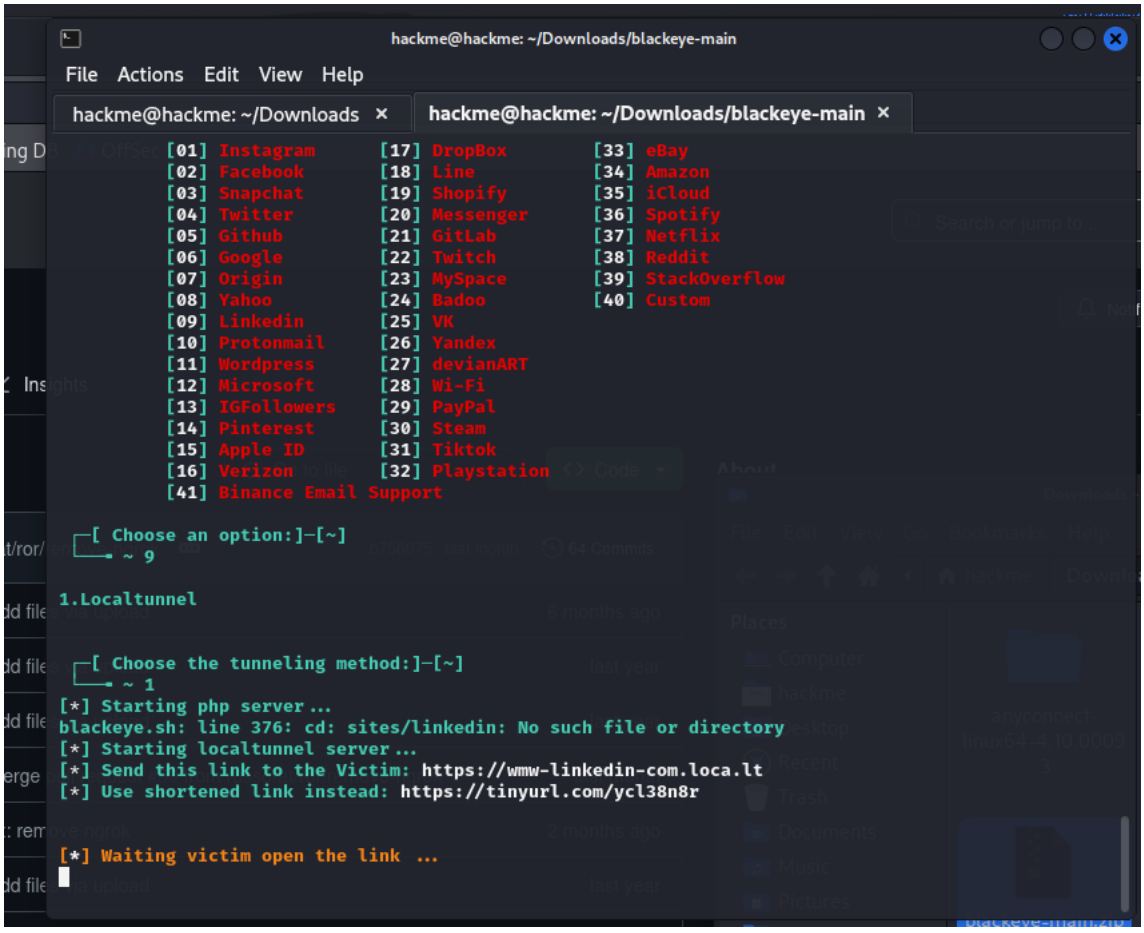
Social engineering on AMIR ZANDIEH

We will offer him a job to her LinkedIn profile as we have her LinkedIn profile. First we will create the fake LinkedIn website. The social engineering attack we are doing is credential harvesting.

We will use kali default “blackeye” tool to send the phishing link.



Blackeye tool generating link

Now we will send the email to AMIR ZANDIEH offering him a job with the link https://wmw-linkedin-com.loca.lt. If he fall for it she will put the credential on the clone fake LinkedIn and we will see it.

We will use SET toolkit to send the email

Shell No. 1
File Actions Edit View Help
set:mailer>1
Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template
set:phishing>2
set:phishing> Subject of the email: Exciting Career Opportunity at BrightTech Innovations – Join O
ur Team!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Dear AMIR ZANDIEH,
I hope this message finds you well. We came across your impressive background and experience, and
we believe you'd be an excellent fit for an exciting opportunity here at BrightTech Innovations, a
leading company in tech solutions and innovation.
We are currently expanding our team and are looking for skilled professionals like you to help dri
ve our projects forward. Based on your expertise, we'd love to invite you to explore this role fur
ther and submit your application through the link below:
https://wmw-linkedin-com.loca.lt
We would be thrilled to discuss how your talents can align with the vision of BrightTech Innovatio
ns. If you have any questions or need additional details, feel free to reach out.
Looking forward to your response!
Best regards,
James Anderson
Recruitment Lead
BrightTech Innovations
james.anderson@brighttechinnovations.com
Next line of the body: Next line of the body: Next line of the body: Next line of the body: Next l
ine of the body: Next line of the body: Next line of the body: Next line of the body: Next line of
the body: Next line of the body: Next line of the body: Next line of the body: Next line of the b
ody: Next line of the body: Next line of the body:

Shell No. 1
File Actions Edit View Help
we believe you'd be an excellent fit for an exciting opportunity here at BrightTech Innovations, a
leading company in tech solutions and innovation.
We are currently expanding our team and are looking for skilled professionals like you to help dri
ve our projects forward. Based on your expertise, we'd love to invite you to explore this role fur
ther and submit your application through the link below:
https://wmw-linkedin-com.loca.lt
We would be thrilled to discuss how your talents can align with the vision of BrightTech Innovatio
ns. If you have any questions or need additional details, feel free to reach out.
Looking forward to your response!
Best regards,
James Anderson
Recruitment Lead
BrightTech Innovations
james.anderson@brighttechinnovations.com
Next line of the body: Next line of the body: Next line of the body: Next line of the body: Next l
ine of the body: Next line of the body: Next line of the body: Next line of the body: Next line of
the body: Next line of the body: Next line of the body: Next line of the body: Next line of the b
ody: Next line of the body: Next line of the body: END
set:phishing> Send email to: azandieh@deakin.edu.au
1. Use a gmail Account for your email attack.
2. Use your own server or open relay
set:phishing>1
set:phishing> Your gmail email address: james12345567788gh@gmail.com
set:phishing> The FROM NAME the user will see: James Anderson
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails

Email send