OUTCOME BASED EDUCATION

CURRICULUM AND DETAILED SYLLABI

FOR

M.E. COMPUTER SCIENCE AND INFORMATION SECURITY DEGREE PROGRAMME

TWO CREDIT COURSES

FOR THE STUDENTS ADMITTED IN THE

ACADEMIC YEAR 2016-17 ONWARDS

THIAGARAJAR COLLEGE OF ENGINEERING

(A Government Aided ISO 9001:2008 certified Autonomous Institution affiliated to Anna University)

MADURAI – 625 015, TAMILNADU

Phone: 0452 – 2482240, 41
Fax: 0452 2483427
Web: www.tce.edu

Passed in Board of Studies Meeting on 29.04.2016 Approved in Academic Council Meeting on 18.06.2016

LIST OF TWO CREDIT COURSES

S. No.	COURSE CODE	COURSE NAME
1	14IS2A0	MALICIOUS SOFTWARE ANALYSIS
2	14IS2B0	ADVANCES IN NETWORK SECURITY AND MANAGEMENT

14IS2A0	MALICIOUS SOFTWARE ANALYSIS	Category	L	T	P	Credit
		PE	2	0	0	2

Preamble

This course explores malware analysis tools and techniques in depth. Understanding the capabilities of malware is critical to an organization's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside-out.

Prerequisite

- 14IS120 - Cryptography
- 14IS130 - Network Security
- 14IS210 - System Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1:	Explain the characteristics of Malware and its effects on Computing systems.	Understand
CO2:	Practice the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.	Apply
CO3:	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	L										
CO2	M	M			L						
CO3	S	S	M		M	M		M	M	L	

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	CAT - I	Terminal Examination
Remember	-	20
Understand	-	30
Apply	40	50
Analyse	60	0
Evaluate	-	0
Create	-	0

- CAT – 1 is used to evaluate the CO2 and CO3 in 40% and 60% respectively through Lab Assessment
- Terminal Examination is used to evaluate CO1, CO2 and CO3 through written examination.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Define Malware
2. List the types of Malware Anaysis.
3. State the need and types of Malware Analysis
4. State the reason for Malware Analysis in the online webpages.
5. Compare the PE and Non-PE Structure.
6. Describe the use of YARA Rules in Dynamic Analysis
7. Give the working principle for Anti-virus.

