RED TEAMS

Deel 1


YELLOW TEAM
Software coders and Architects "The Builders"
ORANGE TEAM
Facilitate interaction and education
RED TEAM
Offensive security "The Breakers"
Integrating defensive tactics with offensive results
BLUE TEAM
Defensive security "The Defenders"
GREEN TEAM
Enhance security and automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management

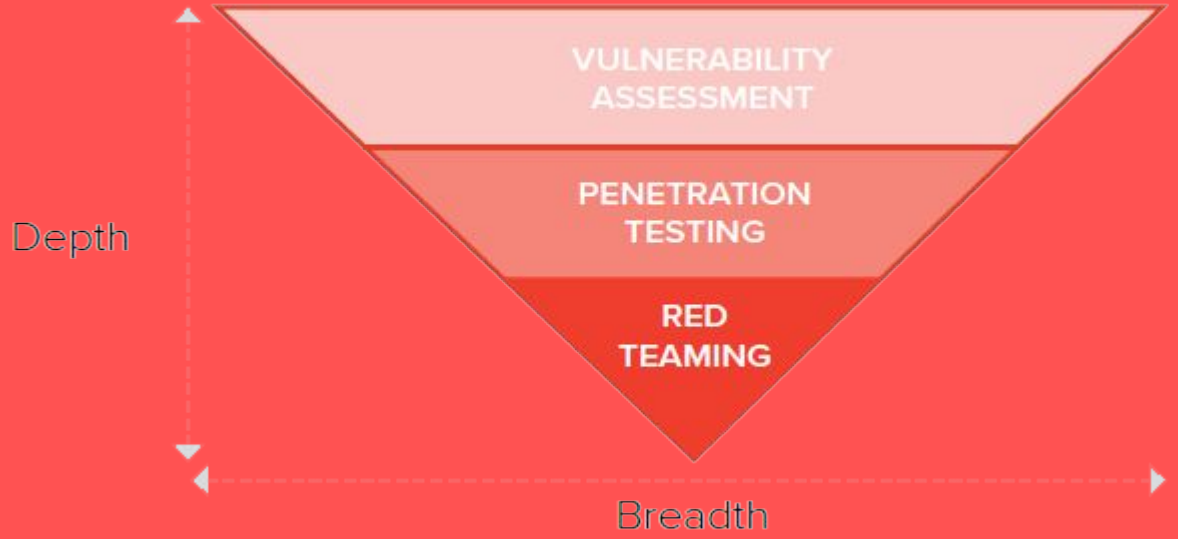
PXL DIGITAL

RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

PXL DIGITAL

ETHICAL HACKING - Pen-testing



https://purplesec.us/types-penetration-testing/

https://bishopfox.com/blog/primer-to-red-teaming

PXL DIGITAL

ETHICAL HACKING - Pen-testing

	PENETRATION TESTING	RED TEAMING
Skill Level Required	High	Higher
Scope	Defined by organization	Identified by red team
Objective	Confined results	Uncover many vulnerabilities
Threat Emulation	Partial	Advanced and persistent
Systems Testing	Independently	Simultaneously
Rules	Well defined	Anything goes
Employee Awareness	Typically aware	Limited number
Targeted Users	✓	✓
Vulnerability Scanning	✓	✓
Manual Testing Simulating Attackers	✓	✓
Social Engineering, people	–	✓
Physical Testing, offices, warehouses, data centers, etc.	–	✓

PXL DIGITAL


Project Initiation
• Threat Modeling
• Define Trophies
• Determine Schedule
• Develop Attack Playbook
Recon Phase
• Open Source Intelligence
• Covert Observation
• Asset Identification
• Social Engineering
Compromise Target
• Scanning
• Penetrate Network and/or applications
• Obtain Credentials
• Lateral movement
• Escalate privileges
• Obtain trophies
Security Improvements
• Share findings/weaknesses
• Discuss improvements
• Provide remediation guidance

PXL DIGITAL

PROJECT INITIATION

This describes the project, the situation the team faces, the target, and what supporting activities the team will have to achieve their objective.

In this phase, the team gets exposed to the upcoming project or operation:

- Scoping Meeting
- Questionnaires for different scopes
- Network, Web Application, WiFi, Physical, Social Engineering
- Framing conditions
- Start & end date, IP ranges & domains, dealing with 3rd parties etc.
- Emergency Contact Information
- Rules of Engagement

Threat modeling as described in white teaming is also done to asses the target.

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

RECON PHASE

This phase is the most important one. If done right it will most likely end in the success of the project. A good team can ID the targets quickly, modify the plan accordingly, adapt the tools and finish the project.

