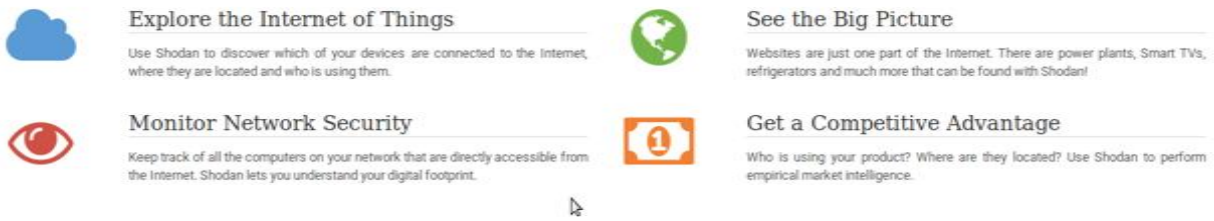
iCoaching

SHODAN.io como herramienta de seguridad y pentesting

iSEC



¿qué es SHODAN?

- Motor de búsqueda de dispositivos conectados a internet⟶Servidores (de todo), IoT (de todo), Hosts (de todo!)...
- motor de búsqueda de **banners de servicios conectados**⟶ojo: se cree todo lo que le dicen

Shodan como motor de búsqueda

se puede **parametrizar o segmentar** la búsqueda por regiones geográficas, por tecnologías, también se puede **restringir** los resultados ⟶

- country:ar https://www.shodan.io/search?query=country%3Aar
- hostname:Speedy https://www.shodan.io/search?query=hostname%3ASpeedy
- modicon https://www.shodan.io/search?query=modicon
- port:25 https://www.shodan.io/search?query=port%3A25
- os:Windows https://www.shodan.io/search?query=os%3AWindows
- net:138.186.0.0/24 https://www.shodan.io/search?query=net%3A138.186.0.0%2F24

SHODAN
Computer Search Engine

¿qué buscan todos?

https://www.shodan.io/explore/popular

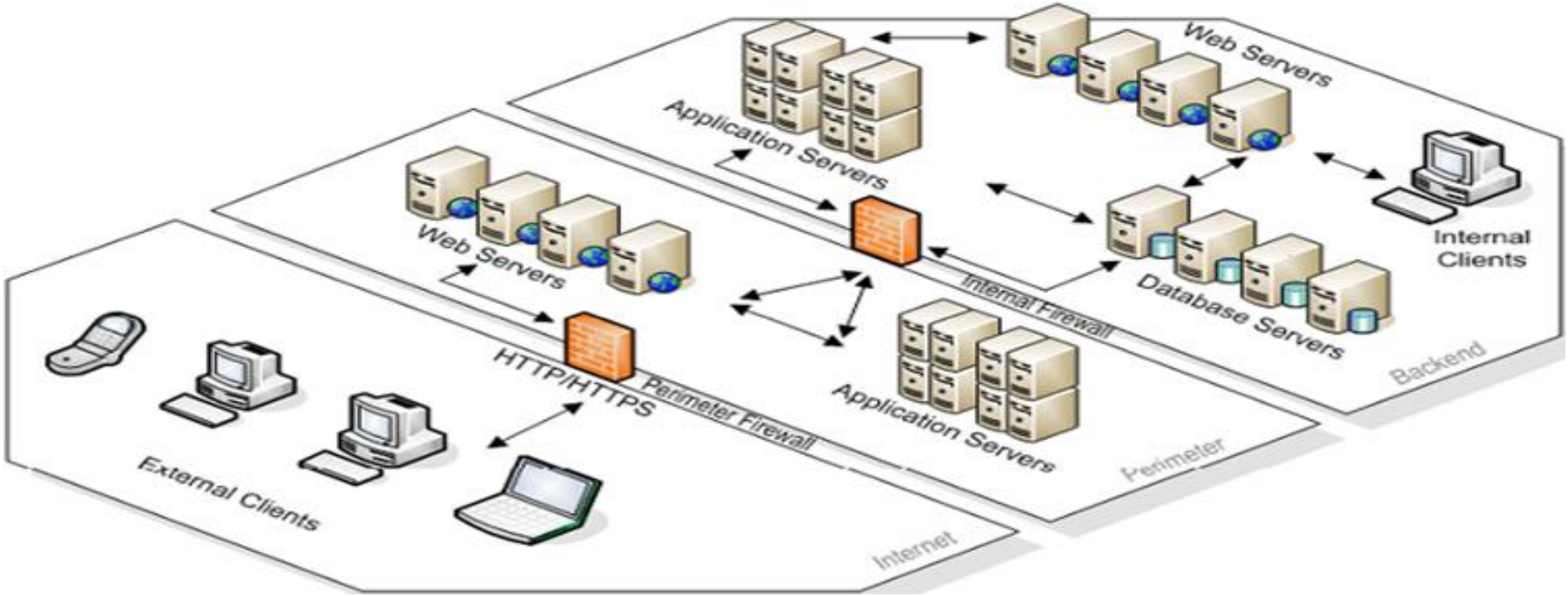
nosotros la vamos a usar para penetration testing

