

Layer 2 Security Workshop

LAN network protection is generally neglected, which is a high risk to the organization or company. This Workshop will help you understand L2 vulnerabilities. By the end of this Workshop, you will gain real-world practical skills necessary for LAN security, this workshop is suitable for all interested in cybersecurity, Network Security and Penetration Testing.

Workshop Level

Intermediate level

Instructor

Mohanned Adil Omer

Requirements

- Participants must have a good knowledge about networking, TCP/IP and IP addressing; also know the basic knowledge of Linux.
- Participants must have a Good understanding of switching behavior and protocols.
- Participants should understand network services (DHCP, DNS, AD ... etc.).
- Participants should bring a laptop computer to participate in the lab, with 4GB RAM as minimum.

Date & Time

- Date: Saturday, x.x.x
- Time: 9:00 to 15:30

Outlines

1. Why L2 Security.
2. Switching review.
 - How switch work?
 - Switch weakness.
3. Sniffing Techniques
 - Packet Sniffers
 - PCAP and promiscuous mode.
 - Sniffing Tools.
 - Active and Passive Sniffing.
4. L2 Attacks and Defenses
 - Mac table Flooding.
 - ARP attack.

1. Introduction.
 2. When ARP is used?
 3. Types of ARP message.
 4. Example use of ARP.
 5. ARP cache.
 6. RARP.
 7. ARP Types.
 8. ARP Attacks.
 9. ARP Spoofing.
 10. ARP Denial of Service.
 11. Defenses.
 12. S-ARP.
 13. Conclusion.
5. DHCP attack
 - How DHCP Work.
 - DHCP Spoofing Attack.
 - DHCP Starvation Attack.
 - Defenses.
 - Conclusion.
 6. Some Guides to Minimum Security Baseline for any organization.
-

Revision #1

Created 28 October 2024 14:45:23 by sara

Updated 28 November 2024 13:10:52 by sara