- OSINT
- Covert Gathering (Corporate / HUMINT)
- Footprinting
- Identify Protection Mechanisms

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

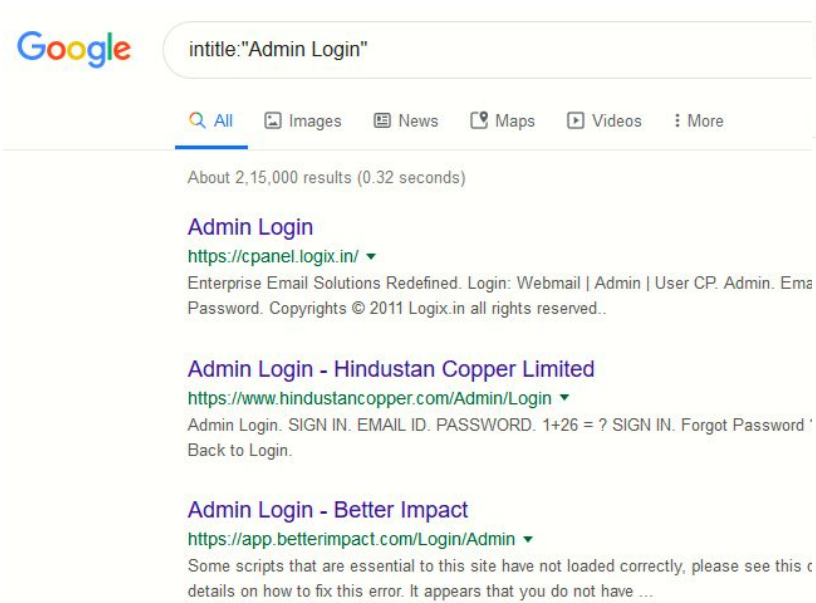
OSINT

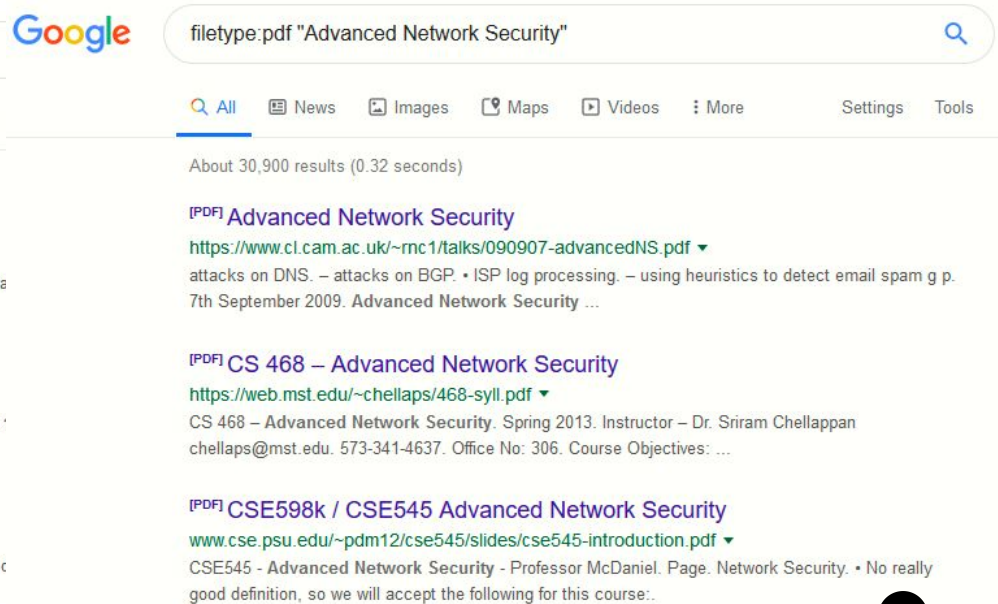
Open Source Intelligence (OSINT) takes three forms; Passive, Semi-passive, and Active.

- Passive Information Gathering: Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. This type of profiling is technically difficult to perform as we are never sending any traffic to the target organization neither from one of our hosts or “anonymous” hosts or services across the Internet. This means we can only use and gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered from a third party.

