JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule PuneUniversity,Pune)

Structure and Syllabus

for

B. Tech. Information Technology

with Honors in

"Machine Learning for Cyber Security"

w. e. f. Academic Year 2021-2022

(2019 Pattern)

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

B. Tech. Information Technology
(Honors Course)
Machine Learning for Cyber Security

Course Code	Course	Teaching Scheme			Examination Schemes						Credits
		TH	Tut	Lab	Theory			Practical		Total	Total
					ISE (15)	MSE (25)	ESE (60)	TW	Lab		
T. Y. Sem V											
ITH3101	Foundations of Cyber Security	04	-	-	15	25	60	-	-	100	04
T. Y. Sem VI											
ITH3102	Machine Learning and Cyber Security	03	-	02	15	25	60	-	25	125	04
ITH3103	Machine Learning for Penetration Testing	03	-	02	15	25	60	-	25	125	04
B. Tech. Sem VII or Sem VIII											
ITH4101	Usable Security	04	-	-	15	25	60	-	-	100	04
ITH4102	Software Security	04	-	-	15	25	60	-	-	100	04
Total		**18**	**-**	**04**	**75**	**125**	**300**	**-**	**50**	**550**	**20**

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

T. Y. B. Tech (Department of Information Technology)
Academic Year – 2021-2022 Semester -V
[ITH3101]: Foundations of Cyber Security

Teaching Scheme:	Credits:	Examination Scheme:
TH : 04 Hours/Week	TH : 04	In Sem. Evaluation : 15 Marks Mid Sem. Exam : 25 Marks End Sem. Exam : 60 Marks Total Marks : 100 Marks

Course Prerequisites: Computer Networks

Course Objective:
To learn about the most basic aspects of cyber security, including the impact of cyber attacks and the most common cyber security roles.

Course Outcome:
After successful completion of the course, students will able to:
CO1: Learn security fundamentals, including common threats and tools to prevent attacks
CO2: Study basics of cryptography, such as public-key infrastructure
CO3: Implement some advanced topics, like penetration testing
CO4: Examine the cyber security job market
CO5: Analyze intrusion detection systems with a case study
CO6: Implement fundamental cryptography in a real practice

Course Contents

UNIT-I	Introduction to Security Trends	07 Hours
The Computer Security Problem - Targets and Attacks - Approaches to Computer Security - Ethics - Basic Security Terminology - Security Models		
UNIT-II	**Operational and Organizational Security**	**07 Hours**
Policies, Procedures, Standards, and Guidelines - Security Awareness and Training - Interoperability Agreements - The Security Perimeter - Physical Security - Environmental Issues - Wireless - Electromagnetic Eavesdropping - People—A Security Problem - People as a Security Tool		
UNIT-III	**Cryptography**	**07 Hours**
Cryptography in Practice - Historical Perspectives - Algorithms - Hashing Functions - Symmetric Encryption - Asymmetric Encryption - Quantum Cryptography- Cryptography Algorithm Use		
UNIT-IV	**Authentication and Remote Access**	**07 Hours**

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

User, Group, and Role Management - Password Policies - Single Sign-On - Security Controls and Permissions - Preventing Data Loss or Theft - The Remote Access Process - Remote Access Methods		
UNIT-V	**Intrusion Detection Systems**	**07 Hours**
History of Intrusion Detection Systems - IDS Overview - Network-Based IDSs - Host-Based IDSs Intrusion Prevention Systems - Honeypots and Honeynets – Tools		
UNIT-VI	**Network Security**	**07 Hours**
Principles of Network Security, Network Security Terminologies, Network Security and Data Availability, Components of Network Security, Network Security Policies.		

