PUE 5TH DAY
MADRID 2018

#PUEDAY18

WORKSHOP CCNA CYBER OPS

13:05h a 14:05h

CCNA Cybersecurity Operations: capacitando a los futuros expertos en Centros de Operaciones de Seguridad (SOC)

Ponente: Amador Gabaldón, IT Product Manager at PUE

Networking Academy

Descripción de la sesión

En el presente taller se explora el nuevo curso de Ciberseguridad haciendo énfasis en los laboratorios. Se mostrarán posibles escenarios, requisitos y recursos, las disposiciones y topologías de prácticas disponibles, con el objetivo de mostrar cómo se gestionan las ciberamenazas a las que se enfrentan esos los perfiles de monitorización y respuesta a incidencias en un centro de operaciones de ciberseguridad.

Trataremos un escenario básico y un escenario réplica de un SOC centrándonos en la distribución Security Onion. Se ilustrará, con un ejemplo de actuación, cómo se integran los sistemas de detección de intrusiones (Snort/Suricata), monitorización de eventos (Sguil/Squert), captura de datos (Wireshark y NetworkMiner) y análisis (Bro) para clasificar y dar respuesta a alertas de seguridad.

AGENDA

- **Cisco Networking Academy – Cybersecurity Track**
- **CCNA Cybersecurity Operations**
  - **Ficha técnica del curso**
  - **Laboratorios – Topologías**
- **Laboratorios - Requisitos**
- **Laboratorios - Componentes y características**
- **Topología Simple – 1 x VM**
- **Topología Completa – 4 x VMs**

El portafolio educativo de Networking Academy

Alineado con la certificación

Requiere capacitación a cargo de instructor

Autoinscripción

Colaborar para generar impacto

Introduction to Packet Tracer | **Packet Tracer** | **Hackatones** | **Prototyping Lab** | **Prácticas laborales**

	Exploratorio	Básico	Profesional
Redes		**Networking Essentials** **Mobility Fundamentals** **Talleres de tecnología emergente:** Programabilidad de redes con Cisco APIC-EM*	**CCNA R&S:** Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks **CCNP R&S:** Switch, Route, TShoot
Seguridad	**Introduction to Cybersecurity**	**Cybersecurity Essentials**	**CCNA Cyber Ops** **CCNA Security**
IoT y análisis	**Introduction to IoT**	**IoT Fundamentals:** Connecting Things, Big Data & Analytics, IoT Security* Hackathon Playbook	
SO y TI	**NDG Linux Unhatched**	**NDG Linux Essentials** **IT Essentials**	**NDG Linux I** **NDG Linux II**
Programación		**CLA: Programming Essentials in C** **CPA: Programming Essentials in C++** **PCAP: Programming Essentials in Python** **Talleres de tecnología emergente:** Experimentando con API REST utilizando Cisco Spark*	**CLP: Advanced Programming in C*** **CPP: Advanced Programming in C++**
Laboral	**Be Your Own Boss**	**Entrepreneurship**	
Instrucción digital	**Get Connected**		

El portafolio educativo de Networking Academy

Alineado con la certificación
Requiere capacitación a cargo de instructor
Autoinscripción

Colaborar para generar impacto

Introduction to Packet Tracer | **Packet Tracer** | **Hackatones** | **Prototyping Lab** | **Prácticas laborales**

	Exploratorio	Básico	Profesional
Redes		**Networking Essentials** **Mobility Fundamentals** **Talleres de tecnología emergente:** Programabilidad de redes con Cisco APIC-EM*	**CCNA R&S:** Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks **CCNP R&S:** Switch, Route, TShoot
Seguridad	**Introduction to Cybersecurity**	**Cybersecurity Essentials**	**CCNA Cyber Ops** **CCNA Security**
IoT y análisis	**Introduction to IoT**	**IoT Fundamentals:** Connecting Things, Big Data & Analytics, IoT Security* Hackathon Playbook	
SO y TI	**NDG Linux Unhatched**	**NDG Linux Essentials** **IT Essentials**	**NDG Linux I** **NDG Linux II**
Programación		**CLA: Programming Essentials in C** **CPA: Programming Essentials in C++** **PCAP: Programming Essentials in Python** **Talleres de tecnología emergente:** Experimentando con API REST utilizando Cisco Spark*	**CLP: Advanced Programming in C*** **CPP: Advanced Programming in C++**
Laboral	**Be Your Own Boss**	**Entrepreneurship**	
Instrucción digital	**Get Connected**		