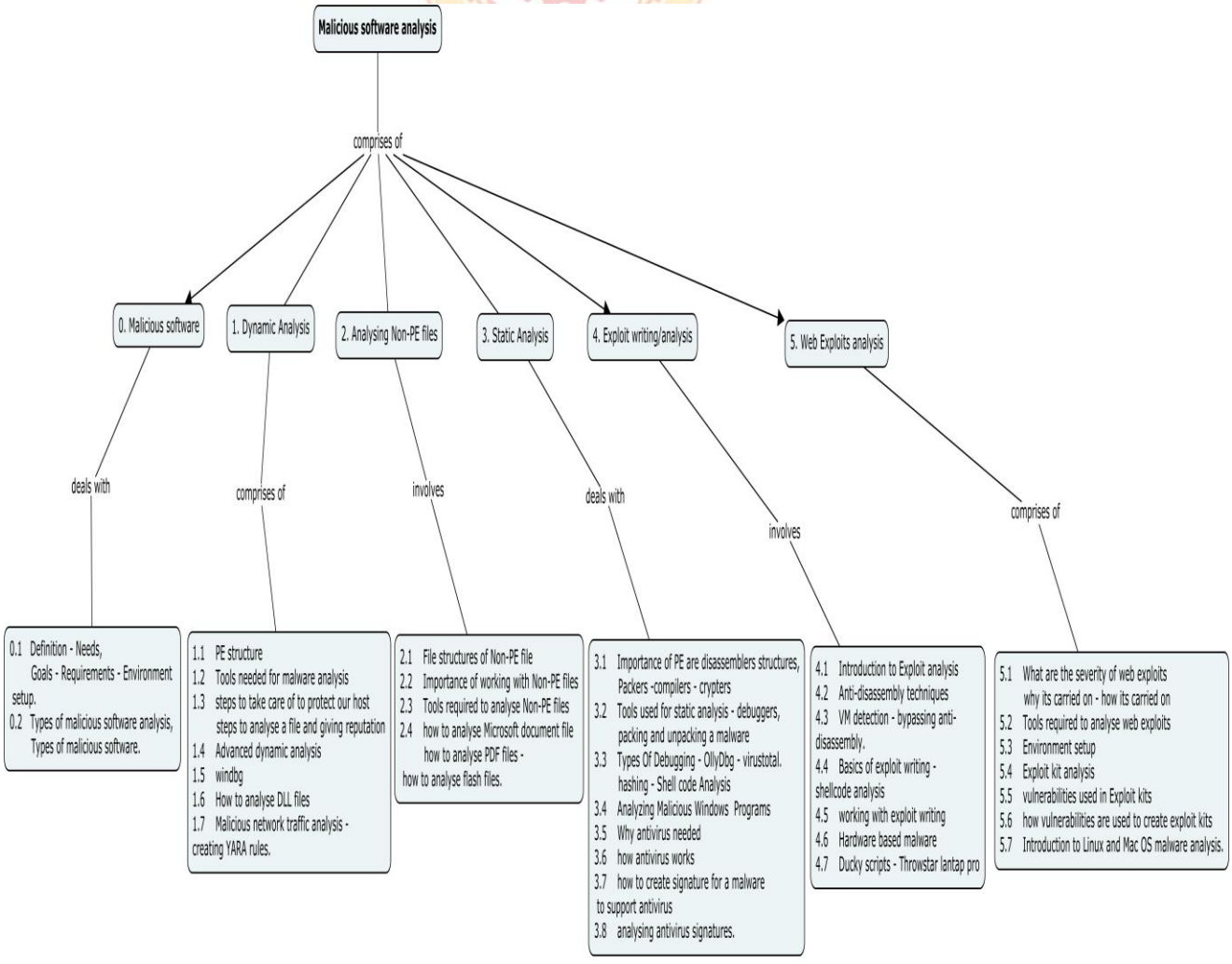
Course Outcome 2 (CO2):

1. Illustrate with suitable example, how to create YARA rules.
2. Apply suitable Malware analysis, through which malware signature can be created for Anti-virus.
3. Distinguish the use of Static and Dynamic Analysis in Malware applications.
4. Compare the application of Web exploits in Malware

Course Outcome 3 (CO3)

Analyze the Banking application for the possible vulnerabilities and perform Malware analysis using, FakeAV malware, ZeroAccess Rootkit, Ransomware, DLL malware and Trojan.

Concept Map



Syllabus

Malicious software: Definition - Needs - Goals - Requirements - Environment setup - Types of malicious software analysis, Types of malicious software.

Dynamic Analysis: PE structure - Tools needed for malware analysis - steps to take care of to protect our host - steps to analyse a file and giving reputation - Advanced dynamic analysis - windbg - How to analyse DLL files - Malicious network traffic analysis - creating YARA rules.

Analysing Non-PE files: File structures of Non-PE file - Importance of working with Non-PE files - Tools required to analyse Non-PE files - how to analyse Microsoft document file - how to analyse PDF files - how to analyse flash files.

Static Analysis: Importance of PE are disassemblers structures - Packers -compilers - crypters - Tools used for static analysis - debuggers - packing and unpacking a malware - Types Of Debugging - OllyDbg - virustotal - hashing - Shell code Analysis - Analyzing Malicious Windows Programs - Why antivirus needed - how antivirus works - how to create signature for a malware to support antivirus - analysing antivirus signatures.

Exploit writing/analysis: Introduction to Exploit analysis - Anti-disassembly techniques - VM detection - bypassing anti-disassembly - basics of exploit writing - shellcode analysis - working with exploit writing - Hardware based malware - Ducky scripts - Throwstar lantap pro.

Web Exploits analysis: What are the severity of web exploits - why its carried on - how its carried on - tools required to analyse web exploits - Environment setup -Exploit kit analysis - vulnerabilities used in Exploit kits - how vulnerabilities are used to create exploit kits - Introduction to Linux and Mac OS malware analysis.