Text Books:

T1. W.A.Coklin, G.White, Principles of Computer Security: Fourth Edition, McGrawHill, 2016

T2. William Stallings, Cryptography and Network Security Principles and Practices, Seventh Edition,Pearson

Reference Books:

R1. Achyut S. Godbole, Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing, Tata McGraw-Hill Education, 2013

R2. AtulKahate, ―Cryptography and Network Security‖, Tata McGraw-Hill, 2003

MOOC Platform:

https://www.springboard.com/resources/learning-paths/cybersecurity-foundations/

Dr. Ram Joshi BoS Chairman & Dean of Academics

Dr. Rakesh K. Jain Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

T. Y. B. Tech (Department of Information Technology)
Academic Year – 2021-2022 Semester -V
[ITH3102]: Machine Learning and Cyber Security

Teaching Scheme:	Credit	Examination Scheme:
TH: - 04 Hours/Week Lab:- 02 Hours/Week	TH:03 LAB:01	In Sem. Evaluation:15 Marks Mid Sem. Exam: 25 Marks End Sem. Exam : 60 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:

1. To study how machine learning can help in securing data.
2. To learn how machine learning has contributed to the success of filters
3. To understand quick way to detect anomalies
4. To conduct malware analysis by extracting used information from computer binaries
5. To examine how attackers exploit consumer-facing websites and app functionality
6. To translate your machine learning algorithms from the lab to production

Course Outcome:
After successful completion of the course, students will able to:
CO1: Learn different machine learning algorithms to secure information
CO2: Implement filtering methods using machine learning techniques
CO3: Analyze different methods of detecting anomalies.
CO4: Perform malware analysis using information
CO5: Visualize the attacks on consumer websites
CO6: Model machine learning based model to create a production system

Course Contents

UNIT-I	Convergence of Machine Learning and Cyber Security	06 Hours
Cyber Threat Landscape,The Cyber Attacker's Economy, Overview of Machine Learning, Real-World Uses of Machine Learning in Security, Spam Fighting: An Iterative Approach		
UNIT-II	**Anomaly Detection**	**07 Hours**
Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods, Feature Engineering for Anomaly Detection, Anomaly Detection with Data and Algorithms, Challenges of Using Machine Learning in Anomaly Detection		
UNIT-III	**Malware Analysis**	**07 Hours**

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

Understanding Malware, Feature Generation, From Features to Classification, Live malware analysis, dead malware analysis, Android Malware Analysis		
UNIT-IV	**Network Traffic Analysis**	**07 Hours**
Theory of Network Defense, Machine Learning and Network Security, Building a Predictive Model to Classify Network Attacks		
UNIT-V	**Protecting the Consumer Web**	**07 Hours**
Monetizing the Consumer Web, Types of Abuse and the Data That Can Stop Them, Supervised Learning for Abuse Problems, Clustering Abuse		
UNIT-VI	**Production Systems**	**07 Hours**
Defining Machine Learning System Maturity and Scalability, Data Quality, Model Quality, Performance, Maintainability, Monitoring and Alerting, Security and Reliability		

Lab Contents

Guidelines for Assessment

1) Continuous assessment shall be based on experiments performed, submission of results of practical assignments in the form of journal / reports, timely completion, attendance, understanding, performance.
2) Practical / Oral examination shall be based on the practical's performed in the lab.
3) Lab assessment marks shall be based on continuous assessment and performance in Practical/Oral examination.

List of Laboratory Assignments

1. Anomaly detection using supervised learning algorithm.
2. Study and implement intrusion detection system using SVM
3. Live malware analysis using unsupervised learning algorithm
4. Study and implement clustering abuse.

Text Books:

T1. Clarence Chio, David Freeman **"Machine Learning and Security",** O'Reilly Media, Inc.ISBN: 9781491979907
T2. SumeetDua, Xian Du. "Data Mining and Machine Learning in Cybersecurity", CRC Press, ISBN:978-1439839423

Reference Books:

R1. Learning Nessus for Penetration Testing, by Himanshu Kumar
R2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ed
R3. Mastering Modern Web Penetration Testing by Prakhar Prasad

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to SavitribaiPhule Pune University, Pune)

T. Y. B. Tech (Department of Information Technology)
Academic Year – 2021-2022 Semester -V
[ITH3103]: Machine Learning for Penetration Testing

Teaching Scheme:	Credit	Examination Scheme:
TH: - 4 Hours/Week LAB:-2 Hours/Week	TH:03 LAB:01	In Sem. Evaluation:15 Marks Mid Sem. Exam : 25 Marks End Sem. Exam : 60 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:

1. To understand basics of machine learning and the algorithms used to build robust systems.
2. To know how security products leverage machine learning
3. To identify machine learning development environments and Python libraries
4. To understand machine learning techniques for detection of phishing, botnet, etc.
5. To analyze best practices for Machine Learning and Feature Engineering