se podría utilizar dentro de un pentest en las etapas de **reconocimiento y scanning**

reconocimiento⟶scaning⟶gaining access (obtención de acceso)⟶maintaining access (consolidación)⟶clearing tracks (borrado de rastros)

antes veamos un poco de networking

-despliegues de servidores típicos en internet-



antes veamos un poco de networking

-despliegues de IoT típicos en internet-

despliegue con administración en la nube

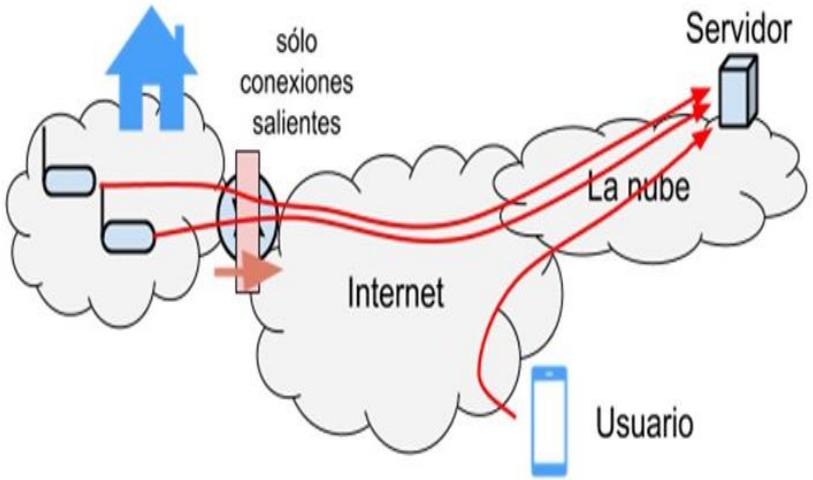
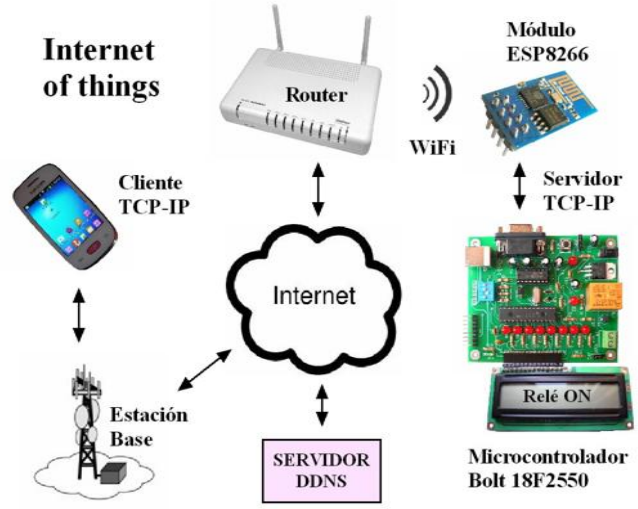


