CYBER SECURITY TRAINING

Cyber Security Skill Set: General ICT Security

UNITS COVERED

ICTNWK502 Implement secure encryption technologies
ICTNWK406 Install, configure and test network security
ICTSAS418 Monitor and administer security of an ICT system
ICTNWK416 Build security into virtual private networks
Note: for unit details visit training.gov.au/Search/Training

FOCUS

The training focuses on:

- Learning encryption technologies based on current industry best practice and standards.
- Ensuring local networks security and connecting LANs together over public network with secure encrypted site-to-site VPN.
- Monitoring network and system securing to identify breaches.

SECURITY POLICY AND PLAN

The focus of the training program is on ISO 27000 series of standards (27001 and 27002) and the Australian Signals Directorate's Australia Government Information Security Manual. All recommended solutions are relevant to standards and best practice for compliance.

TRAINING APPROACH

The training approach for all Skill Sets has an all-of-infrastructure approach, as one aspect of security cannot be independent of another.

The training program strategy is to focus on one aspect at a time whilst always emphasising the need to consider integration.

Each skill set will also include underpinning knowledge about the processes, which are being practiced.

The cyber security program makes extensive use of the training materials for Cisco CCNA, CCNA Security, CompTIA Security +, Microsoft, Cisco Networking Academy and other materials including VMware.

The program also includes many Open Source projects including CentOS/RHEL and Debian with a multitude of their associated applications.

The emphasis throughout is on hands-on practice in a controlled environment where intentional vulnerabilities are provided for offensive security practice.

RTO 60142

ABOUT THE TRAINER

Michael Schmalfuss is a Cisco Certified Network Associate (CCNA), Microsoft Certified Professional (MCP), holds CompTIA Security + Certification, is a Cisco Networking Academy Instructor, has ICT60515 Advanced Diploma of Computer Systems Technology, maintains Australian Skills Quality Authority (ASQA) registered trainer and has more than 10 years of ICT Training and Assessment experience.

WE USE:

NMAP
Nessus
Wireshark
Kali Linux
Snort
SNMPSysLog
Alien Vault
Cisco IOS
Microsoft Servers
CentOS/RHEL
Debian
Nagios
Grafana
Cacti

CISCO CCNA SECURITY

The CCNA Security training material covers the various encryption levels in detail, which may then be applied to the practical tasks.

The training here starts with taking two servers and encrypting the traffic between them using IPSec. This is done by implementing a Security Policy in the Advanced Firewall configuration of the two hosts.

The Remote Access VPN practical task utilises various encrypt ion standards.

FIREWALLS

The first line of defence in protecting the enterprise digital assets is a firewall. Firewalls take many forms such as host -based, network-based and appliance. The training in this program utilises many different firewall technologies in the practical lab tasks as dictated by the infrastructure scenario. An example is for remote access VPN services the firewall must be configured on the Outside Edge Router , then the Inside LAN Router and then on the VPN Host Server itself.

Firewall technologies covered include:

- Windows Firewall
- Cisco Routers ACL and Context-Based
- iptables
- firewalld
- pfSense
- ipFire
- vyos

INTRUSION DETECTION AND PREVENTION WITH SNORT IDSIPS

This training program uses Snort Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) utilising the community rule sets and is now part of Cisco.

What can I do with Snort? "Snort has three primary uses: It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion prevention system."

DOES CISCO SELL SNORT?

"While Cisco does offer a commercial version of the Snort technology, we do not sell Snort. Cisco embraces the open source model and is committed to the GPL. Cisco leverages the Snort detection engine and Snort Subscriber Rule Set as the foundation for the Cisco Next Generation IPS and Next Generation Firewall. All enhancements made to the Snort technology for Cisco's commercial offerings are released back to the open source community."

