



IPSec

3 days Hands on

1. Introduction to Tunneling
2. Security Associations
3. Just Enough IPsec Legacy
4. tcpdump Overview
5. Symmetric Encryption
6. PKI Encryption
7. Diffie-Hellman
8. Oakley
9. Extensible Authentication Protocol
10. Mode of Operation
11. IPsec Negotiation
12. How NAT Impacts IPsec
13. Encapsulation in Depth
14. IPsec ESP Protocol
15. IPsec AH Protocol
16. Penetration Testing

Lab Exercises:

1. Using tmux
2. Site-to-Site User Deployed Configs with PSK
3. IPsec Logging
4. IKEv2 Packet Analysis
5. Nflog Interface
6. Challenge - Problem at MS
7. Road Warrior PSK IKEv2
8. Challenge - Broken VPN
9. Challenge - Broken VPN
10. x509 Key Generation
11. Road Warrior x509 IKEv2
12. Certificate Revocation
13. Decrypting Existing pcap with Wireshark
14. Use Wireshark to decrypt IKEv2 from tcpdump
15. IKEv1 Capture
16. IKEv1 Analysis

17. IKEv2 Analysis
18. Radius
19. rw-eap-tls-only.md
20. ikev2-rw-eap-md5-rsa.md
21. Ram Based IP Pool
22. Challenge - New Road Warrior
23. Challenge - Broken Road Warrior #1
24. Challenge - Broken Road Warrior #2
25. IKE Penetration Testing