Module 9: Information Gathering and Reconissance

PASSIVE RECON OVERVIEW:

Physical/ Social
-Location information
-satellite images
-Drone recon
-Building layout (badge readers, break areas, security, fencing)
-Job information
-Employees (name, job title, phone number, manager, etc)
-pictures (badge photos, desk photos, computer photos, etc)

Web/Host
-Target Validation (WHOIS, nslookup, dnsrecon)
-Finding Subdomains (Google Fu, dig, Nmap, sublist3r, Bluto, crt.sh, etc.)
-Fingerprinting (Nmap Wappalyzer, WhatWeb, BuildWith, Netcat)
-Data Breaches (HavelBeenPwned, Breach-Parse, WeLeakInfo)

Bugcrowd.com is a bugbounty website that can be used to practice and also make a bit of cash

---

Email Address Gathering with Hunter.io

-Start with items on websites regarding users, email format, breach credentials

---

Visit Hunter.io

Use Hunter.io to Search for companies and their email information/patterns/list of people etc. LOTS of information

---

Gather Breached Credentials with Breach-Parse

https://github.com/hmaverickadams/breach-parse

**need to search how to find username and password dumps

Utilizing theHarvester
This tool is in kali linux to help us to find usernames/passwords etc.

HUNTING SUBDOMAINS

Wildcard "*"

"*.tesla.com" means we can search any .tesla.com subdomain

Kali Tool "sublister" - used to get subdomains
OR
use crt.sh (looks for certificates) subdomains

OWASP AMASS is one of the best tools to use. Find it at github or it comes in kali linux repositiory (NEED TO WATCH TUTORIALS ON THIS)

IDENTIFYING WEBSITE TECHNOLOGIES

Looking at what a website is built with

WEBSITE TECH
BuiltWith.com (which frameworks are the sites running on, programming language, etc

A better way ->wappalyzer (Chrome or firefox extension)

Shows content management system, programming languages, etc.

whatweb (kali) - gives us similar information but its a bit messy

BURPSUITE - Web proxy (intercepts web traffic) (NEED TO WATCH TUTORIALS ON THIS)

GOOGLE FU (Using google to find stuff is crucial) *Google search syntax*

Using Social Media
Looking for things like badge photos, environments, deskstuff, etc.
-Linkdin
-facebook

-twitter

*What kind of credentials can we gather? Look for breached credentials etc

People are always the weekest point in any company