OSINT

Google Dork





OSINT

SHODAN

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

2

TOP COUNTRIES

Belgium	2

TOP CITIES

Hasselt	2

TOP ORGANIZATIONS

Telenet	1
Skynet Belgium	1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

81.82.216.183

d5152d8b7.static.telenet.be

Telenet

Added on 2019-12-25 11:52:09 GMT

Belgium, Hasselt

ics

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 315-2 DP
Unknown (129): Boot Loader          A
Module: 6ES7 315-2AH14-0AB0  v.0.4
Basic Firmware: v.3.3.7
Module name: CPU 315-2 DP
Serial number of module: S C-C9UC10902012
Plant identification:
Basic Hardware: 6ES...
```

81.244.121.235

235.121-244-81.adsl-dyn.isp.belgacom.be

Skynet Belgium

Added on 2020-01-01 09:05:41 GMT

Belgium, Hasselt

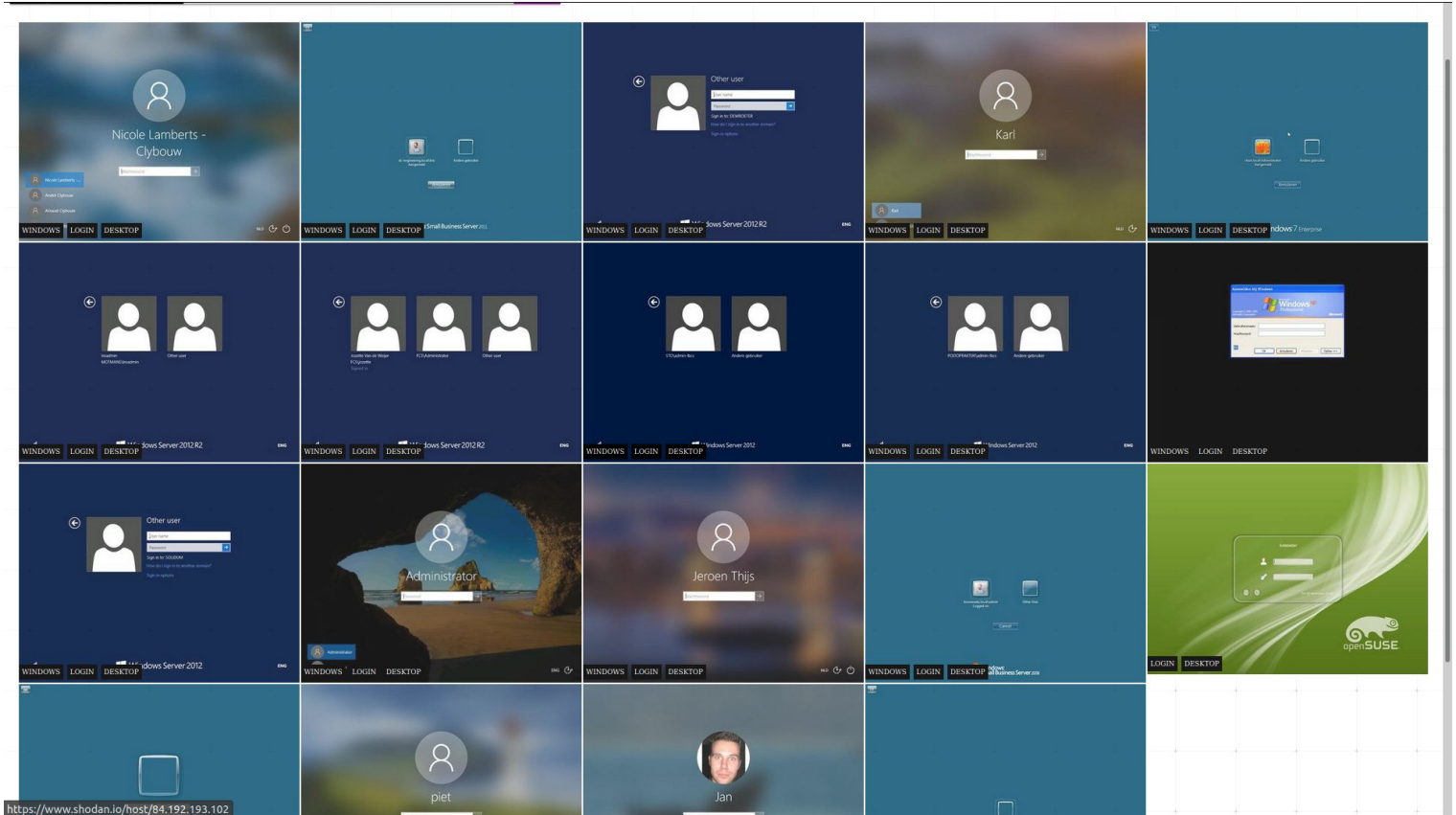
ics

