INFORME DE PENTESTING ARQUITECTURA SDN

1. Introducción

En el contexto de una arquitectura SDN, se ejecuta un pentest aplicando la metodología Offensive Securiy con la finalidad de identificar las amenazas presentes en la arquitectura; dentro de la misma línea se realiza un análisis de vulnerabilidades aplicando la metodología OCTAVE con el objetivo de detectar e identificar las vulnerabilidades presentes dentro de la infraestructura.

2. Resumen ejecutivo

Se detecta que la arquitectura SDN desplegada es susceptible a ataques que se pueden ejecutar dentro de una red tradicional, tales como: DDoS y MITM, estos son la base para realizar una gran cantidad de otros ataques. Las vulnerabilidades detectadas están relacionadas en su gran mayoría a las presentes dentro del propio sistema operativo de lo servidores analizados, el resto de las vulnerabilidades están relacionadas al protocolo ICMP y TCP, tanto en el controlador como en la infraestructura Mininet. En total se han encontrado 33 (20 altas, 11 medias y 2 bajas) vulnerabilidades en el controlador ONOS y 11 (4 altas, 5 medias y 2 bajas) en la infraestructura Mininet.

Se recomienda realizar un plan de mitigación que pase por alguna fase de remediación de las vulnerabilidades encontradas y que se implemente alguna solución que permita detectar y si es posible parar los ataques de DDoS y MITM.

3. Metodología

Para la realización del pentest se ha seguido la metodología de Offensive Security, siguiendo las siguientes fases:

A. Recolección de información

Empleando las herramientas de nmap para la enumeración y fase inicial de escaneo de puertos y servicios.

B. Análisis de vulnerabilidades

Se ha utilizado la herramienta de OpenVas para el escaneo de vulnerabilidades. En esta fase se ha implementado la metodología de OCTAVE.

C. Explotación

- Se ha empleado la herramienta sFlow-RT, Slowloris, XERXES y Hping3 para realizar ataques de DDoS.
- Se ha utilizado la herramienta Ettercap para realizar ataques de MITM.
- Se ha utilizado la herramienta Sdnpwn para realizar otros tipos de ataques propios de una SDN, como lo son: XSS, inyección HTML, CSRF, instalación de aplicación sin autenticación, websocket sin autenticación, ataques de protocolo ARP y ataque de LLDP replay.

D. Post Explotación

En la arquitectura SDN analizada se puede ejecutar la fase de post explotación, especialmente ejecutando técnicas de pivoting entre capas de datos y control de SDN.

4. Conclusiones

A. En la fase de enumeración con la herramienta nmap se encuentran abiertos los siguientes puertos:
   - En el controlador

- **Puertos:** ssh (22), rmiregistry (1099), cisco-vpath-tun (6633). Openflow (6653), ldoms-migr (8101), intermapper (8181), sd (9876) y unknown (41469).
- **Servicios:** ssh (22), java-rmi (1099), http (8181) y sd (9876)

- En Mininet
  - **Puertos:** ssh (22)
  - **Servicios:** ssh (22)

B. En la fase de análisis de vulnerabilidades con OpenVas, se ha encontrado en total 33 (20 altas, 11 medias y 2 bajas) vulnerabilidades en el controlador ONOS y 11 (4 altas, 5 medias y 2 bajas) en la infraestructura Mininet. En el Apéndice A se adjunta la tabla de vulnerabilidades en detalle encontradas para el controlador y en el Apéndice B para Mininet.

C. En la fase de definición de objetivos con las herramientas nmap y netdiscover se puede identificar dos objetivos el controlador ONOS (192.168.41.113) y la infraestructura Mininet (192.168.41.114).

D. En la fase de explotación se realizan los siguientes ataques:
   - **DDoS:** se realizan ataques de DDoS con las herramientas sFlow-RT, Slowloris, XERXES y Hping3, siendo esta última la que genera una mayor amenaza para el controlador ONOS, observándose que afecta considerablemente al rendimiento de la GUI de ONOS. Si el ataque viene desde un host interno de la red, se ha realizado diversos tipos de ataques DDoS, observando que el Smurf attack es el que causa mayor daño.
   - **MITM:** se realiza un ataque de MITM con la herramienta Ettercap y se prueba accediendo a la GUI de ONOS y monitorizando el tráfico de red con Wireshark; se observa que se puede obtener las credenciales de acceso en texto plano.
   - **Cross-Site Scripting (XSS), inyección de HTML y CSRF:** se realiza un ataque de XSS con la herramienta Sdnpwn y se observa que la versión del controlador ONOS 2.7.0 no es vulnerable.
   - **Instalación de aplicación onos sin autenticación:** con la herramienta Sdnpwn se intenta instalar una aplicación en el controlador ONOS, sin embargo, este ataque no tiene éxito para la versión de ONOS 2.7.0.
   - **Uso de websocket sin autenticación:** se intenta realizar un ataque al websocket de ONOS con la ayuda de la herramienta Sdnpwn; sin embargo, esta no tiene éxito para la versión de 2.7.0 de ONOS.
   - **Secuestro de ubicación de host de red mediante envío de respuestas ARP:** se intenta secuestrar la ubicación de un host mediante el protocolo ARP con ayuda de la herramienta Sdnpwn, pero el módulo falla y no se logra realizar el ataque.
   - **Ataque LLDP replay con Sdnpwn:** si se intenta realizar un ataque de LLDP-replay con la herramienta Sdnpwn, se observa que al ejecutar el módulo no se produce ninguna actividad fuera de lo normal.
   - **Para la ejecución de cualquier otro ataque con la herramienta Sdnpwn:** se observa que los módulos producen errores de ejecución de código.

