MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO PARANÁ
SETOR PALOTINA

Departamento de Engenharias e Exatas

Ficha 2 (variável)

Disciplina: Segurança de Sistemas Computacionais						Código DEE345
Natureza: (X) Obrigatória ( ) Optativa	(X) Semestral ( ) Anual ( ) Modular					DEE
Pré-requisito:	Co-requisito:	Modalidade: ( ) Presencial (x) Totalmente EaD ( ) % EaD*				
CH Total: 30 **CH semanal: 2**	Padrão (PD): 30	Laboratório (LB): 0	Campo (CP): 0	Estágio (ES): 0	Orientada (OR): 0	Prática Específica (PE): 0

EMENTA (Unidade Didática)

Visão geral sobre auditoria de sistemas. Segurança de sistemas. Políticas de segurança. Privacidade na era digital. Análise de riscos em sistemas de informação. Aspectos especiais: vírus, criptografia, acesso não autorizado, ataques. Implementar mecanismos de garantia de segurança. *Firewall*, mecanismos de criptografia: simétrica e assimétrica, assinatura digital, certificados digitais. Plano de contingência organizacional. Metodologias de auditoria. Técnicas de avaliação de sistemas.

JUSTIFICATIVA PARA OFERTA PARCIALMENTE A DISTÂNCIA

PROGRAMA (itens de cada unidade didática)

1. Conceitos básicos: princípios e propriedades fundamentais para segurança computacional; ameaças, vulnerabilidades e ataques; base de computação confiável;
2. Introdução à criptografia: cifragem simétrica e assimétrica; hashes; assinaturas digitais; certificados; infraestruturas de chaves públicas;
3. Autenticação: local; em rede; distribuída;
4. Controle de acesso: políticas; modelos; mecanismos;
5. Segurança de sistemas e aplicações: ataques contra sistemas e mecanismos de defesa; segurança de sistemas; segurança em aplicações Web; desenvolvimento seguro;
6. Segurança em redes: filtragem de pacotes; firewalls; DMZ; ataques contra redes; protocolos de segurança;
7. Auditoria: logs; testes de invasão; detecção de intrusão; antivírus; análise de malware;
8. Gestão da segurança: normas e padrões; gerenciamento de vulnerabilidades; ética em segurança.

Aula 1 – Introdução e Conceitos Fundamentais
Apresenta o escopo da disciplina, definições de segurança (Security, Safety, Reliability), o modelo CIA (Confidencialidade, Integridade, Disponibilidade) e as “Seis Barreiras D” (Desencorajar, Dificultar, Discriminar, Detectar, Deter, Diagnosticar).

Aula 2 – Reconhecimento Passivo e Ativo (Footprint & Fingerprint)
Explora técnicas e ferramentas de OSINT (Google Dorks, Shodan, Censys, Wappalyzer, Maltego, theHarvester, SpiderFoot), coleta de metadados, consultas WHOIS/DNS (dig, nslookup) e fingerprinting de SO e serviços com Nmap e análise de TTL.

Aula 3 – Engenharia Social e Defesa de Credenciais
Estuda táticas de phishing (tática T1566 do MITRE ATT&CK), spearphishing, ataques de dicionário e força bruta a senhas (John the Ripper, THC-Hydra), políticas de hardening de senhas em Linux (chage, usermod) e introdução ao MFA/2FA e ferramentas de conscientização (Have I Been Pwned, How Secure Is My Password).

Aula 4 – Vazamento de Dados e Vulnerabilidades Web (OWASP Top 10)
Analisa causas e consequências de vazamentos (LGPD), casos reais, relação com SQL Injection e XSS. Introduz OWASP Top 10 e demonstrações práticas de testes em aplicações web.

Aula 5 – Reconhecimento e Defesa de Credenciais Aprimorados
Aprofunda técnicas OSINT (lanmap, extração de metadados de imagens), fingerprinting avançado com Nmap (-sS, -sU, -A), inferência de SO via TTL e práticas de captura de pacotes.

