Identifying Infrastructure Assets

Jerod Brennen
CISSP, INFOSEC GEEK

@slandail www.slandail.net

Overview

Technical Footprint

Interactive Applications

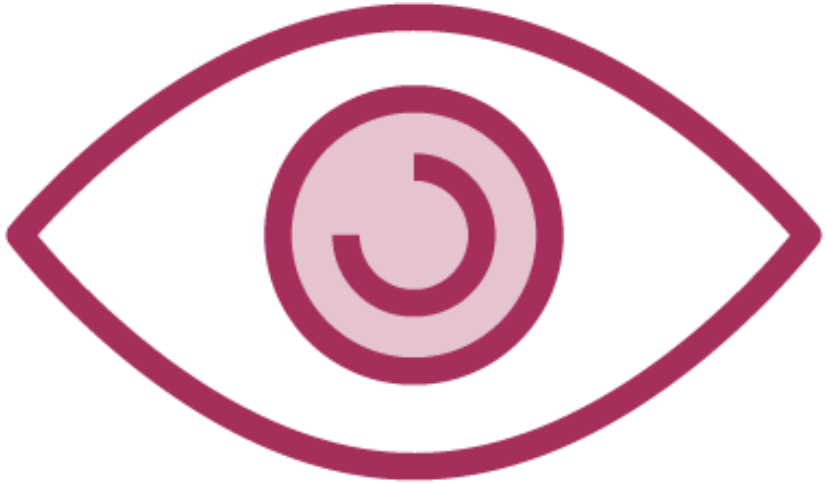
Defensive Capabilities

Network Blocks (L1)

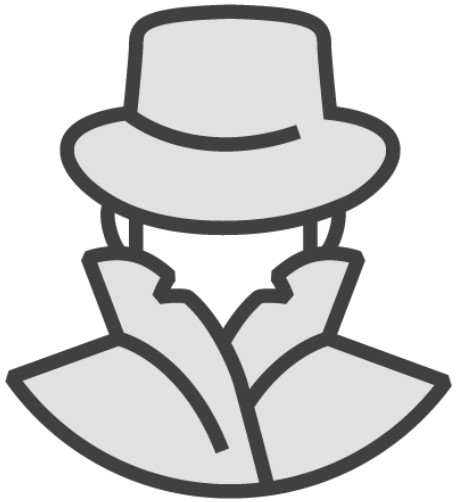
Network Block

Each range of IP addresses considered in-scope for the penetration test

Visibility



Active



Passive

DNSStuff Toolbox

- http://www.dnsstuff.com/tools

Zone Transfer

Whois

- Name Servers
- Contacts
  - Registrant
  - Administrative
  - Technical

Hurricane Electric BGP Toolkit

- http://bgp.he.net/

CIDR > DNS

- PTR records
- IP addresses

Recon-ng

- https://bitbucket.org/LaNMaSteR53/recon-ng

Whois Data Miner

- whois_miner

Netblocks as input

- whois_orgs
- reverse_resolve
- shodan_net
- census_2012
- sonar_cio

Email Addresses (L1)

Derivative Information

Usernames

Domain Structure

Headers

Where?

Company Website

LinkedIn

Search Engine Queries

Automated Scripts and Tools

```
mailto company_domain.com

site:company_domain.com directory
```

Search Engine Queries

Usage: Identify email addresses associated with the target organization.

Maltego Community Edition (CE)

- https://www.paterva.com/

Run Machine > Company Stalker

Maltego CE vs. Maltego Classic

API key

- CE = 12 results

TheHarvester

- http://www.edge-security.com/theharvester.php
- https://github.com/laramies/theHarvester

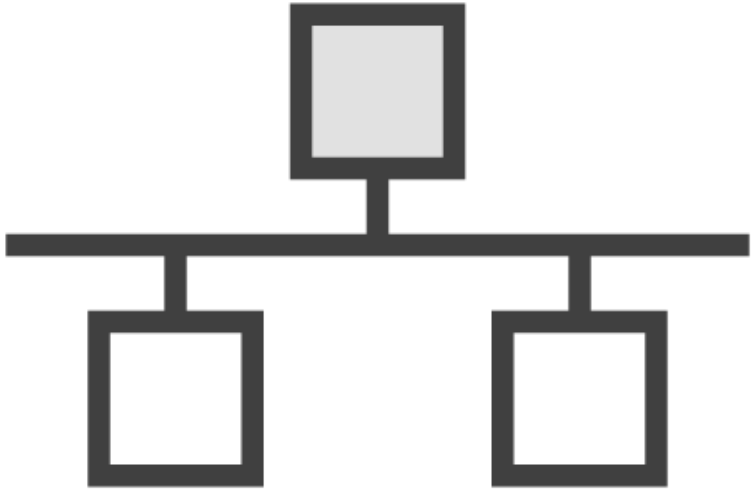
Passive and Active

LinkedIn domain search

External Infrastructure Profile (L1)

External -> Internal

External Network



Internal Network

Shodan

- https://shodan.io/

Internet-connected devices

Basic search: *domain_name*

org:"*organization_name*"

Available Services

Web Server Banners

Operating Systems

Geolocations

Product Names

Shodan Results

CVE Details

- https://www.cvedetails.com/

Extract version info from Shodan results

Search for exploitable vulnerabilities

- Remote Code Execution (RCE)

```
site:cvedetails.com product_name version
```

Search Engine Queries

Usage: Identify known product vulnerabilities, based on product name and version.