E. En la fase de post explotación se observa que para la arquitectura SDN en análisis se puede ejecutar esta fase del pentesting (cabe mencionar que no siempre se puede ejecutar), y se puede ejecutar un pivoteo entre el plano de datos y el plano de control haciendo uso del protocolo SSH.

5. Recomendaciones

Se recomienda tomar las siguientes acciones:

- Solucionar las vulnerabilidades detectadas en orden de severidad, es decir como prioridad se deben resolver las vulnerabilidades High, pasando por las Medium y terminando con las Low.
- Implementar medidas de seguridad a nivel de detección y monitorización (aplicar monitoreo continuo), algunas herramientas que pueden ayudar con esta labor pueden ser: IDS y SIEM. El SIEM de Wazuh podría ser una opción completa.
- Implementar medidas de seguridad a nivel de toma de acciones frente ataques como los testeados, tales como: IPS, SIEM y WAF.
- Implementar reglas dentro del Firewall para el tratamiento de los protocolos relacionados con las comunicaciones dentro de una SDN, como por ejemplo OpenFlow; y adicionalmente gestionar el protocolo SSH para que no pueda ser utilizado fuera de los usuarios y grupos permitidos sin necesidad de autenticación.
- Implementar un plan de riesgo y ejecutar autorías internas de manera cíclica para medir y detectar de manera permanente en el tiempo las vulnerabilidades detectadas. Una herramienta muy interesante es la de Wazuh que además de ser un SIEM, tiene integrado un módulo de gestión de vulnerabilidades.

6. Referencias

[1] SDN

https://www.vmware.com/es/topics/glossary/content/software-defined-networking.html

[2] DDoS

https://www.akamai.com/es/our-thinking/ddos#:~:text=Un%20ataque%20DDoS%2C%20o%20ataque,que%20no%20pueda%20funcionar%20correctamente.

[3] MITM

https://www.pandasecurity.com/es/mediacenter/seguridad/ataque-man-in-the-middle/

[4] ONOS

https://opennetworking.org/onos/

[5] Mininet

http://mininet.org/

[6] XSS

https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/

[7] CSRF

https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf/

[8] Websocket

https://developer.mozilla.org/es/docs/Web/API/WebSockets_API

[9] LLDP

https://www.whatsupgold.com/es/network-discovery/protocolo-de-deteccion-de-capas-lldp#:~:text=Link%20Layer%20Discovery%20Protocol%20(LLDP,sus%20pares%2Fvecinos%20conectados%20directamente.

[10] OpenVas

https://openvas.org/

[11] Offensive Security

https://www.offsec.com/reports/sample-penetration-testing-report.pdf

[12] OCTAVE

https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/

7. Anexos

Apéndice A.- Tabla de vulnerabilidades encontradas en el controlador ONOS.

VULNERABILIDADES EN CONTROLADOR ONOS					
Vulnerabilidad	**Severidad (Score)**	**Severidad**	**QoD**	**Host**	**Localización**
Ubuntu: Security Advisory (USN-5885-1)	9,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5825-2)	9,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5870-1)	9,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5891-1)	9,1	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5851-1)	8,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5867-1)	8,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5893-1)	8,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5958-1)	8,1	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5963-1)	7,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5912-1)	7,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5900-1)	7,8	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5892-1)	7,5	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5844-1)	7,5	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5901-1)	7,5	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5945-1)	7,5	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5848-1)	7,5	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5871-1)	7,5	High	97%	192.168.41.113	package