Course Outcome:
After successful completion of the course, students will able to:
CO1: Demonstrate the use of machine learning algorithms for penetration testing
CO2: Apply machine learning methods to detect phishing attacks
CO3: Apply machine learning methods for botnet detection
CO4: Identify the steps to detect advanced persistent threats
CO5: To implement machine learning based applications to detect Intrusion Detection Systems
CO6: To use best practices for machine learning to solve real examples

Course Contents

UNIT-I	Introduction to Machine Learning in Penetration Testing	07 Hours
Introduction, technical requirements, machine learning development environment and python libraries, ML in penetration testing- promises and challenges		
UNIT-II	**Phishing Domain Detection**	**07 Hours**
Introduction, social engineering overview, Steps of social engineering penetration testing, Building real-time phishing attack detectors using different machine learning models		
UNIT-III	**Botnet Detection with Machine Learning**	**07Hours**
Overview of Botnet, technical requirement, building a botnet detector model with multiple machine learning techniques, how to build a Twitter bot detector – a case study		

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

UNIT-IV	**Detecting Advanced Persistent Threats**	**07 Hours**
Introduction, threats and risk analysis, Threat-hunting methodology, Threat hunting with the ELK Stack		
UNIT-V	**Evading Intrusion Detection Systems**	**07 Hours**
Introduction, technical requirements, Adversarial machine learning algorithms, Evading intrusion detection systems with adversarial network systems		
UNIT-VI	**Best Practices for Machine Learning and Feature Engineering**	**07Hours**
Introduction, Feature engineering in machine learning, Feature selection algorithms, Best practices for machine learning		

Lab Contents

Guidelines for Lab Assessment

1) Continuous assessment shall be based on experiments performed, submission of results of practical assignments in the form of journal / reports, timely completion, attendance, understanding, performance.
2) Practical / Oral examination shall be based on the practical's performed in the lab.
3) Lab assessment marks shall be based on continuous assessment and performance in Practical/Oral examination.

1. Study and implement penetration testing using machine learning algorithm
2. Design and implement phishing attack using suitable ML algorithm
3. Study and implement Botnet detection using ML algorithm
4. Implement and compare accuracy of different ML algorithms for intrusion detection system.

Text Books:

1. Chiheb Chebbi, "Mastering Machine Learning for Penetration Testing", Packt, ISBN9781788997409
2. Learning Nessus for Penetration Testing, by Himanshu Kumar,
3. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition.
4. Mastering Modern Web Penetration Testing by Prakhar Prasad
5. Rtfm: Red Team Field Manual by Ben Clark

Reference Books:

R1. "Practical Malware Analysis" by Michael Sikorski and Andrew Honig
R2. "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition by Reverend Bill Blunden
R3. "Rootkits: Subverting the Windows Kernel" by Jamie Butler and Greg Hoglund
R4. "Practical Reverse Engineering" by Dang, Gazet, Bachaalany

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

T.Y.B. Tech (Department of Information Technology)
Academic Year – 2022-2023 Semester -VII
[ITH4101]: Usable Security

Teaching Scheme:	Credit	Examination Scheme:
TH: - 4Hours/Week	TH:4	In Sem. Evaluation:15 Marks Mid Sem. Exam : 25 Marks End Sem. Exam : 60 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:
To design and build secure systems with a human-centric focus with basic principles of human-computer interaction, and apply these insights to the design of secure systems with the goal of developing security measures that respect human performance and their goals within a system.

Course Outcome:
After successful completion of the course, students will able to:
CO1: Study fundamentals of Human-Computer Interaction: users, usability, tasks, and cognitive models
CO2: Design and build systems with a human-centric focus
CO3: Learn principles of usability and human-computer interactions
CO4: Define Security measures that respect human performance and their goals within a system
CO5: Implement authentication mechanisms, browsing security, mobile security and privacy and social media
CO6: Integrate usability into security software with hands-on exercises in designing, building, evaluating, and critiquing systems