Hands-on Topics:

1. Live analysis on FakeAV malware, DLL malware samples and ZeroAccess Rootkit.
2. Practical session on Ransomware and FakeAv for trainees.
3. Practical session on Trojan.RAT dll file, Pony loader malware, mass-mailer worm, zbot trojan for trainees.
4. Live analysis on Microsoft document file embedded with malware
5. Practical session on w97m.downloader, OLE component w97m.downloader malware.
6. Analysis of suspicious JPG file.
7. Practical session on JPG malware analysis.
8. Live analysis on PDF file embedded with malware
9. Practical session on DOC,PDF malware files for trainees.
10. Live session on static analysis of a malware sample (PlugX rat), basic exploit writing.
11. Practical session on static analysis of a Netsky worm for trainees, static analysis of packers
12. Practical session on exploit writing, hardware based malware, JavaScript malwares, creating signature for a malware, analysing web exploits for trainees.
13. Live analysis of Web exploits, antivirus signature creation.
14. YARA rules creation.
15. Live session on exploiting vulnerabilities in a program, windows vulnerability and installing Ransomware

Textbook

1. Michael Sikorski and Andrew Honig, "Practical Malware Analysis" ,No starch press, February, 2012.
2. Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard , "Malware Analyst's Cookbook" , John Wiley & Sons, October, 2010.
3. Mark Russinovich, David A. Solomon, Alex Ionescu "Windows Internals", Microsoft Press, 6th edition, 2012.

4. Abraham Silberschatz , Peter B. Galvin, Greg Gagne, "Operating System Concepts", John Wiley & Sons, Inc., 9th edition, 2015.

Web References

1. http://opensecuritytraining.info/ReverseEngineeringMalware.html
2. https://zeltser.com/reverse-malware-cheat-sheet/
3. http://arteam.accessroot.com/arteam/site/download.php?view.112
4. https://tuts4you.com/download.php?list.17
5. https://technet.microsoft.com/en-in/sysinternals/bb963901.aspx
6. http://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103/.git/HEAD
7. https://zeltser.com/build-malware-analysis-toolkit/

Course Contents and Lecture Schedule

Module .No	Topics	No. of Lectures
0.	**Malicious software**	
0.1	Definition - Needs - Goals - Requirements - Environment setup.	1
0.2	Types of malicious software analysis, Types of malicious software.	
1.	**Dynamic Analysis**	
1.1	PE structure	1
1.2	Tools needed for malware analysis	
1.3	steps to take care of to protect our host - steps to analyse a file and giving reputation	1
1.4	Advanced dynamic analysis	
1.5	windbg	1
1.6	How to analyse DLL files	
1.7	Malicious network traffic analysis - creating YARA rules.	1
2.	**Analysing Non-PE files**	
2.1	File structures of Non-PE file	1
2.2	Importance of working with Non-PE files	1
2.3	Tools required to analyse Non-PE files	
2.4	how to analyse Microsoft document file - how to analyse PDF files - how to analyse flash files.	2
3.	**Static Analysis**	
3.1	Importance of PE are disassemblers structures - Packers - compilers - crypters	2
3.2	Tools used for static analysis - debuggers - packing and unpacking a malware	
3.3	Types Of Debugging - OllyDbg - virustotal - hashing - Shell code Analysis	2
3.4	Analyzing Malicious Windows Programs	
3.5	Why antivirus needed	3
3.6	how antivirus works	
3.7	how to create signature for a malware to support antivirus	
3.8	analysing antivirus signatures.	

4.	**Exploit writing/analysis**	
4.1	Introduction to Exploit analysis	1
4.2	Anti-disassembly techniques	
4.3	VM detection - bypassing anti-disassembly.	2
4.4	Basics of exploit writing - shellcode analysis	
4.5	working with exploit writing	2
4.6	Hardware based malware	
4.7	Ducky scripts - Throwstar lantap pro	
5.	**Web Exploits analysis**	
5.1	What are the severity of web exploits - why its carried on - how its carried on	1
5.2	Tools required to analyse web exploits	1
5.3	Environment setup	1
5.4	Exploit kit analysis	1
5.5	vulnerabilities used in Exploit kits	1
5.6	how vulnerabilities are used to create exploit kits	1
5.7	Introduction to Linux and Mac OS malware analysis.	1
Total Lecture Hours		**28**

Course Designers:

1. Ms..J.Reegun Richard reegunj@outlook.com

Industry : Symantec Corporation, India

Area of Interests : Vulnerability researching in windows and web application penetration testing, analysing targeted attacks like exploit kits, Dynamic& static analysis of malware, Network traffic analysis, Adding rules to malicious network traffic, detailed analysis on malicious network traffic to get the URI patterns for exploit kits and targeted attacks, Expertise in removing malwares/rootkits manually.