Ubuntu: Security Advisory (USN-5960-1)	7,5	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5921-1)	7,4	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5908-1)	7,2	High	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5886-1)	6,8	Medium	97%	192.168.41.113	package
Missing Linux Kernel mitigations for 'RETbleed' hardware vulnerabilities	6,5	Medium	80%	192.168.41.113	general/tcp
Ubuntu: Security Advisory (USN-5923-1)	5,5	Medium	97%	192.168.41.113	package
Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities	5,5	Medium	80%	192.168.41.113	general/tcp
Ubuntu: Security Advisory (USN-5928-1)	5,5	Medium	97%	192.168.41.113	package
Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities	5,5	Medium	80%	192.168.41.113	general/tcp
Ubuntu: Security Advisory (USN-5897-1)	5,3	Medium	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5846-1)	5	Medium	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5964-1)	5	Medium	97%	192.168.41.113	package
Ubuntu: Security Advisory (USN-5843-1)	5	Medium	97%	192.168.41.113	package
Cleartext Transmission of Sensitive Information via HTTP	4,8	Medium	80%	192.168.41.113	8181/tcp
TCP timestamps	2,6	Low	80%	192.168.41.113	general/tcp
ICMP Timestamp Reply Information Disclosure	2,1	Low	80%	192.168.41.113	general/icmp

Tabla 1.- Vulnerabilidades en controlador ONOS.

Apéndice B.- Tabla de vulnerabilidades encontradas en Mininet.

VULNERABILIDADES EN INFRAESTRUCTURA MININET					
Vulnerabilidad	**Severidad (Score)**	**Severidad**	**QoD**	**Host**	**Localización**
Ubuntu: Security Advisory (USN-5958-1)	8,1	High	97%	192.168.41.114	package

Ubuntu: Security Advisory (USN-5963-1)	7,8	High	97%	192.168.41.114	package
Wireshark Security Update (wnpa-sec-2023-08) - Linux	7,5	High	80%	192.168.41.114	general/tcp
Ubuntu: Security Advisory (USN-5960-1)	7,5	High	97%	192.168.41.114	package
Missing Linux Kernel mitigations for 'RETbleed' hardware vulnerabilities	6,5	Medium	80%	192.168.41.114	general/tcp
Ubuntu: Security Advisory (USN-5181-1)	6,1	Medium	97%	192.168.41.114	package
Missing Linux Kernel mitigations for 'SSB - Speculative Store Bypass' hardware vulnerabilities	5,5	Medium	80%	192.168.41.114	general/tcp
Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities	5,5	Medium	80%	192.168.41.114	general/tcp
Ubuntu: Security Advisory (USN-5964-1)	5	Medium	97%	192.168.41.114	package
TCP timestamps	2,6	Low	80%	192.168.41.114	general/tcp
ICMP Timestamp Reply Information Disclosure	2,1	Low	80%	192.168.41.114	general/icmp

Tabla 12.- Vulnerabilidades en Mininet.

8. Glosario

- **SDN:** Red definida por software. representan un enfoque en el que las redes utilizan controladores basados en software o interfaces de programación de aplicaciones (API) para dirigir el tráfico en la red y comunicarse con la infraestructura de hardware subyacente
- **DDoS:** Un ataque DDoS, o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente.
- **MITM:** es un tipo de ciberataque en el que los criminales interceptan una conversación o una transferencia de datos existente, ya sea escuchando o haciéndose pasar por un participante. A la víctima le parecerá que se está produciendo un intercambio de información normal, pero al introducirse en la conversación o transferencia de datos, el hacker puede obtener la información mientras pasa desapercibido.
- **ONOS:** es el controlador SDN de código abierto líder para crear soluciones SDN/NFV de próxima generación.

- **Mininet:** crea una red virtual realista, ejecutando código real de kernel, switch y aplicación, en una sola máquina (VM, nube o nativa)
- **XSS:** es un tipo de ataque en el cual actores maliciosos logran inyectar un script malicioso en un sitio web para luego ser procesado y ejecutado. Comúnmente, este proceso que se basa en la confianza que tiene el sitio sobre la entrada de los datos, consiste en enviar la URL con el payload precargado al usuario víctima con un objetivo determinado: robar datos personales del usuario, cookies de sesión, implementar técnicas de ingeniería social, entre otras.
- **CSRF:** técnica llamada falsificación de petición en sitios cruzados, proviene de su nombre en inglés Cross Site Request Forgery (CSRF o XSRF). Este ataque fuerza al navegador web de su víctima, validado en algún servicio (como por ejemplo correo o home banking) a enviar una petición a una aplicación web vulnerable.
- **Websocket:** es una tecnología avanzada que hace posible abrir una sesión de comunicación interactiva entre el navegador del usuario y un servidor. Con esta API, puede enviar mensajes a un servidor y recibir respuestas controladas por eventos sin tener que consultar al servidor para una respuesta.
- **LLDP:** es un protocolo de detección de vecino de la capa 2 que permite que los dispositivos anuncien la información del dispositivo a sus pares/vecinos conectados directamente. Es recomendable permitir que LLDP a nivel mundial estandarice la topología de red en todos los dispositivos si tiene una red de varios proveedores.