

Obsah

Predhovor	6
1. Firewally.....	8
1.1. Základné pojmy	8
1.2. Typy firewallov	8
Paketový filter	9
Stavový firewall	10
Proxy server.....	11
Next generation firewall	13
1.3. Zapojenia firewallov.....	13
1.4. Príklad implementácia firewallu IPFire.....	15
1.5. Príklad implementácia firewallu OPNsense	21
1.6. Úlohy a otázky na zamyslenie:.....	28
2. Virtuálne privátne siete	29
2.1. Základné pojmy	29
2.2. Typy pripojenia	29
VPN model vzdialený klient	30
Peer-to-peer VPN	30
VPN brána na pobočke.....	30
2.3. Najbežnejšie technológie pre VPN.....	32
2.4. Príklad implementácia WireGuard v OPNsense	34
2.5. Úlohy a otázky na zamyslenie:.....	37
3. IDS	39
3.1. Formy IDS.....	39
3.2. Základné komponenty IDS.....	40
3.3. Formy detekcie.....	40
IPS	40
3.4. Spôsoby obchádzania systémov IDS.....	40
3.5. Implementácia a experiment.....	41
Predpríprava	42
Konfigurácia koncové systému “Útočník”	42
Konfigurácia koncové systému “WebServer”	42
Konfigurácia koncové systému „Suricata“.....	43
Sieťová konfigurácia koncových systémov.....	45
Sieťová konfigurácia koncového systému “Útočník”	46
Sieťová konfigurácia koncového systému “WebServer”	46
Sieťová konfigurácia koncového systému “Suricata”	46
Príprava útokov	47
Monitoring na IDS.....	48
Zhodnotenie.....	49
3.6. Pokročilé nástroje prevencie prieniku	49
3.7. Príklad implementácia IPS Suricata v pfSense.....	50
3.8. Úlohy a otázky na zamyslenie:.....	54
4. Manažment systémových záznamov a SIEM.....	55
4.1. Základné pojmy	55
4.2. Normalizácia záznamov	57
4.3. Graylog.....	58
4.4. Wazuh.....	65
4.5. Úlohy a otázky na zamyslenie:.....	67
5. DNS Over HTTPS.....	69
5.1. DNS.....	69
Autoritatívny DNS	69
Koreňový (root) Name Server	70
Rekurzívny DNS server.....	70

Komunikácia medzi DNS resolverom.....	70
DNS proxy.....	71
DNS Hijacking.....	72
5.2. DNS over HTTPS.....	72
Komunikácia pomocou DNS over HTTPS.....	72
Výhoda DoH oproti štandardnému DNS.....	74
DNS over HTTPS Proxy.....	74
5.3. DNS over TLS.....	74
Oblivious DNS-over-HTTPS.....	74
DNS over Quic.....	75
5.4. Praktická implementácia na Raspberry Pi.....	76
Inštalácia DNSCrypt-proxy a vypnutie existujúceho DNS resolveru.....	76
Konfigurácia DNSCrypt-proxy, aby používal DoH upstream.....	76
Konfigurácia soketu.....	76
Spustenie DNSCrypt-proxy.....	77
Zmena DNS serverov.....	77
Test funkčnosti.....	77
Ukážka rozdielu medzi DNS komunikáciou a DNS over HTTPS komunikáciou.....	77
5.5. Porovnanie implementovaného modelu a komerčného produktu.....	80
Zhodnotenie.....	81
5.6. Úlohy a otázky na zamyslenie:.....	81
6. Sieťový analyzátor.....	83
6.1. Najpoužívanejšie voľne dostupné sieťové analyzátory.....	84
6.2. Detegovanie sieťového analyzátora v sieti.....	84
6.3. Netflow.....	85
6.4. Hrubý zber sieťovej komunikácie zo sieťového rozhrania.....	86
Zachytávanie komunikácie zo špecifickej koncovej stanice a pre špecifickú koncovú stanicu....	87
Zachytávanie komunikácie špecifického protokolu a portu.....	87
Zhodnotenie.....	87
6.5. Simulácia útoku na Wi-Fi modul ESP8266.....	88
6.6. Úlohy a otázky na zamyslenie:.....	90
7. Honeypot.....	92
7.1. SSH Honeypot.....	93
Cowrie.....	93
Kippo-Graph.....	93
7.2. Implementácia na Raspberry Pi.....	94
Inštalácia Cowrie.....	94
Konfigurácia SSH honeypotu.....	95
Konfigurácia IPTables.....	95
Konfigurácia prostredie.....	96
7.3. Zhodnotenie.....	97
7.4. Úlohy a otázky na zamyslenie:.....	98
8. Útoky SQL Injection.....	99
8.1. Rôzne druhy injection útokov.....	99
8.2. SQL.....	101
Ukážka použitia SQL jazyka.....	102
8.3. Princíp SQL Injection.....	103
Príklad jednoduchého SQL Injection útoku.....	103
8.4. Metódy SQL Injection.....	104
8.5. Obrana proti injection útokom.....	106
8.6. Testovacie prostredie.....	107
8.7. Príklad útoku SQL injection.....	108
8.8. Úlohy a otázky na zamyslenie:.....	109
9. Moderné symetrické šifry.....	111
9.1. Princíp symetrického šifrovania.....	111

Prúdové vs. blokové šifry	112
9.2. Prúdové šifry	113
Vernamova šifra	113
Šifra A5	114
Šifra ChaCha20	114
9.3. Blokové šifry	114
Dizajn blokových šifier	114
AES (Rijndael)	116
Módy blokových šifier	116
9.4. Symetrické šifry používané v praxi	118
9.5. Úlohy a otázky na zamyslenie:	119
10. Kryptografické hašovacie funkcie	121
10.1. 1.1. Základné pojmy	121
Definícia a vlastnosti:	121
Ilustračný príklad	122
10.2. Známe a používané kryptografické hašovacie funkcie	123
Princíp fungovania	124
10.3. Narodeninový paradox	124
10.4. Použitie hašovacích funkcií	126
Hašovacie funkcie pre ukladanie hesiel	127
10.5. Praktické použitie hašovacej funkcie na kontrolný súčet softvéru	128
10.6. Úlohy a otázky na zamyslenie:	129
11. Asymetrické šifrovanie, digitálny podpis	131
11.1. Princíp asymetrického šifrovania	131
11.2. Digitálny podpis	132
11.3. Používané algoritmy	133
RSA	133
DSA	135
Diffie-Hellmanov protokol výmeny kľúčov	136
11.4. Výpočtová náročnosť, hybridné šifrovanie	138
11.5. Infraštruktúra verejného kľúča	138
11.6. Príklad – certifikát vydaný serveru	140
11.7. Úlohy a otázky na zamyslenie:	142