

SOCIAL ENGINEERING WORKSHOP

by Oleksandr Goranskyy

RnD Day 2019

epages



AGENDA



1. What is Social Engineering 
2. Information gathering 
3. Delivery methods 
4. Exploitation 
5. Post-exploitation 
6. How to protect yourself 



WHAT IS SOCIAL ENGINEERING



"any act that influences a person to take an action that may or may not be in their best interest."

SOCIAL HACKING

- Phishing 
- Vishing 
- Impersonation 



INFORMATION GATHERING



- SOCMINT - Social media intelligence
- OSINT - Open-source intelligence
- Maltego - a popular tool for OSINT

DELIVERY METHODS



- Phishing emails
- Infected USB
- BeEF



EXPLOITATION 😈

- "Reverse shell"
- meterpreter
- VEIL, Empire, MSVENOM



POST-EXPLOITATION



- upgrade dropper to trojan
- gain more privileged access
- harvest passwords and other personal data
- use victim computer as a pivot to spread throughout the network



HOW TO PROTECT YOURSELF



- always check the urls and email addresses
- do not insert random usb sticks in your computer
- only no-script plugin can save agains BeEF
- always doublecheck
- know your coworkers



QUESTIONS?