THREAT DETECTION, INCIDENT RESPONSE, LOGGING, MONITORING AND COMPLIANCE WITH ALIENVAULT

This Cyber Security training program also uses AlienVault OSSIM for unified security for threat detection, incident response, and compliance. AlienVault OSSIM The world's most widely used open source Security Information and Event Management (SIEM). OSSIM is used to deploy and configure Host Based Intrusion Detection System (HIDS) agents, for configuring syslog and enabling plugins, for scanning your network for assets and vulnerabilities. OSSIM leverages the power of the AlienVault Open Threat Exchange (OTX).

VULNERABILITY ASSESSMENT WITH NESSUS

What are the vulnerabilities?

Once we have identified the hosts and services we will identify vulnerabilities using Nessus Vulnerability Assessment tools and Open VAS which will report to the system administrator potential weaknesses.

What are the threats?

Nessus will identify the threats by specific definitions and produce a report to highlight the relevant.

What is the risk?

We will study and practice risk levels and categories of risk in order to prioritise the remedial actions.

Mitigation

Nessus plugins provide recommendations for actions to take for each of the vulnerabilities detected.

Vulnerable Hosts Provided in Controlled Environment

A range of vulnerable hosts will be provided for the training course for students' to practice their techniques in a controlled environment. These systems stated here are provided for training as ready to use virtual machine appliances. The focus is on using the systems rather than installation and configuration.

Identify Hosts and Services with NMAP

The training will involve the practical use of network and service scanning to identify services visible to the network using ZenMap Network Scanner.

PENETRATION TESTING WITH KALI LINUX

Penetration testing with Kali Linux by Offensive Security includes a multitude of security tools covering all aspects of ICT. The use of these tools is based around the philosophy that you need to be able to use the tools which a hacker uses in order to properly deploy counter measures.

Categories Kali Linux Tools

- Information Gathering
- Vulnerability Analysis
- Wireless Attacks
- Web Applications
- Exploitation Tools
- Stress Testing
- Forensics Tools
- Sniffing and Spoofing
- Password Attacks
- Maintaining Access
- Reverse Engineering
- Hardware Hacking
- Reporting Tools

MICROSOFT RRAS, NAP, NPS AND VPN

Remote Access Virtual Private Network (VPN) using Microsoft Routing and Remote Access Service (RRAS) including Network Access Protection (NAP) and Network Policy Service (NPS) for Remote User access to the main enterprise campus via the public network.

This measure also includes Active Directory Domain Services (ADDS) User Authentication and Group Policy Object s (GPO).

MICROSOFT ADDS WITH GPO AND NTFS PERMISSIONS

The unit is covered with the training task which focuses on Active Directory Domain Services (ADDS) User Authentication and Group Policy Objects (GPO) for security enforcement. Password Policy managed in ADDS based on best practice recommendations. Password testing is carried out using the Kali Linux Security Tools utilities.

SITE-TO-SITE VPN WITH IPSEC AND CISCO IOS

Site-to-Site VPN using IPSec protocol stack on Cisco IOS Router and Switch infrastructure to make a secure remote office connection to the main enterprise campus via the public network.

Site-to-Site VPN with IPSec and Cisco IOS

Site-to-Site VPN using IPSec protocol stack on Cisco IOS Router and Switch infrastructure to make a secure Remote Office connection to the main enterprise campus via the public network.

Logging and Alerts with AlienVault, Grafana, Cacti and Nagios

Audit and alerts performed with system logs and monitoring being sent to the logging server. In training we use OpenNMS Network Monitoring Service and Grafana for Reporting and Analysis. Other platforms for logging and recording are AlienVault or CactiEZ and Nagios.

Web Services SSL and PKI Certificate Authority

You will learn about Web Server Hardening and the importance of Security for Web Services using Secure Socket Layer (SSL) with and Certificate Authority (CA).

Email services are provided for training with spam and virus protection including monitoring and logging. We use ISPconfig3 as a Web Hosting and Email Server

Training Materials Available via Online Learning Management System trainict.net/lms