CCNA Cyber Ops

Descripción general del curso

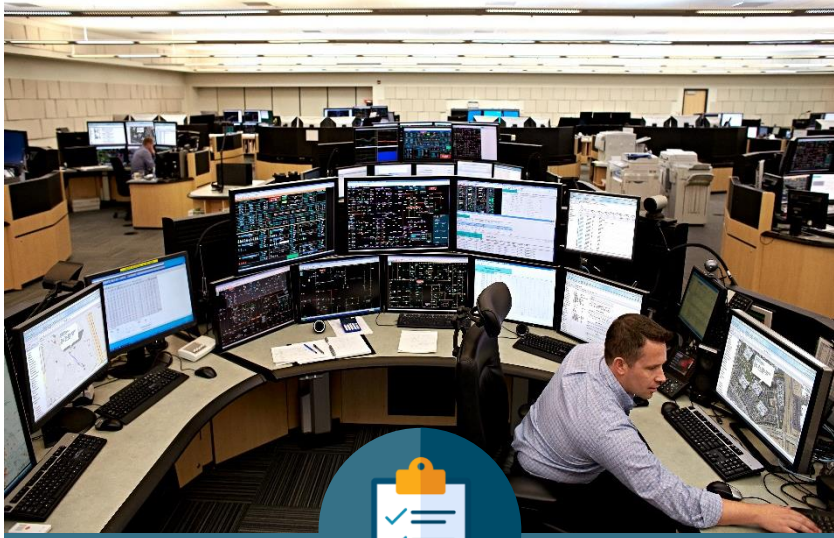
CCNA Cyber Ops introduce los conceptos de seguridad fundamentales y las habilidades necesarias para monitorear, detectar, analizar y dar respuesta a la ciberdelincuencia, el ciberespionaje, las amenazas internas, las amenazas persistentes avanzadas, los requisitos normativos y otros problemas de ciberseguridad que enfrentan las organizaciones. Pone énfasis en la aplicación práctica de las habilidades necesarias para mantener y garantizar la disponibilidad operativa de seguridad de los sistemas en red protegidos.

Beneficios

Los alumnos adquirirán y aplicarán destrezas en el área de operaciones de ciberseguridad a nivel técnico. El curso está coordinado con la certificación Cisco CCNA Cybersecurity Operations.

Componentes educativos

- 13 capítulos, cuestionarios de final de capítulo modificables y exámenes de final de capítulo
- 13 cuestionarios de práctica sobre términos y conceptos
- 54 actividades interactivas
- 45 prácticas de laboratorio (27 máquinas virtuales de uso)
- 5 actividades de Packet Tracer
- Una por cada uno: evaluación de habilidades, examen final de práctica, examen final
- 2 exámenes de práctica para la certificación
    - 1x 210-250 SECFND
    - 1x 210-255 SECOPS



Coordinado con la certificación

Características

Público objetivo: estudiantes de carreras terciarias y universitarias de dos y cuatro años.

