

Passive Reconnaissance



Alexander Tushinsky

Cybersecurity & Software Development Consultant

@ltmodcs alextushinsky.com



Overview



- Reconnaissance
 - What is reconnaissance?
 - Why is this important?
 - Types of reconnaissance
 - Passive reconnaissance



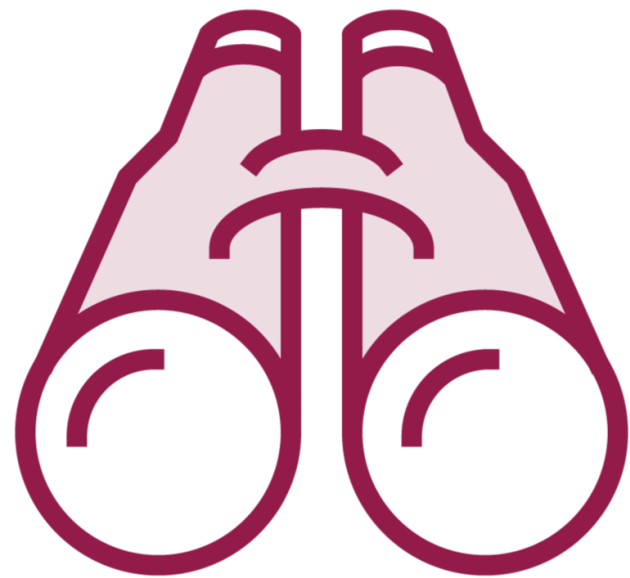
Reconnaissance Overview





Phases of a Penetration Test

- Engagement and project initiation
- Information Gathering
 - Passive Reconnaissance
 - Active Reconnaissance
- Vulnerability Assessment
- Exploitation
- Reporting
- Project close-out



Passive Reconnaissance

- No direct interaction with the target
- Uses publicly known sources

Active Reconnaissance

- Actions against target resources
- Uses information obtained during passive reconnaissance and expands on it further



Passive Reconnaissance

- Leads to the identification of attack vectors
- Provides valuable details of the attack surface
- Saves time later

Passive Reconnaissance





Passive Reconnaissance

- Company information
- Who are the employees?
- Infrastructure details
- Technology being used
- Domain and sub-domain information
- What does Google know?



Open-source Intelligence

- Google and the Exploit Database
- LinkedIn.com and Indeed.com
- Hunter.io
- MxToolBox.com
- DNSDumpster.com & Crt.sh
- Shodan.io
- Dehashed.com and HavelBeenPwnd.com
- OSINT Framework
- Maltego, TheHarvester and MetaGooFil
- Spiderfoot.net
- OWASP Amass



Open-source – Additional Tools

- Google Image Search & PimEyes.com
- Yandex
- JupyterPen
- Social Media
- <https://attack.mitre.org/>





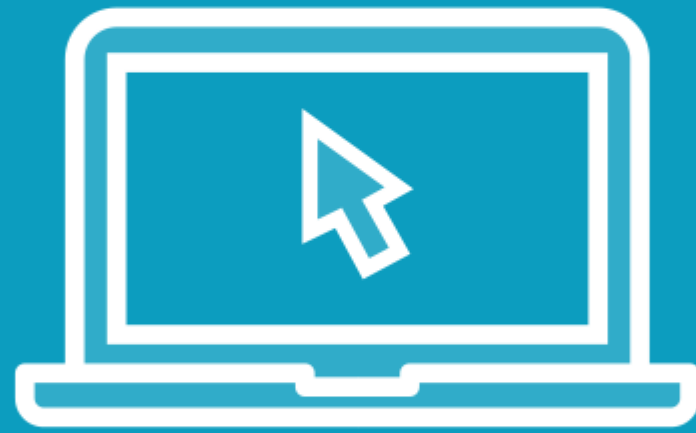
More Information

Red Team Tools

<https://app.pluralsight.com/paths/skill/red-team-tools>



Demo



Passive Recon - Infrastructure

- LinkedIn and Indeed
- Shodan.io



Demo



Passive Recon – User Enumeration

- [Hunter.io](#)
- [Dehashed.com](#)



Demo



Passive Recon – Automation

- Google Dorks
- MetaGooFil
- theHarvester
- OWASP Amass