```
Basic Hardware: 6ES7 212-1BE31-0XB0  v.0.1
Module: 6ES7 212-1BE31-0XB0  v.0.1
Basic Firmware: 6ES7 212-1BE31-0XB0  v.3.0.1
```

PXL DIGITAL

OSINT

SHODAN



PXL DIGITAL

Shodan Scanhub Developers View All...

SHODAN

Honeypot Or Not?

Enter an IP to check whether it is a honeypot or a real control system:

Please enter an IP... Check for Honeypot

Frequently Asked Questions

1. How does it work?

   The defining characteristics of known honeypots were extracted and used to create a tool to let you identify honeypots! The probability that an IP is a honeypot is captured in a "Honeyscore" value that can range from 0.0 to 1.0. This is still a prototype/ work-in-progress so if you find some problems please email me at jmath@shodan.io

2. What's the purpose?

   Honeypots are a great tool for learning more about the Internet, the latest malware being used and keep track of infections. When trying to catch an intelligent attacker though, many honeypots fall short in creating a realistic environment. Honeyscore was created to raise awareness of the short-comings of honeypots.

3. What technology did you use?

   The Honeyscore website and algorithm uses the following APIs/ frameworks:

   - Shodan Developer API
   - Python
   - Jade Node Template Engine

4. Contact information?

   You can reach me at the following locations:

   Email: jmath@shodan.io
   Twitter: @achillean

PXL DIGITAL

OSINT

Google Dork

Meer info over zowel Google Dorks als Shodan:

Play by Play: Exploring the Internet of Vulnerabilities

Zeker voor Shodan: **WEES VOORZICHTIG WANNEER JE ANDERE MENSEN HUN SYSTEMEN/INFORMATIE BENADERT!**

OSINT

- **Semi-passive Information Gathering**: The goal for semi-passive information gathering is to **profile the target with methods that would appear like normal Internet traffic and behavior**. We query only the published name servers for information, we aren't performing in-depth reverse lookups or brute force DNS requests, we aren't searching for "unpublished" servers or directories. We aren't running network level portscans or crawlers and we are only looking at **metadata in published documents and files**; not actively seeking hidden content. The key here is **not to draw attention to our activities**. Post mortem the target may be able to go back and discover the reconnaissance activities but they shouldn't be able to attribute the activity back to anyone.
- **Active Information Gathering**: Active information gathering should be detected by the target as suspicious or malicious behavior. During this stage we are **actively mapping network infrastructure** (think full port scans nmap –p1-65535), **actively enumerating and/or vulnerability scanning the open services**, we are actively searching for unpublished directories, files, and servers. Most of this activity falls into your typically "reconnaissance" or "scanning" activities for your standard pentest.

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

COVERT GATHERING

Corporate

- Physical security inspections
- Wireless scanning / RF frequency scanning
- Employee behavior inspection
- Accessible/adjacent facilities (shared spaces)
- Dumpster diving
- Types of equipment in use

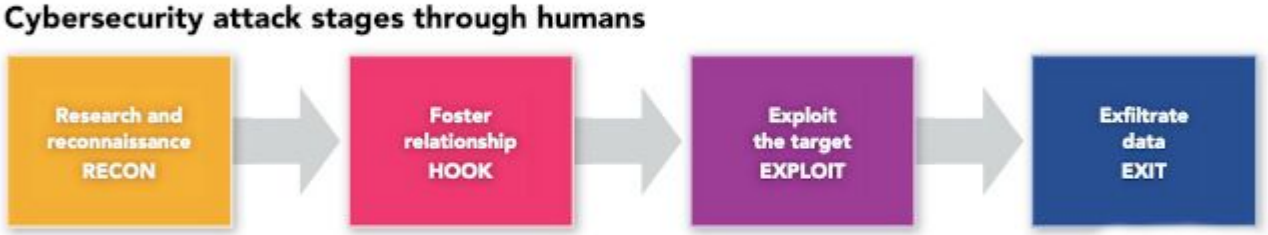
HUMINT

Human intelligence complements the more passive gathering on the asset as it provides information that could not have been obtained otherwise, as well as add more “personal” perspectives to the intelligence picture (feelings, history, relationships between key individuals, “atmosphere”, etc...)

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

SOCIAL ENGINEERING

HUMINT & OSINT put to work to gain access



RECON PHASE

FOOTPRINTING

Definition: External information gathering, also known as footprinting, is a phase of information gathering that consists of interaction with the target in order to gain information from a perspective external to the organization.

WHY: Much information can be gathered by interacting with targets. By probing a service or device, you can often create scenarios in which it can be fingerprinted, or even more simply, a banner can be procured which will identify the device. This step is necessary to gather more information about your targets. Your goal, after this section, is a prioritized list of targets.

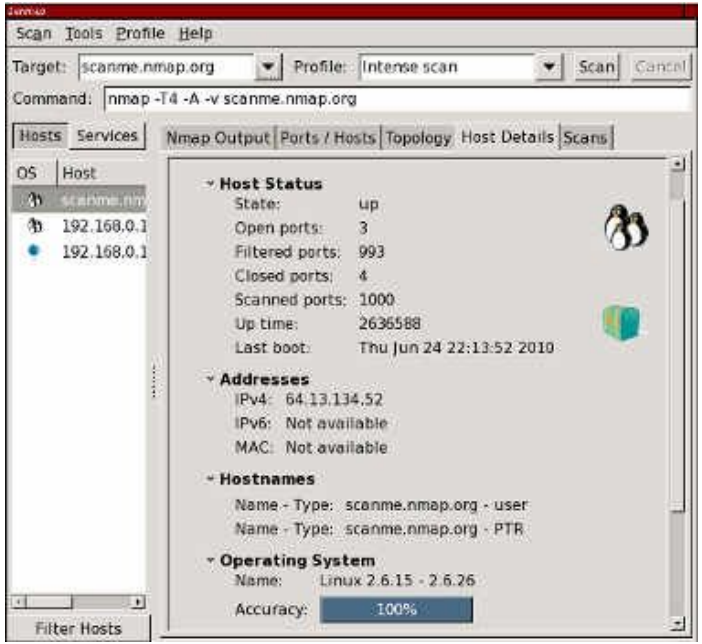
The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

PXL DIGITAL

EXTERNAL FOOTPRINTING

Active Footprinting

- Port Scanning
- Banner Grabbing
- SNMP Sweeps
- SMTP Bounce Back
- Zone Transfers
- DNS Bruteforce
- Forward/Reverse DNS
- Web Application Discovery
- Virtual Host Detection & Enumeration



Establish External Target List

Once the activities above have been completed, a list of users, emails, domains, applications, hosts and services should be compiled

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

EXTERNAL FOOTPRINTING

Identify Customer External Ranges

One of the major goals of intelligence gathering is to determine hosts which will be in scope. There are a number of techniques which can be used to identify systems, including using reverse **DNS lookups, DNS bruting, WHOIS** searches on the domains and the ranges.

Passive Reconnaissance

- Whois lookups
- BGP looking glasses