Requisitos previos: conocimientos básicos de sistema operativo y redes

Idiomas: inglés

Presentación del curso: con instructor

Tiempo estimado para completar el curso: 70 horas

Próximo curso recomendado: CCNA Security

Capacitación a cargo de instructor: obligatoria

TEMARIO

Módulo 1. Ciberseguridad: el Centro de Operaciones de Seguridad – SOC

Módulo 2. Sistema operativo Windows

Módulo 3. Sistema operativo Linux

Módulo 4. Protocolos y servicios de red

Módulo 5. Infraestructura de red

Módulo 6. Principios de seguridad en red

Módulo 7. Ataques de red: Una inspección detallada

Módulo 8. Protección de la red

Módulo 9. Infraestructura y Criptografía de clave pública

Módulo 10. Análisis y seguridad de dispositivos finales

Módulo 11. Monitorización de seguridad

Módulo 12. Análisis de datos de intrusiones

Módulo 13. Respuesta y gestión de incidencias

Visión General y 1ª Aprox. al SOC

TEMARIO

Módulo 1. Ciberseguridad: el Centro de Operaciones de Seguridad – SOC

Módulo 2. Sistema operativo Windows

Módulo 3. Sistema operativo Linux

Módulo 4. Protocolos y servicios de red

Módulo 5. Infraestructura de red

Módulo 6. Principios de seguridad en red

Módulo 7. Ataques de red: Una inspección detallada

Módulo 8. Protección de la red

Módulo 9. Infraestructura y Criptografía de clave pública

Módulo 10. Análisis y seguridad de dispositivos finales

Módulo 11. Monitorización de seguridad

Módulo 12. Análisis de datos de intrusiones

Módulo 13. Respuesta y gestión de incidencias

Fundamentos SO → IT Essentials

TEMARIO

Módulo 1. Ciberseguridad: el Centro de Operaciones de Seguridad – SOC

Módulo 2. Sistema operativo Windows

Módulo 3. Sistema operativo Linux

Módulo 4. Protocolos y servicios de red

Módulo 5. Infraestructura de red

Redes, protocolos, servicios
→ CCNA Routing &Switching 1-2

Módulo 6. Principios de seguridad en red

Módulo 7. Ataques de red: Una inspección detallada

Módulo 8. Protección de la red

Módulo 9. Infraestructura y Criptografía de clave pública

Módulo 10. Análisis y seguridad de dispositivos finales

Módulo 11. Monitorización de seguridad

Módulo 12. Análisis de datos de intrusiones

Módulo 13. Respuesta y gestión de incidencias

TEMARIO

Módulo 1. Ciberseguridad: el Centro de Operaciones de Seguridad – SOC
Módulo 2. Sistema operativo Windows
Módulo 3. Sistema operativo Linux
Módulo 4. Protocolos y servicios de red
Módulo 5. Infraestructura de red
Módulo 6. Principios de seguridad en red
Módulo 7. Ataques de red: Una inspección detallada
Módulo 8. Protección de la red
Módulo 9. Infraestructura y Criptografía de clave pública
Módulo 10. Análisis y seguridad de dispositivos finales
Módulo 11. Monitorización de seguridad
Módulo 12. Análisis de datos de intrusiones
Módulo 13. Respuesta y gestión de incidencias

Fundamentos de seguridad
Conceptos y aplicación
Descripción de Ataques
Protección CIA
Herramientas
→ **CCNA Security**

Networking Academy

IMPULSANDO EL CONOCIMIENTO TIC CUALIFICADO

TEMARIO

Módulo 1. Ciberseguridad: el Centro de Operaciones de Seguridad – SOC
Módulo 2. Sistema operativo Windows
Módulo 3. Sistema operativo Linux
Módulo 4. Protocolos y servicios de red
Módulo 5. Infraestructura de red
Módulo 6. Principios de seguridad en red
Módulo 7. Ataques de red: Una inspección detallada
Módulo 8. Protección de la red
Módulo 9. Infraestructura y Criptografía de clave pública
Módulo 10. Análisis y seguridad de dispositivos finales
Módulo 11. Monitorización de seguridad
Módulo 12. Análisis de datos de intrusiones
Módulo 13. Respuesta y gestión de incidencias

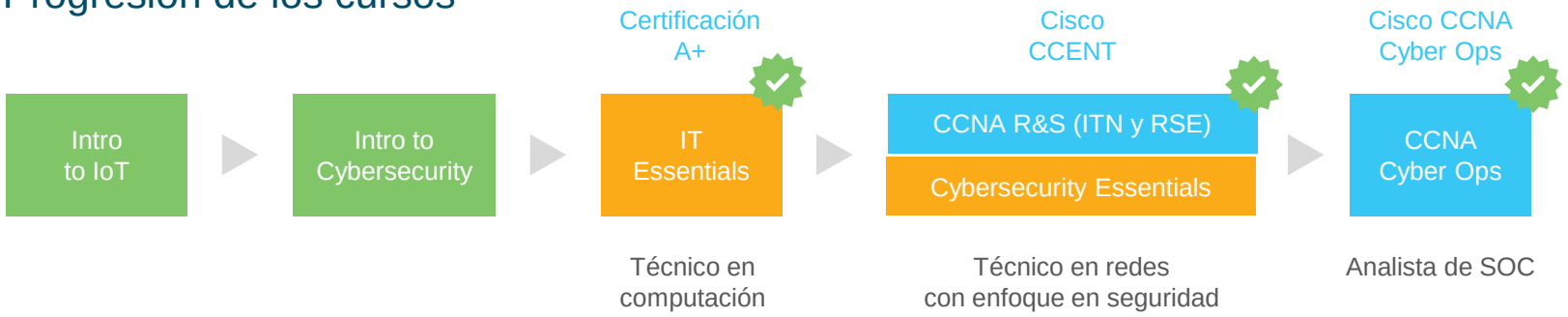
Ciberseguridad
Tecnologías y procedimientos
Registros, eventos, alertas
Análisis y clasificación
Modelos de respuesta y gestión
→ **Fundamentos de Ciberseguridad**

