NETWORKING KNOWLEDGE DOMAIN

TYPICAL INDUSTRY ROLES

JUNIOR TESTER | PRACTITIONER TESTER | SENIOR TESTER | PRINCIPAL TESTER

KNOWLEDGE EXPECTATIONS FROM JUNIOR TO PRINCIPAL

NETWORK ARCHITECTURE

- Can interpret logical network diagrams
- Understands the various networks types that could be encountered during a penetration test:
  • CAT 5 / Fibre • 10/100/1000baseT • Wireless (802.11)
- Understand the difference beween LAN and WAN
- Understand internal (RFC 1918) IP ranges
- Understand basic subnetting
- Understand basics of IPv6 addressing
- Understand the security implications of copper cables vs fibre
- Understands the security benefits of tiered architectures, DMZs and air gaps
- Understands the security implications of shared media and can exploit its vulnerabilities during a penetration test
- Understands the security implications of switched networks
- Understands the security implications of VLANS
- Understands the core principles and concepts of a Software Defined Network (SDN), including:
  • Disassociation of data plane and control plane
  • The role of controllers in the control plane and commonly associated weaknesses
  • The role and common security risks of the application plane, the northbound API and common SDN applications

NETWORK ROUTING

- Understand default gateways and static routes
- Demonstrate ability to configure static IPs and routes
- Understands network routing and its associated protocols, including:
  • RIP• OSPF • EIGRP • BGP • IGMP
- Understands the security attributes of these protocols

NETWORK MAPPING

- Can demonstrate the mapping of a network using a range of tools, such as traceroute, traceroute and ping, and by querying active searches, such as DNS and SNMP servers
- Can accurately identify all hosts on a target network that meet a defined set of criteria, e.g., to identify all FTP servers or CISCO routers
- Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices
- Understand and exploit PXE

MANAGEMENT PROTOCOLS

- Understands and can demonstrate the use of protocols often used for the remote management of devices, including:
  • Telnet • SSH 16 • HTTP/HTTPS
  • SNMP • Cisco Reverse Telnet
  • TFTP • NTP • RDP •VNC
- Can analyse e-mail headers to identify system information
- Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices
- Can present the map as a logical network diagram, detailing all discovered subnets and interfaces, including routers, switches, hosts and other devices

TRAFFIC ANALYSIS

- Can intercept and monitor network traffic, capturing it to disk in a format required by analysis tools (e.g. PCAP)
- Understands and can demonstrate how network traffic can be analysed to recover user account credentials and detect vulnerabilities that may lead to the compromise of a target device

CONFIGURATION ANALYSIS

- Understands configuration files of Cisco routers and switches and can advise on how their security can be approved (most common features, such as access-lists and enabled services)
- Can interpret the configuration files of other network devices, including those produced by a variety of vendors (most common features, such as access-lists and enabled services)

ROUTERS & SWITCHERS

- Understands and can demonstrate the exploitation of vulnerabilities in routers and switches, including the use of the following protocols:
  • Telnet • SSH • HTTP/HTTPS • TFTP • SNMP

VOIP

- Understands VoIP services, such as SIP, and can identify and fingerprint devices offering these services