DISCLAIMER:
This session contains security stuff, sexual content and strong language- basically all the good stuff

OSINT

Open-Source Intelligence

(HOW TO BE CREEPY ONLINE 101)

What is it?

OSINT is produced from publicly available information

- Metadata
- News articles
- Social media posts
- Public data(govt. Records, statements, etc.)

Why do OSINT?

- First step of gaining access to any target(Recon)
- To better understand one’s internet presence
- To better get a grab on business competitions
- To profile a person
- To find weak points in your network

Recon, what is that?

- Recon is short for *reconnaissance*
- There’s two types:
  - Active recon(illegal without authorization)
  - Passive recon(mostly legal)

Active recon

Warning: Illegal without authorization, can lead to jail-term and heavy fines

- Port scans
- Vulnerability scan

Passive recon

- Whois lookup
- Reverse DNS lookup
- Metadata of publicly available content
- Database dumps
- Robots.txt
- Google dorks
- Shodan.io

Whois lookup

- Owner contact information
- Domain registrar
- Domain tenure

Reverse DNS lookup

Metadata from websites

CASE STUDY: pragyan.org

Step 1 :Understanding the target

Step 2: Understanding the state of software stack

Step 3: Identifying (applicable)vulnerabilities

CASE STUDY 2: vitap.ac.in

Step 1: Listing all web pages in the domain

Step 2: Accessing robots.txt and (hopefully) finding admin page

Step 3: Looking up shodan.io to find more information

SCADA – Where stability matters more than security

- **What are they?**

  Power plants, wind farms, factories, temperature control systems

- **Why should I know about them?**
  Cyber war now means taking down SCADA systems.
  SCADA is the backbone of any country

SCADA communication protocols

Protocol	Port	Application
Modbus	502	Powerplants, Dams, electricity grid
S7	102	Phone records and directories
Fox protocol (Niagara framework)	1911,4911	Building automation
Universal Plug and Play(upnp)	80, 443(mostly)	IoT

Database dumps

Check the following websites:

- havibeenpwned.com
- Pasebin.com
- Piratebay.com
- Data.ddosecrets.com
- Torum (Darknet)
- Intel repository (Darknet)

Following the money trail(crypto)

- Money is laundered using cryptocurrencies
- Bitcoin is pseudonymous – with enough processing power, transactions can be traced
- Bitcoin is the most popular currency on dark net markets

Trace Labs: Finding Missing People

Can OSINT get me into trouble?

- Sometimes, yes. It cost Aron Swartz, a genius coder and the co-founder of Reddit , his life. He was 26.
- General rule of thumb: limit direct interaction with target and don’t touch anything that’s behind an authentication firewall.