Aula 6 – Governança, Normas e Conformidade (ISO, NIST, PCI-DSS, ITIL, COBIT)
Cobre frameworks de segurança (ISO 27001/27002 com ciclo PDCA, NIST 800-series, CIS Controls, NIST CSF), planos de continuidade de negócios, inventário (OCS-NG) e papel de CSIRT (cert.br, RNP-CAIS).

Aula 7 – Criptografia I: Hash e Criptografia Simétrica
Introduz esteganografia (steghide), funções de hash (MD5, SHA-1/2/3, colisões) e ciphers simétricos (DES, AES, 3DES, Twofish, Blowfish) em modos ECB, CBC, CTR e GCM.

Aula 8 – Criptografia II: Assimétrica e Certificados Digitais
Explica RSA, ECC, Diffie-Hellman, princípios de Kerckhoffs e uso de certificados X.509. Prática de SSH com geração e distribuição de chaves (ssh-keygen, scp, ssh-copy-id).

Aula 9 – Hardening de Sistemas e Acesso Remoto
Demonstra endurecimento de Linux/Windows (SELinux, AppArmor, Bastille, OpenSCAP, Lynis), práticas SSH (porta não padrão, PermitRootLogin, Fail2Ban, Port Knocking), TMOUT para logout automático e ferramentas de auditoria de segurança.

Aula 10 – Autenticação, Autorização e AAA Avançado
Detalha o modelo AAA, credenciais UNIX (UID/EUID/SUID/GID, /etc/passwd, /etc/shadow), SSO (SAML, OAuth 2.0, OIDC, JWT), FIDO2/WebAuthn, biometria, ACLs, RBAC e práticas de sudoers e permissões em UNIX.

Aula 11 – Vulnerabilidades Web e Injeção de Código
Estudo prático de SQL Injection (sqlmap), XSS (refletido, armazenado, DOM), uso de VEGA, OWASP ZAP e scanners de WordPress, além de introdução a DevSecOps, SDL e CLASP.

Aula 12 – Ataques e Segurança de Redes
Ferramentas Netcat, hping3 (SYN Flood), T50, análise Wi-Fi com aircrack-ng, sniffing (tcpdump, Wireshark), MITM (Bettercap), firewalls (iptables, pfSense), proxies (Squid, SquidGuard, sarg, DansGuardian), VPN (OpenVPN), IPsec, DNSSEC, DMARC, NAT.

Aula 13 – Auditoria, Monitoramento e Detecção de Intrusões
Conceitos de auditoria, syslog, análise de logs (grep, tail), IDS/IPS (Snort, Suricata, Bro/Zeek), honeypots, EDR/XDR, SIEM, SOAR, scanners de vulnerabilidade (Nessus, Metasploit), verificadores de integridade (Tripwire, AIDE, OSSEC), rootkit scanners.

Aula 14 – Testes de Invasão, Hacking Ético e Quebra de Senhas
Metodologias (OSSTMM, OWASP Testing Guide, NIST SP 800-115), contratos/NDA, tipos de pentest (Double Blind, Gray Box), ferramentas John the Ripper, THC-Hydra, Ophcrack, Pydictor, criptoanálise, ataques de canal lateral e introdução a CTFs.

Aula 15 – Segurança Aplicada, Computação Forense e Novas Ameaças
Anonimização (anon-proxy, temp-mail), engenharia reversa (Ghidra, IDA, OllyDbg), sandboxing (Cuckoo, Firejail), recuperação de dados (Recuva, TestDisk, PhotoRec), APTs, MITM, deepfakes, zero-days,

DoS/DDoS, contêineres (Docker Bench, Clair, Falco, Kube-Bench), princípios forenses (NIST 800-86, OWASP Forensics), legislações (Marco Civil, LGPD, crimes cibernéticos).