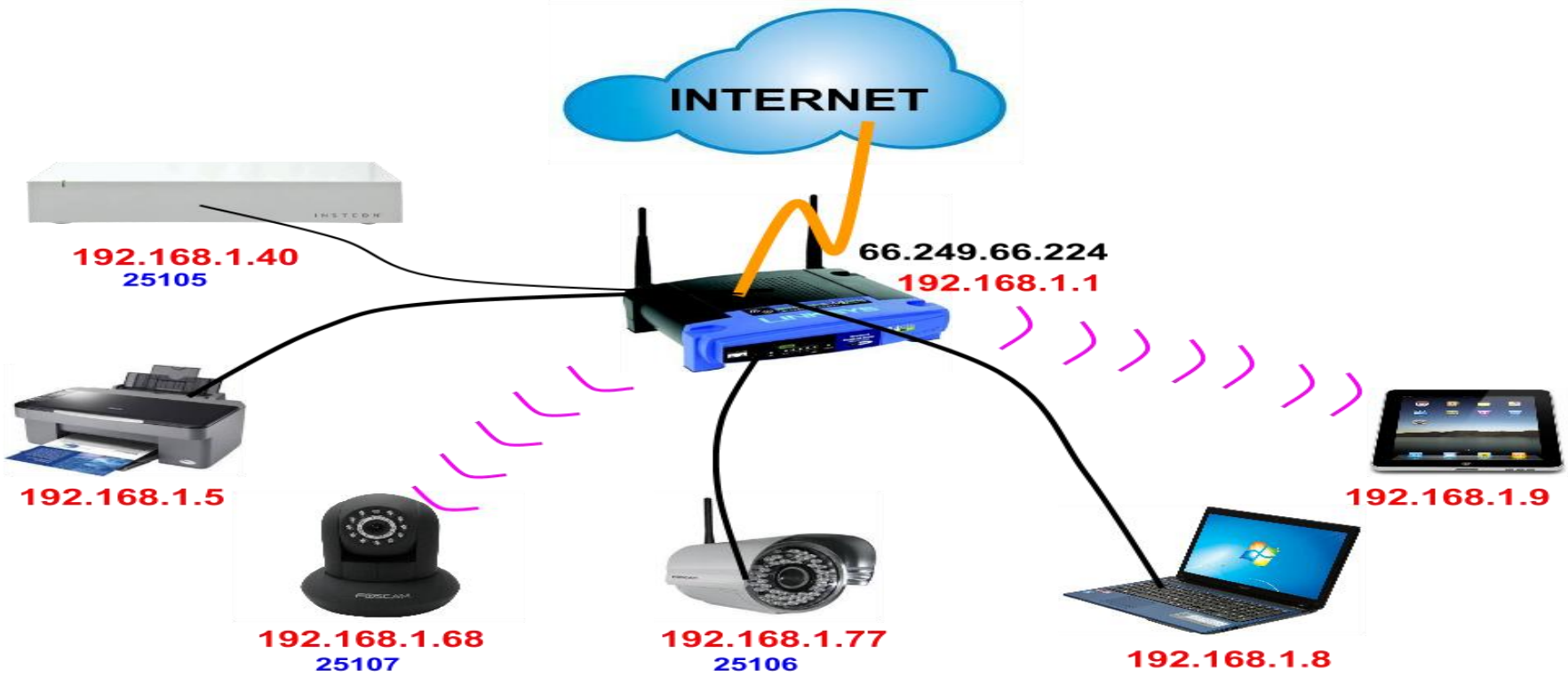
Figura 1. Diagrama comunicación vía servidor en la nube

despliegue administrado en red local



antes veamos un poco de networking

-IoT despliegues de todo lo demás!-



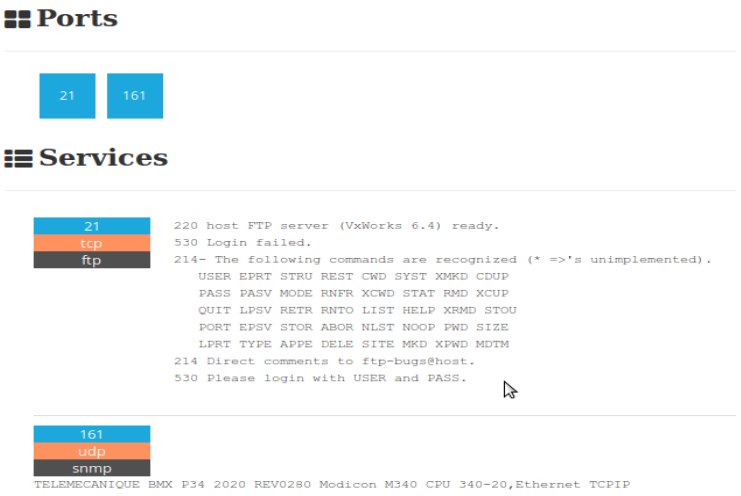
información de reconocimiento

-ejemplo de un sensor sumergido en un río-

analizar el paquete resultado de shodan en formato raw⟶
https://www.shodan.io/host/174.33.1.22/raw