2. Ms.M.Thangavel thangavelmuruganme@gmail.com / mtit@tce.edu

14IS2B0	ADVANCES IN NETWORK SECURITY AND MANAGEMENT	Category	L	T	P	Credit
		PE	2	0	0	2

Preamble

Network management and security are essential factors in the reliable, efficient, and secure operation of networks. As businesses become increasingly dependent on networking services, keeping these services running and secure becomes synonymous with keeping the business running. This course provides a thorough introduction to network management technologies and standards as well as to a wide variety of techniques for evaluating, monitoring, and defending the security of computer networks and systems. This course provides the fundamental knowledge to analyze risks to the system and implement a workable security policy that protects the information assets from potential intrusion, damage or theft. Topics include secure routing and switching, Firewall technologies, VPN Technology, Intrusion Prevention/Detection systems.

Prerequisite

14IS130 - Network Security

Course Outcomes

On the successful completion of the course, students will be able to

Course Outcomes		Bloom's Level
CO1	Examine the need of security for the given network scenario.	Apply
CO2	Criticize the preventive measures to secure routing and switching.	Analyze
CO3	Infer the design of firewall, VPN and IDS / IPS for the given network.	Analyze

Mapping with Programme Outcomes

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	M	M			L						
CO2	S	S	M		M	M		M	M	L	S
CO3	S	S	M		M	M		M	M	L	S

S- Strong; M-Medium; L-Low

Assessment Pattern

Bloom's Category	CAT - I	Terminal Examination
Remember	-	20
Understand	-	30
Apply	40	50
Analyse	60	0
Evaluate	-	0
Create	-	0

- CAT – 1 is used to evaluate the CO2, CO3 in 40%, 60% respectively through Lab Assessment
- Terminal Examination is used to evaluate CO1, CO2, CO3 through written examination.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Infer the importance of CIA in Network security.
2. Relate Network attack methods and vectors.
3. Outline the importance of Network security for a virtual environment
4. Explain data loss and exfiltration methods
5. Interpret good security practices for network management.