TEMARIO

- Comprender los **principios, roles y responsabilidades** involucrados en las operaciones de ciberseguridad, así como las tecnologías, herramientas, regulaciones y estándares disponibles.
- Describir las **vulnerabilidades y amenazas comunes** en los dispositivos de usuario y en las infraestructuras de red
- Demostrar habilidades fundamentales aplicadas a la **monitorización, detección, investigación, análisis y respuesta a incidentes** de seguridad.
- **Clasificar eventos** intrusivos según categorías definidas por **modelos** de seguridad y establecer acciones defensivas.
- Llevar a cabo con éxito las tareas, deberes y responsabilidades de un **Analista de Seguridad** de nivel asociado en un Centro de Operaciones de Seguridad (SOC)

Analista de operaciones de Ciberseguridad

Progresión de los cursos



Actividades de aprendizaje complementarias

Amplíe sus conocimientos

- Networking Essentials (alternativa posible a IT Essentials)
- PCAP: Programming Essentials in Python
- NDG Linux Essentials
- Webinars de tecnología de seguridad y redes

IoT Fundamentals

- Connecting Things
- Big Data and Analytics
- Hackathon Playbook

CCNA R&S: (certificación CCNA R&S)

- Escalamiento de redes
- Conexión de redes

Colaborar para generar impacto

- Cisco Prototyping Lab
- Juegos de Packet Tracer
- Prácticas laborales
- Webinars de NetAcad Advantage
- Hackatones

Coordinado con la certificación

PRÁCTICAS Y LABORATORIOS

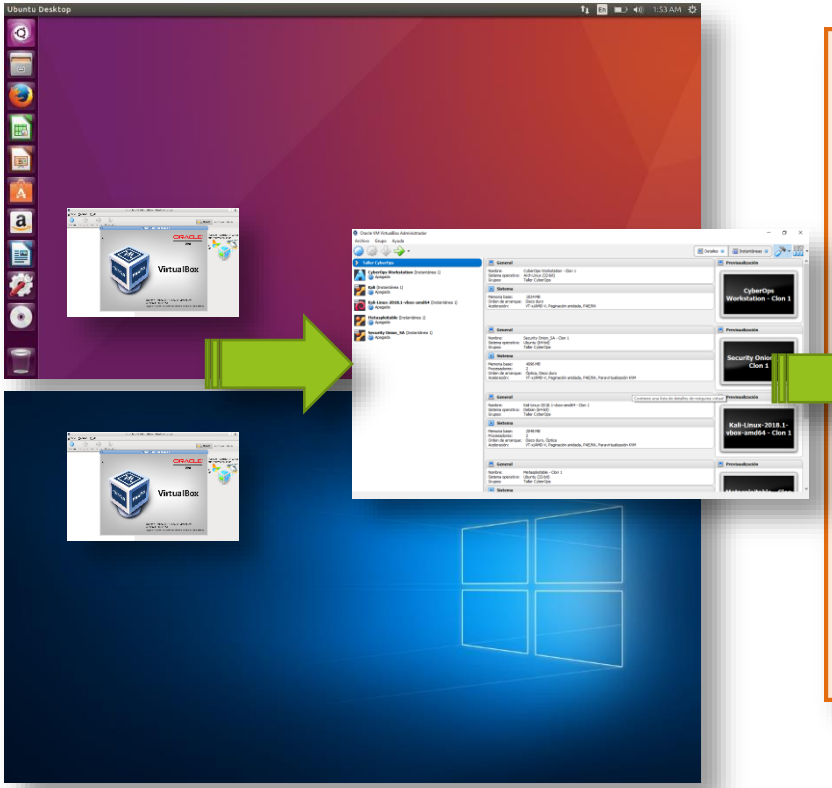
- **Requisitos**
- **Estructura**
- **Componentes y características**