- country_name **United States**
- data.0.data TELEMECANIQUE BMX P34 2020 REV0280 **Modicon M340 CPU 340**-20,Ethernet TCPIP
- data.0.hostnames [**'host1743300221.direcway.com'**]
- isp **Hughes Network Systems**
- latitude **37.751**
- longitude **-97.822**
- ports [**161, 21**]

analizar la info específica de **puertos y servicios puestos en escucha y sistema operativo**:
https://www.shodan.io/host/174.33.1.22



información de reconocimiento

-analizar puertos y servicios puestos en escucha y sist. operativo-

¿que es? tratar de reconocer función

- https://www.shodan.io/host/138.219.43.240 (ver todos los puertos que tiene!!!!!!!!)
- Analizar información para reconocimiento

SHODAN
Computer Search Engine

¿cómo hace Shodan.io?

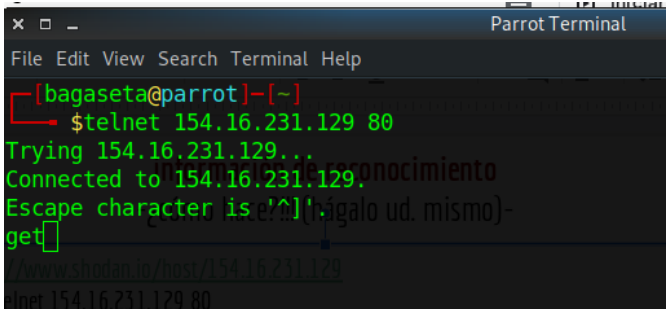
-demo hágalo ud. mismo-

información de reconocimiento

-¿cómo hace?!!! (hágalo ud. mismo)-

https://www.shodan.io/host/138.219.43.240

- telnet 138.219.43.240 80
  - cualquier comando http y espere el banner de respuesta
- telnet 138.219.43.240 25
  - EHLO localhost
  - MAIL FROM:‹christian.vila@isec-global.com›
  - RCPT TO:‹codigo.fiona@gmail.com›



información de reconocimiento

-como análisis de vulnerabilidades-

https://www.shodan.io/host/192.121.196.50

⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2016-0777	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2011-5000	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.
CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2014-1692	The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.
CVE-2010-5107	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion)

Mitre⟶ ¿qué vulnerabilidad?
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0098

SecurityFocus⟶ ¿cómo explotarla?
https://www.securityfocus.com/bid/66303/info

SHODAN
Computer Search Engine

una búsqueda interesante...

https://www.shodan.io/search?query=http.component%3A%22mysql%22+port%3A%2280%22

instructor

Christian Javier Vila

CTO Director de Tecnologías – ISEC Global Inc.
C|EH Certified Ethical Hacker, EC Council.
Sub Inspector (r) Policía PSA ARG
Especialista Investigación de Homicidios (MAT N° 510, ACRA)
Agente de Inteligencia FAA ARG
christian.vila@isec-global.com
www.isec-global.com/icoach
@Infosecurityvip
linkedin

eof

Cada una de las partes protegerá la información obtenida durante el desarrollo del curso de la misma manera en que protege su propia información confidencial, haciéndose responsable por cualquier daño/perjuicio que se pudiera ocasionar por el uso indebido de la información accedida. Nuestros documentos entregables y papeles de trabajo serán de acceso exclusivo para los alumnos, quien podrá disponer para su uso de todos los entregables, que no incluyen metodología ni software utilizado. **PROHBIDA SU REPRODUCCIÓN PARCIAL O TOTAL DEL MATERIAL**

iCoaching