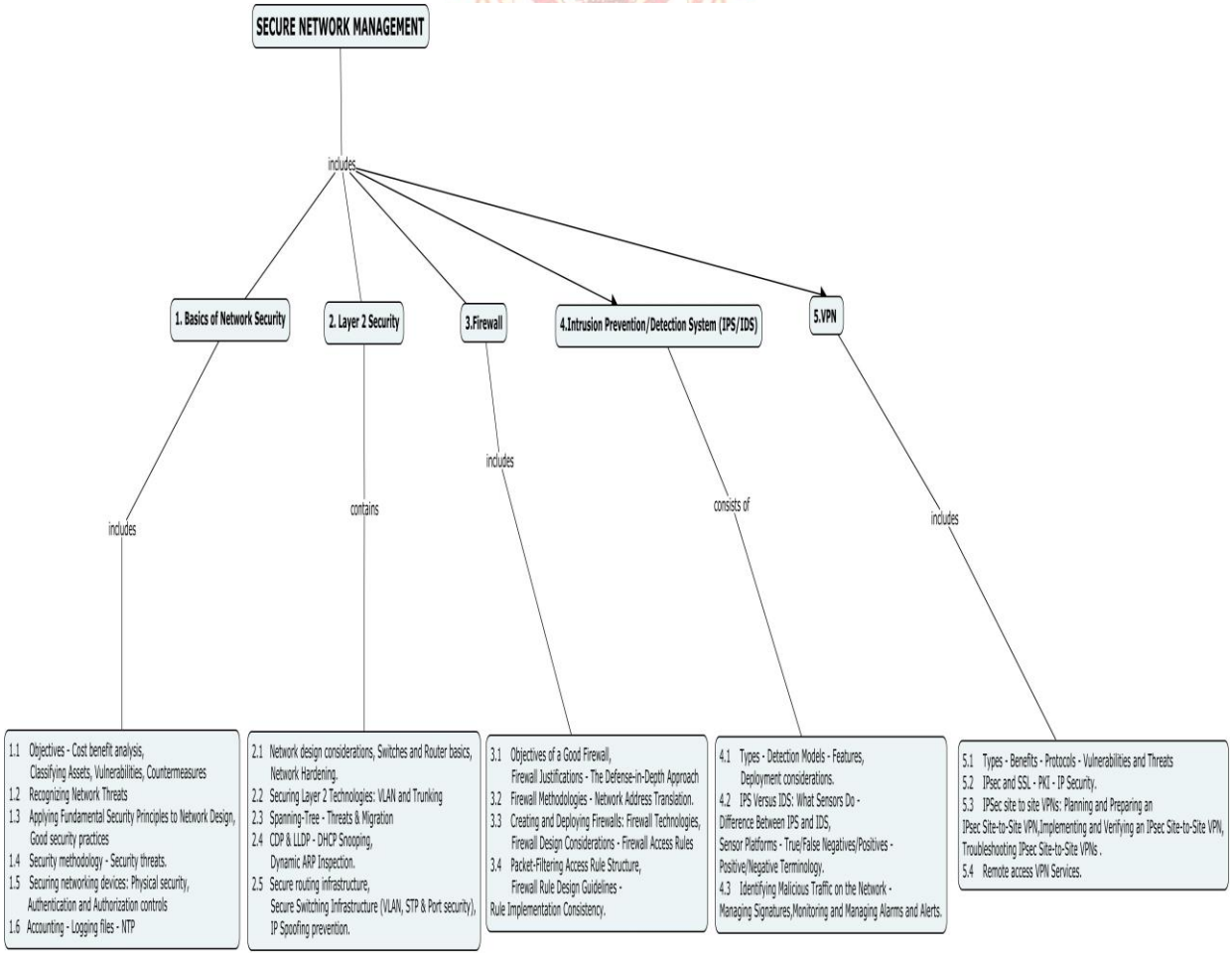
Course Outcome 2 (CO2):

1. Illustrate trunking with 802.1Q.
2. Identify the best practices and security toolkit to migrate from common layer 2 threats.
3. Develop an s secure routing infrastructure between two different organizations.
4. Model secure switching infrastructure for any educational organization.
5. Utilize the IP Spoofing prevention techniques to solve the network security threats and attacks.

Course Outcome 3 (CO3):

1. Analyze the configuration of IPSec for the simulated network.
2. Inspect the troubleshooting steps of IPsec Site-to-Site VPNs in Cisco IOS
3. Examine the Firewall rules in a Desktop computer.
4. Identify the Malicious traffic in the network using appropriate tools.
5. Simplify the steps for monitoring and managing the alerts and alarms

Concept Map



Syllabus

Basics of Network Security: Objectives - Cost benefit analysis - Classifying Assets, Vulnerabilities, Countermeasures - Recognizing Network Threats - Applying Fundamental Security Principles to Network Design - Good security practices - Security methodology - Security threats. Securing Networking Devices: Physical security - Authentication and Authorization controls - Accounting - Logging files - NTP.

Layer 2 security: Network design considerations - Switch and Router basics - Network Hardening. Securing Layer 2 Technologies: VLAN and Trunking - Spanning-Tree - Threats & Migration - CDP & LLDP - DHCP Snooping - Dynamic ARP Inspection. Secure routing infrastructure - Secure Switching Infrastructure (VLAN, STP & Port security) - IP Spoofing prevention.

Firewall: Objectives of a Good Firewall - Firewall Justifications - The Defense-in-Depth Approach - Firewall Methodologies - Network Address Translation. Creating and Deploying Firewalls: Firewall Technologies - Firewall Design Considerations - Firewall Access Rules - Packet-Filtering Access Rule Structure - Firewall Rule Design Guidelines - Rule Implementation Consistency.

Intrusion Prevention/Detection System (IPS/IDS): Types - Detection Models - Features - Deployment considerations. IPS Versus IDS: What Sensors Do - Difference Between IPS and IDS - Sensor Platforms - True/False Negatives/Positives - Positive/Negative Terminology. Identifying Malicious Traffic on the Network - Managing Signatures - Monitoring and Managing Alarms and Alerts.