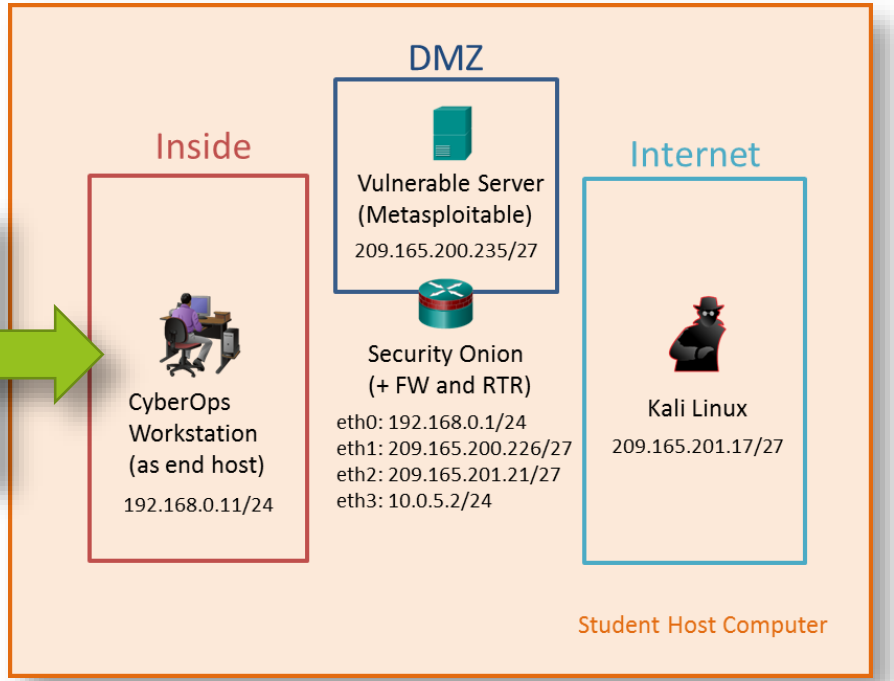
- **1 PC – [SO + VirtualBox] + OVA(s)**

- **Básico**
  - 1 VM CyberOps WKS
    - RAM → 2GB
    - Disco → 8GB
  - OVA descargable
    - Linux - Arch Linux
    - Aplicaciones y script adaptados

- **Completo**
  - 1 VM CyberOps WKS
  - 1 VM Security Onion
  - 1 VM Kali Linux
  - 1 VM Metasploitable
    - RAM → 8GB
    - Disco → 45GB
  - OVAs descargables

LABORATORIOS - ESTRUCTURA





Networking Academy

pue IMPULSANDO EL CONOCIMIENTO TIC CUALIFICADO

LABORATORIOS – COMPONENTES Y CARÁCTERÍSTICAS - 1

Cyber Ops Workstation:

→ Arch Linux

→ RAM 1GB;Disco 7GB

→ Wireshark, tcpdump

→ Hping3, scapy, nmap

→ ELK, Filebeat,Python

→ IDLE

→ mininet, Pox,

→ Snort, iptables

→ nginx,vsftpd, tftp, sshd

→→ Scripts y pre-configuraciones de soporte a prácticas

LABORATORIOS – COMPONENTES Y CARÁCTERÍSTICAS - 2

Security Onion:

→RAM 4GB;Disco 10GB

→ Ubuntu Linux

→ Distribución NSM:

→ Snort

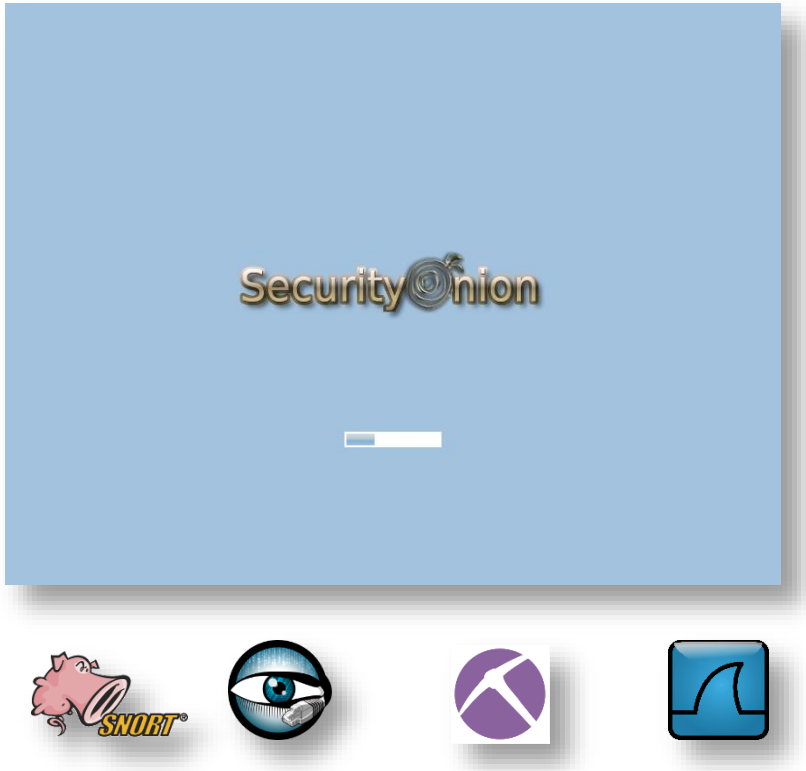
→ Bro

→ Network Miner

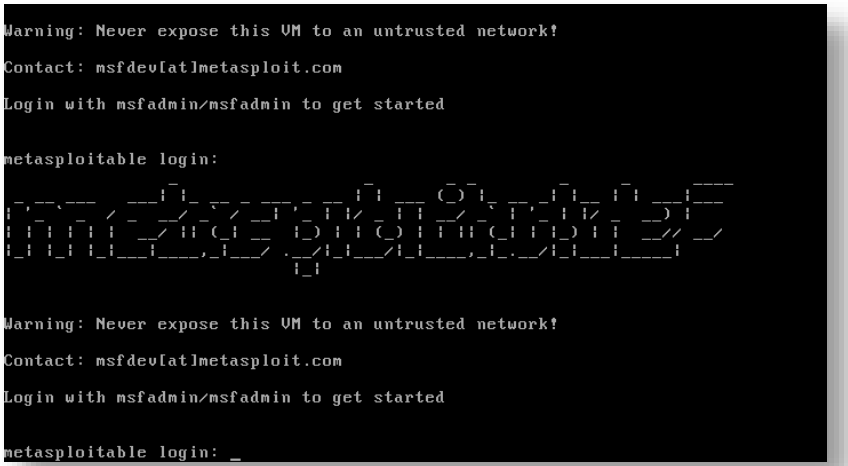
→ Wireshark

→ ELSA

→ Suricata, CapMe, Squert …



Metasploitable:



→ RAM 512MB;Disco <1GB

→ Ubuntu Linux

→ Entorno para pruebas

→ Servicios vulnerables

→ Puertos abiertos

→ Metasploit Framework – Consola de uso de exploits

Kali Linux:

→ RAM 1GB;Disco 10GB

→ Linux Debian

→ Distribución orientada:

→ Pruebas de Penetración

→ Análisis Forense

→ Hacking Ético

→ Incluye 600+ herramientas

TALLER – I

- **Topología Básica - CyberOps Workstation**
- **Uso de IDS (Snort) y Firewall (Iptables)**