OBJETIVO GERAL

O aluno deve ser capaz de pensar criticamente sobre os problemas de segurança a que um sistema ou rede estão suscetíveis e soluções possíveis para mitigá-los. Deve também ser capaz de buscar formas de identificar ameaças e vulnerabilidades, planejar a implementação de soluções para defesa e gerenciar o processo de manutenção de segurança.

OBJETIVO ESPECÍFICO

1. Entender o que é segurança computacional e os princípios fundamentais que norteiam a área;
2. Identificar ameaças, vulnerabilidades e ataques contra sistemas, redes e informação;
3. Aprender conceitos introdutórios sobre criptografia, mecanismos que a implementam e suas aplicações em segurança;
4. Compreender os mecanismos utilizados para prover autenticação e controle de acesso em sistemas e redes;
5. Estudar ataques clássicos e modernos de forma a entender como são feitos, que vulnerabilidades exploram e por que funcionam;
6. Conhecer o funcionamento dos mecanismos de defesa utilizados em sistemas e redes;
7. Instalar e configurar mecanismos de defesa tradicionais para analisar sua eficácia, eficiência e limitações;
8. Implementar ferramentas para varredura de vulnerabilidades, automatização de ataques e/ou detecção de ameaças;
9. Utilizar ferramentas (defensivas e ofensivas) para gerenciamento de vulnerabilidades em um sistema/rede: configuração, instalação, execução, atualização, monitoramento;
10. Conhecer as normas e padrões que regem a segurança da informação e estudar conceitos éticos sobre pesquisa, desenvolvimento e atuação na área.

PROCEDIMENTOS DIDÁTICOS

A disciplina será desenvolvida mediante aulas expositivas para apresentação dos conteúdos curriculares teóricos ou demonstrações feitas pelo professor, e através de atividades de laboratório nas quais as ferramentas e mecanismos serão implementados ou instalados, bem como avaliados na prática em ambiente controlado. Serão utilizados quadro branco, computador e projetor multimídia, computadores com sistema operacional GNU/Linux e ferramentas livres específicas para estudar cada conceito aplicável em laboratório

FORMAS DE AVALIAÇÃO

Parte Teórica:
N_{aval} = Form1 + Form2 + … Form15
Onde
$Form_1$ = Nota obtida na avaliação 1
$Form_2$ = Nota obtida na avaliação 2
N_{ava}l = Média das nota obtidas nas avaliações teóricas 1 e 2;

BIBLIOGRAFIA BÁSICA

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores**. Bookman, 2013.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Brasport, 2012.

TANENBAUM, Andrew S. **Redes de computadores.** São Paulo: Pearson, [2011]. xvi, 581 p., il., grafs., tabs. Inclui bibliografia e índice.

BIBLIOGRAFIA COMPLEMENTAR (3 títulos)

BARTIÉ, Alexandre. **Garantia da qualidade de software**. Gulf Professional Publishing, 2002.

REZENDE, Pedro Antonio Dourado. Criptografia e segurança na informática. **Apostila-Capítulos**, v. 1, n. 2, p. 3, 1998.

ESCOLA SUPERIOR DE REDES. Administração de Sistemas Linux: redes e segurança. 1.ed.

rev Rio de Janeiro: RNP/ESR, 2013. 228p.,

CASSARRO, Antonio Carlos. **Controles internos e segurança de sistemas: prevenindo fraudes e tornando auditáveis os sistemas.** São Paulo: LTr, 1997. 196 p.

KIM, David. **Fundamentos de segurança de sistemas de informação.** Rio de Janeiro: LTC, 2014. 386p

TRCEK, Denis. **Managing information systems security and privacy.** Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2006. Ebook. v.: digital. (Business and Economics (Springer-11643; ZDB-2-SBE).

Professor da Disciplina: Jéfer Benedett Dörr

Assinatura: _____

Chefe de Departamento: Prof.

Assinatura: _____

**OBS: ao assinalar a opção % EAD, indicar a carga horária que será à distância.*