



TECHNET srl

- Via Renato Cesarini, 58/60 – 00144 – Roma
Tel/1. 06 54229198 Tel/2. 06 5925818
- Via Socrate 26 - 20128 - Milano
Tel. 02 76280395

P. IVA: 01508940663 – CCIAA: 11380/00/AQ



PROMETRIC - PEARSON VUE - KRYTERION
Cisco, Juniper and Microsoft authorized Trainers



70-298: Designing Security for a Microsoft Windows Server 2003 Network MS-2830

Designing Security for Microsoft Networks

Questo corso con istruttore fornisce agli studenti le conoscenze e le competenze necessarie per progettare un'infrastruttura di rete protetta. Gli argomenti trattati comprendono la costituzione di un team di progettazione, la definizione delle minacce e l'analisi dei rischi legati alla protezione allo scopo di soddisfare i requisiti aziendali relativi alla protezione dei computer in un ambiente di rete. Il corso sviluppa le competenze decisionali attraverso uno strumento interattivo che simula scenari di vita reale. Agli studenti verrà affidato il compito di raccogliere le informazioni e di analizzarle in dettaglio per trovare la soluzione più adeguata al requisito assegnato relativo alla protezione.

Obiettivi:

- Progettare un'infrastruttura per la protezione della rete
- Identificare le minacce alla protezione della rete
- Analizzare i rischi relativi alla protezione
- Progettare come proteggere le risorse fisiche
- Progettare come proteggere i computer
- Progettare come proteggere gli account
- Progettare come garantire l'autenticazione
- Progettare come assicurare la protezione dei dati
- Progettare come garantire la protezione della trasmissione dei dati
- Progettare come garantire la protezione dei perimetri di rete
- Definire una procedura di risposta agli incidenti

In questo corso verranno inoltre presentate tre facili appendici che trattano i seguenti argomenti:

- Progettazione di un criterio di utilizzo accettabile
- Progettazione di criteri per la gestione delle reti
- Progettazione di un'infrastruttura di operazioni per la gestione della protezione

Web: www.techneteu.com

Email: tecnico@techneteu.com

B.N.L - Via di Santa Prisca, 28 – 00153 - Roma
IBAN: IT09 L010 0503 2190 0000024920 SWIFT: BNLIITRR

POSTE ITALIANE - Agenzia Business – 00144 - Roma Eur
IBAN: IT76H 07601 03200 000039079777



TECHNET srl

- Via Renato Cesarini, 58/60 – 00144 – Roma
Tel/1. 06 54229198 Tel/2. 06 5925818
- Via Socrate 26 - 20128 - Milano
Tel. 02 76280395

P. IVA: 01508940663 – CCIAA: 11380/00/AQ



PROMETRIC - PEARSON VUE - KRYTERION
Cisco, Juniper and Microsoft authorized Trainers



Programma:

Module 1: Introduction to Designing Security

This module describes the basic framework for designing network security and introduces key concepts used throughout the course. It also introduces an ongoing case study that is utilized in the labs.

Lessons

- Introduction to Designing Security for Microsoft Networks
- Contoso Pharmaceuticals: A Case Study

Module 2: Creating a Plan for Network Security

This module discusses the importance of security policies and procedures in a security design. It also explains how a security design team must include representation from various members of your organization. After completing this module, you will be able use a framework for designing security and create a security design team.

Lessons

- Introduction to Security Policies
- Defining a Process for Designing Network Security
- Creating a Security Design Team

Lab A: Planning a Security Framework

Module 3: Identifying Threats to Network Security

This module explains how to identify likely threats to a network and explains attacker motivations. After completing this module, you will be able to explain common threats and predict threats by using a threat model.

Lessons

- Introduction to Security Threats
- Predicting Threats to Security

Lab A: Identifying Threats to Network Security

Module 4: Analyzing Security Risks

This module explains how to determine what resources in an organization require protection and how to categorize them in order to assign an appropriate level of protection. After completing this module, you will be able to apply a framework for planning risk management.

Lessons

- Introduction to Risk Management
- Creating a Risk Management Plan

Lab A: Analyzing Security Threats

Web: www.techneteu.com

Email: tecnico@techneteu.com

B.N.L - Via di Santa Prisca, 28 – 00153 - Roma
IBAN: IT09 L010 0503 2190 0000024920 SWIFT: BNLIITRRR

POSTE ITALIANE - Agenzia Business – 00144 - Roma Eur
IBAN: IT76H 07601 03200 000039079777



TECHNET srl

- Via Renato Cesarini, 58/60 – 00144 – Roma
Tel/1. 06 54229198 Tel/2. 06 5925818
- Via Socrate 26 - 20128 - Milano
Tel. 02 76280395

P. IVA: 01508940663 – CCIAA: 11380/00/AQ



PROMETRIC - PEARSON VUE - KRYTERION
Cisco, Juniper and Microsoft authorized Trainers



Module 5: Creating a Security Design for Physical Resources

This module describes threats and risks to physical resources in an organization, as well as how to secure facilities, computers, and hardware. After completing this module, you will be able to design security for physical resources.