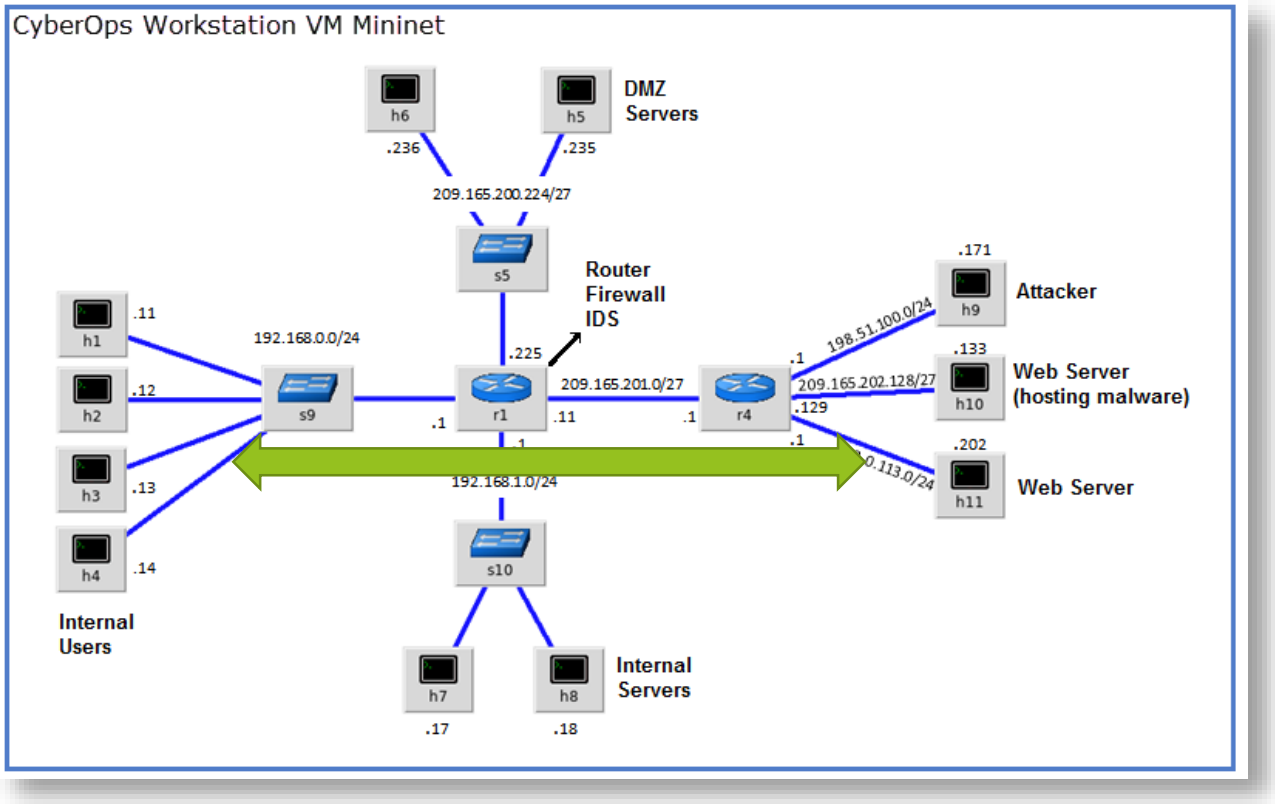
Detección y bloqueo de conexiones

- VM CyberOps WKS
- Mininet Emulator
- Python scripts
- Snort - IDS
- Server – Web/FTP
- Firewall - IPtables

Detección y bloqueo de conexiones

1. Crear topología - Mininet – Python
2. Comprobar conectividad
3. Activar Detector – IDS - Snort
4. Activar Malware Server – Web // FTP Servers
5. Establecer conexión a los servicios
6. Verificar registro IDS
7. Bloquear Conexiones al Malware Server - IPtables
8. Comprobar

CREAR TOPOLOGÍA - MININET – PYTHON



TALLER – II

- Topología completa
- Inyección SQL – Kali -> Metasploit
- Detección – Security Onion