VPN Technology: Types - Benefits - Protocols - Vulnerabilities and Threats - IPsec and SSL - PKI - IP Security. IPSec site to site VPNs: Planning and Preparing an IPsec Site-to-Site VPN - Implementing and Verifying an IPsec Site-to-Site VPN - Troubleshooting IPsec Site-to-Site VPNs . Remote access VPN Services.

Textbook

1. John Stuppi, Omar Santos, "CCNA Security 210-260 Official Cert Guide", Publisher: Cisco Press, ISBN: 9780134077857, Release Date: September 2015.
2. Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg, " Network Security: The Complete Reference", Publisher: McGraw-Hill Osborne Media, Edition: First, Released: October, 2013

References

1. Joseph Migga Kizza, “Computer Network Security”, Springer, 2005.
2. Douglas R. Stinson, “Cryptography Theory and Practice”, Third Edition, Chapman & Hall/CRC, 2006
3. William Stallings, “Network Security Essentials Applications and Standards”, Pearson Education, Fourth Edition, 2011
4. William Stallings, Lawrie Brown, “Computer Security: Principles and Practice”, First Edition, 2008.
5. “VPN Security”, The Government of the Hong Kong Special Administrative Region 2008.

Course Contents and Lecture Schedule

Module. No	Topics	No. of Lectures
1	**Basics of Network Security**	
1.1	Objectives - Cost benefit analysis - Classifying Assets, Vulnerabilities, Countermeasures	1
1.2	Recognizing Network Threats	1
1.3	Applying Fundamental Security Principles to Network Design - Good security practices	1

1.4	Security methodology - Security threats.	1
1.5	Securing Networking Devices - Physical Security - Authentication and Authorization controls	1
1.6	Accounting - Logging files - NTP	1
2	**Layer 2 Security**	
2.1	Network design considerations - Switch and Router basics - Network Hardening.	1
2.2	Securing Layer 2 Technologies: VLAN and Trunking	1
2.3	Spanning-Tree - Threats & Migration	1
2.4	CDP & LLDP - DHCP Snooping - Dynamic ARP Inspection.	1
2.5	Secure routing infrastructure - Secure Switching Infrastructure (VLAN, STP & Port security) - IP Spoofing prevention.	2
3	**Firewall**	
3.1	Objectives of a Good Firewall - Firewall Justifications - The Defense-in-Depth Approach	1
3.2	Firewall Methodologies - Network Address Translation.	1
3.3	Creating and Deploying Firewalls: Firewall Technologies - Firewall Design Considerations - Firewall Access Rules	2
3.4	Packet-Filtering Access Rule Structure - Firewall Rule Design Guidelines - Rule Implementation Consistency.	2
4	**Intrusion Prevention/Detection System (IPS/IDS)**	
4.1	Types - Detection Models - Features - Deployment considerations.	1
4.2	IPS Versus IDS: What Sensors Do - Difference Between IPS and IDS - Sensor Platforms - True/False Negatives/Positives - Positive/Negative Terminology.	1
4.3	Identifying Malicious Traffic on the Network - Managing Signatures - Monitoring and Managing Alarms and Alerts.	2
5	**VPN Technology**	
5.1	Types - Benefits - Protocols - Vulnerabilities and Threats	1
5.2	IPsec and SSL - PKI - IP Security.	1
5.3	IPSec site to site VPNs: Planning and Preparing an IPsec Site-to-Site VPN - Implementing and Verifying an IPsec Site-to-Site VPN - Troubleshooting IPsec Site-to-Site VPNs .	2
5.4	Remote access VPN Services.	2
Total Lecture Hours		**28**

Course Designers:

1. Manigandan Sellamuthu — sendmanigandan@gmail.com
   Industry : Symantec Corporation, India
   Profile : His professional background includes more than 12 years of experience as Network & Information Security Engineer with extensive technical and project management skills.
   He currently Holding various vendor certification such SANS - (GCIA,GCIH,GSSEC),
   Checkpoint - (CCSA,CCSE),
   Cisco -(CCSP,CCIE-Written),
   Sourcefire -(SFCP).
2. Thangavel M — thangavelmuruganme@gmail.com / mtit@tce.edu