Lessons

- Determining Threats and Analyzing Risks to Physical Resources
- Designing Security for Physical Resources

Lab A: Designing Security for Physical Resources

Module 6: Creating a Security Design for Computers

This module explains how to determine threats and analyze risks to computers on your network. After completing this module, you will be able to design security for computers.

Lessons

- Determining Threats and Analyzing Risks to Computers
- Designing Security for Computers

Lab A: Designing Security for Computers

Module 7: Creating a Security Design for Accounts

This module describes the threats and risks to accounts in an organization. After completing this module, you will be able to design security for accounts.

Lessons

- Determining Threats and Analyzing Risks to Accounts
- Designing Security for Accounts

Lab A: Designing Security for Accounts

Module 8: Creating a Security Design for Authentication

This module describes threats and risks to authentication. After completing this module, you will be able to design security for authentication.

Lessons

- Determining Threats and Analyzing Risks to Authentication
- Designing Security for Authentication

Lab A: Designing Authentication Security

Module 9: Creating a Security Design for Data

This module examines threats and risks to data. After completing this module, you will be able to design security for data.

Lessons

Web: www.techneteu.com

Email: tecnico@techneteu.com

B.N.L - Via di Santa Prisca, 28 – 00153 - Roma
IBAN: IT09 L010 0503 2190 0000024920 SWIFT: BNLIITRR

POSTE ITALIANE - Agenzia Business – 00144 - Roma Eur
IBAN: IT76H 07601 03200 000039079777



TECHNET srl

- Via Renato Cesarini, 58/60 – 00144 – Roma
Tel/1. 06 54229198 Tel/2. 06 5925818
- Via Socrate 26 - 20128 - Milano
Tel. 02 76280395

P. IVA: 01508940663 – CCIAA: 11380/00/AQ



PROMETRIC - PEARSON VUE - KRYTERION
Cisco, Juniper and Microsoft authorized Trainers



-
- Determining Threats and Analyzing Risks to Data
 - Designing Security for Data

Lab A: Designing Security for Data

Module 10: Creating a Security Design for Data Transmission

This module discusses threats and risks to data transmission. After completing this module, you will be able to design security for data transmission.

Lessons

- Determining Threats and Analyzing Risks to Data Transmission
- Designing Security for Data Transmission

Lab A: Designing Security for Data Transmission

Module 11: Creating a Security Design for Network Perimeters

This module describes threats to the points where your network connects to other networks, such as the Internet. After completing this module, you will be able to design security for network perimeters.

Lessons

- Determining Threats and Analyzing Risks to Network Perimeters
- Designing Security for Network Perimeters

Lab A: Designing Security for Network Perimeters

Module 12: Designing Responses to Security Incidents

This module provides information about auditing and creating procedures to direct how you respond to security incidents. After completing this module, you will be able to design an audit policy and an incident response procedure.

Lessons

- Introduction to Auditing and Incident Response
- Designing an Audit Policy
- Designing an Incident Response Procedure

Lab A: Designing an Incident Response Procedure

Appendices

Appendix A: Designing an Acceptable Use Policy

This appendix provides information about creating policies for acceptable use of network resources by users.

Lessons

- Analyzing Risks That Users Introduce

Web: www.techneteu.com

Email: tecnico@techneteu.com

B.N.L - Via di Santa Prisca, 28 – 00153 - Roma
IBAN: IT09 L010 0503 2190 0000024920 SWIFT: BNLIITRR

POSTE ITALIANE - Agenzia Business – 00144 - Roma Eur
IBAN: IT76H 07601 03200 000039079777



TECHNET srl

- Via Renato Cesarini, 58/60 – 00144 – Roma
Tel/1. 06 54229198 Tel/2. 06 5925818
- Via Socrate 26 - 20128 - Milano
Tel. 02 76280395

P. IVA: 01508940663 – CCIAA: 11380/00/AQ



PROMETRIC - PEARSON VUE - KRYTERION
Cisco, Juniper and Microsoft authorized Trainers



-
- Designing Security for Computer Use

Appendix B: Designing Policies for Managing Networks

This appendix offers guidelines for ensuring that network administrators manage networks in a secure manner.

Lessons

- Analyzing Risks to Managing Networks
- Designing Security for Managing Networks

Appendix C: Designing an Operations Framework to Manage Security

This appendix explains how to create a framework to ensure security of a network as the network changes and as the security requirements of the organization change.

Lessons

- Analyzing Risks to Ongoing Network Operations
- Designing a Framework for Ongoing Network Operation

Web: www.techneteu.com

Email: tecnico@techneteu.com

B.N.L - Via di Santa Prisca, 28 – 00153 - Roma
IBAN: IT09 L010 0503 2190 0000024920 SWIFT: BNLIITRRR

POSTE ITALIANE - Agenzia Business – 00144 - Roma Eur
IBAN: IT76H 07601 03200 000039079777