TOP TEN - OPEN WEB APPLICATIONS SECURITY PROYECT → INJECTION

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

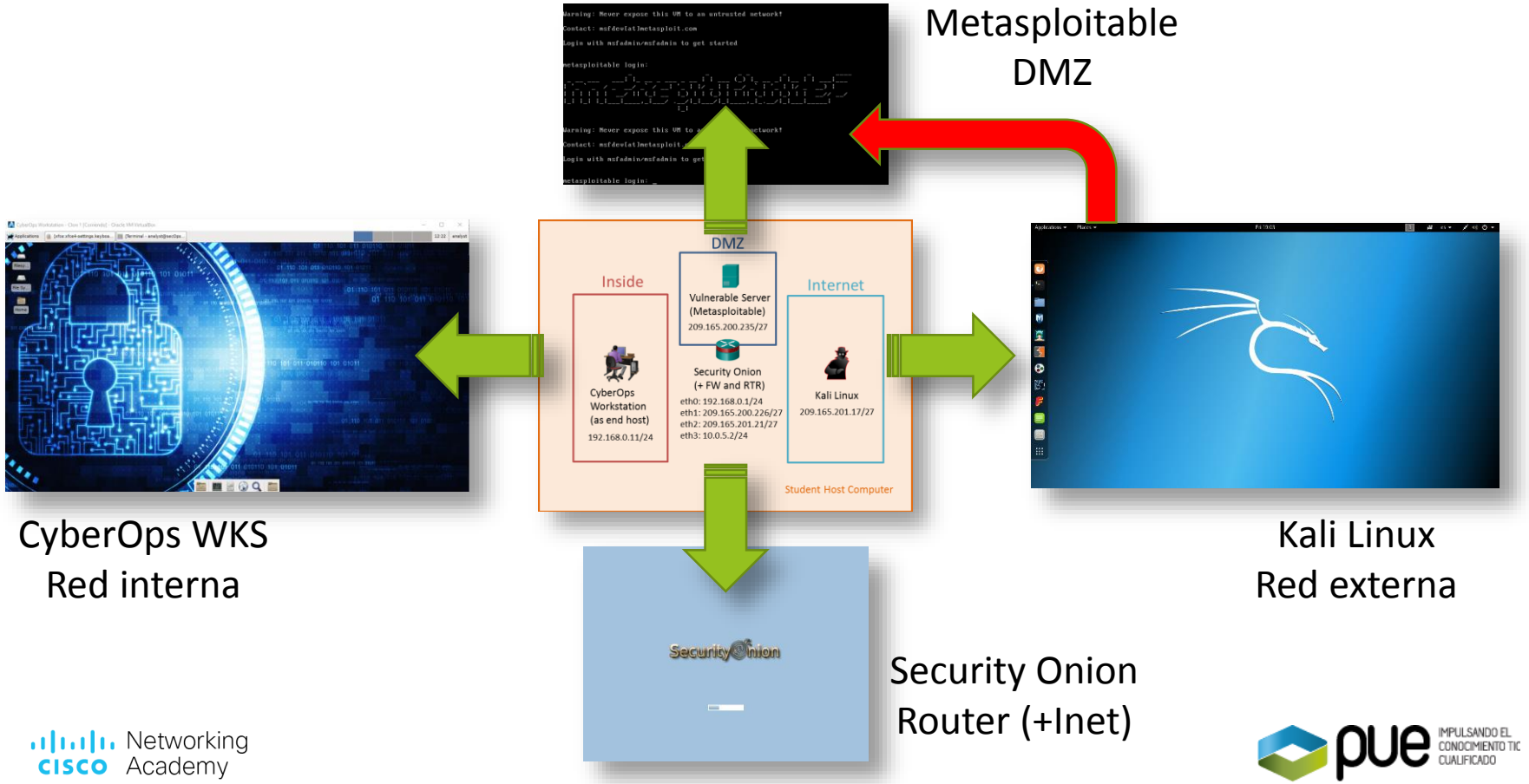
* Image from https://www.owasp.org/

TOP TEN - OPEN WEB APPLICATIONS SECURITY PROYECT → INJECTION

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

* Image from https://www.owasp.org/

LABORATORIOS - ESCENARIO



Networking Academy

IMPULSANDO EL CONOCIMIENTO TIC CUALIFICADO

Security Onion:

- **SGUIL -> Interface gráfico - Pivote**
- **SQUERT -> Interface grafico – Vista alternativa**
- **OSSEC -> HIDS**
- **SNORT -> NIDS – Rules ET**
- **BRO -> Framework de NSM**
- **ELSA -> Enterprise Log Search & Archive**
- **Network Miner -> Herramienta de análisis forense**

Descripción Taller

- **Inyección de SQL**
  - **Bypass Login**
  - **Extracción de datos**
- **Procedimiento**
- **Gestión de alertas, obtención de información**
- **Análisis y clasificación**

Métodos de Inyección:

1. **Inducir errores para revelar estructura o lógica interna**
2. **Determinar qué fragmentos insertar para conformar una sentencia SQL correcta sintácticamente**
3. **Codificar los fragmentos para crear una inyección efectiva**
4. **Inyectar estos fragmentos en las entradas o parámetros disponibles**

EJEMPLO BÁSICO

SELECT * FROM tableN WHERE user='<User>' AND pass='<Pass>'

+

User: ' or 'r' = 'r' --

Pass: 123

SELECT * FROM tableN WHERE user='' or 'r' = 'r' -- ' AND pass='<Pass>'

BARCELONA – MADRID

www.pue.es

¡Gracias!

#PUEDAY18

educacion@pue.es

93 206 02 49

PUE 5TH DAY MADRID 2018

ORACLE ACADEMY

cloudera ACADEMIC PARTNER

Microsoft Imagine Academy

vmware IT ACADEMY

Linux Professional Institute

RED HAT ACADEMY redhat.

Networking Academy cisco