Course Contents

UNIT-I	Fundamentals of Human	06 Hours
Computer Interaction: users, usability, tasks, and cognitive models, What is Human Computer Interaction?, Usability, Chunking Information, Mental Models, Privacy Policy		
UNIT-II	**Design**	**07 Hours**
Design methodology, prototyping, cybersecurity case study, Intro to Design, Design Methodologies, Case Study: SSL Warnings - example user		
UNIT-III	**Evaluation**	**07 Hours**
Usability studies, A/B testing, quantitative and qualitative evaluation, cybersecurity case study, Qualitative Evaluation, Running Controlled Experiments, Usability Studies,		
UNIT-IV	**Strategies for Secure Interaction Design**	**07 Hours**
Authority, guidelines for interface design, Intro to Usable Security Guidelines, Authority Guidelines, Authorization and Communication Guidelines, Interface Guidelines for Usable Security		

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

UNIT-V	Usable Authentication	07 Hours
Authentication mechanisms, biometrics, two-factor authentication, Usable Authentication and Passwords, Two-Factor Authentication, Biometric Authentication, Gesture-based Authentication, Case Study: Smudge Attacks		
UNIT-VI	**Usable Privacy**	**07 Hours**
Privacy settings, personal data sharing, data inference, Usable Privacy Basics, Privacy Policies and User Understanding, Informed Consent for Privacy, 5 Pitfalls of Privacy, Inferring Personal Data and Policy		
Text Books: T1. Simson Garfinkel (Author), Heather Richter Lipford (Author), "Usable Security: History, Themes, and Challenges (Synthesis Lectures on Information Security, Privacy, and Trust)", ISBN-13: 978-1627055291		
MOOC Platform: **https://www.coursera.org/learn/usable-security#about**		

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING
TATHAWADE, PUNE-33
(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

B. Tech (Department of Information Technology)
Academic Year – 2022-2023 Semester -VIII
[ITH4102]: Software Security

Teaching Scheme:	Credit	Examination Scheme:
TH: - 4Hours/Week	TH:4	In Sem. Evaluation:15 Marks Mid Sem. Exam : 25 Marks End Sem. Exam : 60 Marks

Course Prerequisites: Fundamentals of Cyber Security

Course Objective:
To explore the foundations of software security including important software vulnerabilities and attacks and important software vulnerabilities, including advanced testing and program analysis techniques.

Course Outcome:
After successful completion of the course, students will able to:
CO1: Study fundamentals of software security
CO2: Learn important software vulnerabilities and attacks
CO3: Understand software vulnerabilities
CO4: Design defenses that prevent or mitigate attacks
CO5: Implement techniques that can be used to strengthen the security of software systems at each phase of the development cycle
CO6: Test and verify that software is secure

Course Contents

UNIT-I	Security a software Issue	06 Hours
introduction, the problem, Software Assurance and Software Security, Threats to software security, Sources of software insecurity, Benefits of Detecting Software Security What Makes Software Secure: Properties of Secure Software, Influencing the security properties of software, Asserting and specifying the desired security properties?		
UNIT-II	**Requirements Engineering for secure software**	**07 Hours**
Introduction, the SQUARE process Model, Requirements elicitation and prioritization		
UNIT-III	**Secure Software Architecture and Design**	**07 Hours**
Introduction, software security practices for architecture and design: architectural risk analysis, software security knowledge for architecture and design: security principles, security guidelines and attack patterns Secure coding and Testing: Code analysis, Software Security testing, Security testing considerations throughput the SDLC		
UNIT-IV	**Security and Complexity**	**07 Hours**

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director

System Assembly Challenges: introduction, security failures, functional and attacker perspectives for security analysis, system complexity drivers and security		
UNIT-V	**Governance and Managing for More Secure Software**	**07 Hours**
Governance and security, Adopting an enterprise software security framework, How much security is enough?, Security and project management, Maturity of Practice		
UNIT-VI	**Case Studies of Software Security**	**07 Hours**
A case study in open source software security and privacy, Java Card Security Testing, A Case Study of Software Security Test Based on Defects Threat Tree Modeling		
Text Books: T1. Software Security Engineering: Julia H. Allen, Pearson Education		
Reference Books: R1. Developing Secure Software: Jason Grembi, Cengage Learning R2. Software Security : Richard Sinn, Cengage Learning		
MOOC Platform: **https://www.coursera.org/learn/software-security**		

Dr. Ram Joshi BoS
Chairman & Dean of Academics

Dr. Rakesh K. Jain
Director