Robtex

- https://www.robtex.com/

Hostname or IP Address

Results

- Summary
- Forward
- Shared
- Graph

IP Addresses

IPv4

IPv6

Mail Servers

Name Servers

Names Pointing to Same IP Address

Domains Using Same Mail Servers

Robtex Results

MX record

NS record

A record

PTR record

SOA record

- **Mail Exchanger**
  Specify mail server(s) and prioritize mail delivery
- **Name Server**
  Prioritize domain and subdomain resolution
- **Address**
  Map domain to IPv4 address
- **Pointer**
  Perform reverse DNS lookups
- **Start of Authority**
  Information about DNS zone and other DNS records

Technologies Used (L1/L2)

Sources of Information

Job Postings

Support Forums

Popular Tech Support Forums

Reddit

- /r/sysadmin
- /user/*username*

Tom's Hardware

Specific technology vendor

When is social engineering not social engineering?

Social Engineering Scenarios - Vendors

New Employee

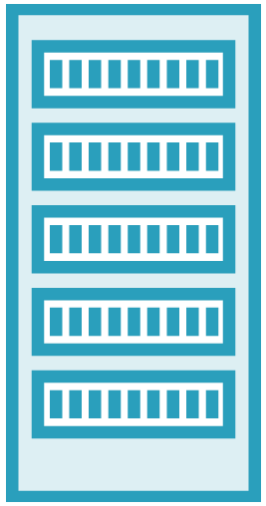
Filling in for normal admin, seeking case history

Manager

Considering expanding licenses, need current info

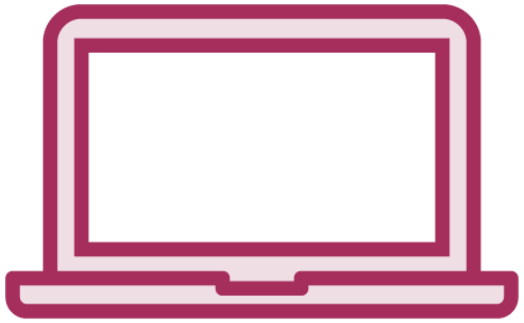
Purchase Agreements (L1/L2/L3)

Purchase Agreements Content



Hardware Licenses

Software Licenses



Existing Assets

```
“company_name” “purchase agreement” filetype:pdf
site:company_domain.com “purchase agreement”
```

Search Engine Queries

Usage: Locate purchase agreements.

Remote Access (L1/L2)

How do employees, clients, and/or vendors connect to the network?

Targets

Remote Access Portals

"How To" Documents

Support Portals

Mobile Device Management

SSL/TLS

Port 443

Port 8443

IPSec

Internet Protocol Security

IKE

Internet Key Exchange

Virtual Private Networks (VPNs)

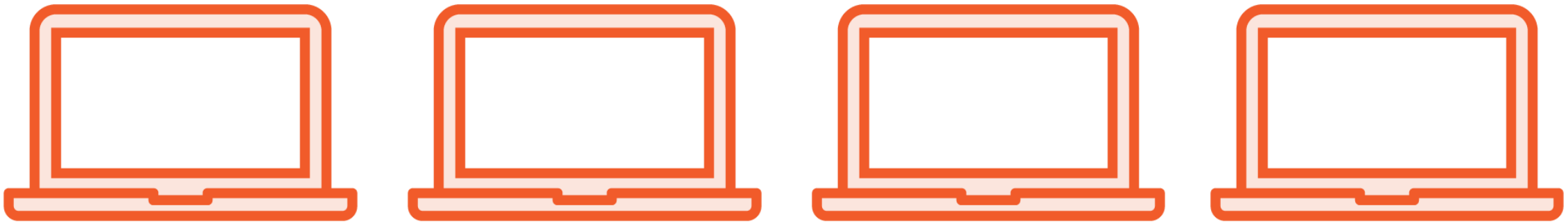
Multifactor Authentication

Something you know, something you have, something you are, somewhere you are

Remote System Administration

Telnet Port 23	SSH Port 22
RDP Port 3389	VNC Ports 5800, 5900

Remote Support Services



Bomgar

GoToAssist

LogMeIn

pcAnywhere

```
“company_name” vpn
“company_name” remote access
site:company_domain.com inurl:vpn
site:company_domain.com inurl:remote
```

Search Engine Queries

Usage: Identify remote access portals.

Application Usage (L1/L2)

What software do they use on their internal network?

Information Sources

Shodan Results

Metadata

Support Forums

Help Desk Job Postings

What about their Internet-facing applications?

Information Sources

Shodan Results

BGP Toolkit

Censys

Qualys SSL Labs

- https://www.ssllabs.com/

Similar to sslyze

Test your server

Specific domain/subdomain

Do not show the results on the boards

Observatory

- https://observatory.mozilla.org/

Includes HTTP header analysis

Third party scanners

No to public search results

Force a rescan

PunkSPIDER

- https://www.punkspider.org/

Search by top level domain

Check all flaws

Check OR

Defensive Technologies (L1/L2/L3)

Fingerprinting Methods

Passive Fingerprinting

Active Fingerprinting

Passive Fingerprinting

- Return to forums
- Marketing information
- Shared assessments
- Company logo on vendor pages

Active Fingerprinting

Probe

- Nmap
- http-waf-detect (NSE)

HTTP header information

- Burp Proxy

TinEye Reverse Image Search

- https://www.tineye.com/

Find logo on company site

Paste logo URL into TinEye search engine

Human Capability (L1/L2/L3)

The Human Factor

Incident Response Team

Advertised Jobs (Security)

Advertised Jobs (Non-Security)

Outsourcing Agreements

Professional Orgs and Conferences

Demo

Riot Games

- https://hackerone.com/riot

Summary

- Network Blocks
- Email Addresses
- External Infrastructure Profile
- Technologies Used
- Purchase Agreements
- Remote Access
- Application Usage
- Defense Technologies
- Human Capabilities

Onto the next module: Gathering Financial OSINT