```
iicybersecurity@kali:~$ dig @192.168.1.1 webimprints.com MX

; <<>> DiG 9.11.3-1-Debian <<>> @192.168.1.1 webimprints.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28465
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;webimprints.com.               IN      MX

;; ANSWER SECTION:
webimprints.com.        1800    IN      MX      10 ALT1.ASPMX.L.GOOGLE.com.
webimprints.com.        1800    IN      MX      10 ALT2.ASPMX.L.GOOGLE.com.
webimprints.com.        1800    IN      MX      0 ASPMX.L.GOOGLE.com.
webimprints.com.        1800    IN      MX      20 ASPMX2.GOOGLEMAIL.com.
webimprints.com.        1800    IN      MX      20 ASPMX3.GOOGLEMAIL.com.

;; AUTHORITY SECTION:
webimprints.com.        3600    IN      NS      ns19.domaincontrol.com.
webimprints.com.        3600    IN      NS      ns20.domaincontrol.com.

;; Query time: 178 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Fri Oct 26 07:55:26 EDT 2018
;; MSG SIZE  rcvd: 226
```

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

INTERNAL FOOTPRINTING

Active Footprinting

- Port Scanning
- Web Application Discovery
- Virtual Host Detection & Enumeration

Comparable with external bit inside the network, reiterating what we know in light of the new context.

Establish External Target List

Once the activities above have been completed, a list of users, emails, domains, applications, hosts and services should be compiled

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

INTERNAL FOOTPRINTING

Active Directory mapping

BloodHound uses graph theory to reveal the hidden and often
unintended relationships within an Active Directory environment.

Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an
Active Directory environment

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2


BLOODHOUND
BloodHound
github.com/BloodHoundAD/BloodHound

IDENTIFY PROTECTION MECHANISMS

The following elements should be identified and mapped according to the relevant location/group/persons in scope. This will enable correct application of the vulnerability research and exploitation to be used when performing the actual attack - thus maximizing the efficiency of the attack, and minimizing the detection ratio.

- Network Based Protections
- Host Based Protections
- Application Level Protections
- Storage Protections
- User Protections

Be aware of your environments!

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

PLURALSIGHT VIDEOS

Pluralsight video: link
Relevant : Shodan: An overview

Pluralsight video: link
Relevant : Active reconaissance: A complete guide

Pluralsight video: link
Relevant : Evading Detection and Bypassing Countermeasures

PXL DIGITAL

PXL DIGITAL