

Spis treści

Słowo wstępne	11
Wprowadzenie	13
Systemy operacyjne	17
Jaka jest różnica między konteneryzacją a wirtualizacją? Jakie są ich zalety oraz wady w kontekście bezpieczeństwa?	17
Jakie rodzaje baz danych można wskazać?	18
Kto może modyfikować plik z uprawnieniami 777?	19
Czym jest hardening i czego dotyczy?	19
Po co stosuje się dowiązanie symboliczne i czym ono jest?	20
Jaka jest różnica pomiędzy uwierzytelnianiem a autoryzacją?	20
Czym są Kerberos, AD oraz GPO?	20
Czym jest Crypto API?	21
Co znajduje się w plikach /etc/passwd i /etc/shadow?	21
Czym są zmienne środowiskowe?	23
Czy FTP jest bezpieczniejszy niż SSH?	24
Jak za pomocą komendy stworzyć nowy katalog na dysku?	24
Jak wyświetlić zawartość pliku za pomocą komendy?	25
Czym jest serializacja?	25
Jak stworzyć ukryty plik/katalog w systemie?	25
Czym różni się konto root od zwykłego konta użytkownika?	26
Jak wyświetlić listę plików w katalogu?	26
Do czego służy cron? W jakich lokalizacjach znajdują się poszczególne pliki?	27
Czym jest Docker?	27
Do czego wykorzystuje się protokół RDP?	27
Czy projekty open source są bezpieczniejsze od zamkniętych rozwiązań?	28
Jak wyświetlić listę uruchomionych procesów?	28
Do czego służą Wget i cURL?	28
Jaka jest różnica pomiędzy bind shell a reverse shell?	29
Jak można wykorzystać program grep?	29
Na jakiej stronie można sprawdzić, jak wyglądały strony w przeszłości?	30
Sieci	31
Czym jest ARP?	31
Jaka jest różnica pomiędzy routerem a switchem?	31
Jaka jest różnica między rozwiązaniami firewall a WAF?	32

Jaka jest różnica między adresem IP a adresem MAC?	32
Jaka jest różnica między publicznym a prywatnym adresem IP?	33
Jaka jest różnica pomiędzy portem zamkniętym a filtrowanym?	34
Jakie standardowe usługi znajdują się pod portami o numerach: 21, 22, 23, 25, 80, 88, 53,143, 443,1433, 1863,3306,3389?	34
Jaka jest różnica pomiędzy TCP a UDP?	35
Po co używa się VLAN-ów?	36
Po co używa się zapory sieciowej?	36
Czym jest ping? Czy warto go wyłączyć w organizacji i dlaczego?	36
Jakie warstwy ma model ISO/OSI?	37
Jakie warstwy ma model TCP/IP?	38
Jakim narzędziem można przechwycić pakiety?	38
Co można znaleźć za pomocą Certificate Transparency Log?	39
Co oznacza skrót LAN?	39
Gdzie kieruje adres 127.0.0.1?	39
Do czego używa się adresów 1.1.1.1 i 8.8.8.8?	39
Do czego służy maska podsieci?	40
Do czego służy DHCP?	40
Co to jest DNS i jak działa?	40
Czym jest TCP handshake?	41
Do czego służy komenda tracert/ traceroute?	41
Aplikacje webowe	43
Jaką przewagę nad ciasteczkami mają tokeny JWT?	43
Jaki nagłówek służy do przesyłania ciasteczek?	43
Jaka jest różnica między metodami POST i GET?	44
Jaka jest różnica pomiędzy HTTP a HTML?	44
Jakie znasz kody i klasy odpowiedzi HTTP?	44
Jakim znakiem rozdziela się parametry w żądaniu GET?	51
Czemu strony korzystają z nagłówka HSTS?	51
Jaka wartość znajduje się w nagłówku X-Forwarded-For?	51
Czego można się dowiedzieć o żądaniu na podstawie nagłówka Content-Length?	52
Do czego wykorzystuje się protokół WebSocket?	52
Przed czym chroni CSP?	52
Czym różni się HTTP/2 od HTTP/1.1?	53
Jakie znasz metody HTTP?	54
Co oznacza, że HTTP jest protokołem bezstanowym?	54
O czym informuje zawartość nagłówka User-Agent?	55
Jak wygląda przykładowy plik w formacie JSON?	55
Jak sprawdzić, czy parametr jest podatny na atak path traversal?	56
Na czym polega mechanizm Same-Origin Policy?	56
W jakim celu stosuje się mechanizm CAPTCHA?	56
Przed czym chroni mechanizm prepared statement?	57
Przed czym może chronić atrybut SameSite dodawany do ciasteczek?	57

Z jakich elementów składa się żądanie HTTP?	57
Czy powinno się ustawiać flagę HTTPOnly/Secure w ciasteczkach i dlaczego tak lub nie?	58
Dlaczego po zalogowaniu strony internetowe zwracają ciasteczko?	58
Kryptografia	59
Jakie informacje znajdują się w certyfikacie SSL?	59
MD5 czy SHA-256 — co jest lepsze i dlaczego?	59
Jakie znasz metody szyfrowania?	60
Kiedy mamy do czynienia z kolizją w kontekście kryptografii?	61
Kiedy stosuje się szyfr blokowy, a kiedy szyfr strumieniowy?	61
Jakiej minimalnej długości powinno być hasło użytkownika?	61
Jaka jest różnica pomiędzy haszowaniem a szyfrowaniem?	62
Po co stosujemy funkcje skrótu?	62
Co zapewnia kod HMAC?	62
Czy jest jakaś różnica pomiędzy SSL a TLS?	63
Jaka jest przewaga kryptografii krzywych eliptycznych nad RSA?	63
Do czego można użyć klucza publicznego?	63
Jak zdefiniować salting i do czego jest on używany?	64
Do czego służą sól i pieprz w kontekście haszowania haseł?	64
Co oznacza utajnianie z wyprzedzeniem?	64
Czym różni się zaufany certyfikat SSL od niezaufanego?	
Po co nam zaufane główne urzędy certyfikacji?	65
Cyberbezpieczeństwo	67
Jaka jest różnica pomiędzy podatnością 0-day a 1-day?	67
Czym jest botnet?	67
Jakie mogą być skutki ataku XSS?	67
Jakie znasz rodzaje wstrzyknięć?	68
Po co istnieją numery CVE i do czego służą?	70
Czym zajmują się red team, blue team i purple team?	70
Czym jest triada CIA i z czego się składa?	71
Jakie znasz rodzaje ataków typu sniffing i jak one przebiegają?	72
Na czym polega atak MITM?	72
Czym są SIEM, EDR i UEBA?	72
Czy podatność open redirection jest niebezpieczna?	73
Co jest przyczyną błędów typu buffer overflow?	73
Czy można przeprowadzać test penetracyjny bez pozwolenia?	74
Do czego służy hashcat?	74
Czy można namierzyć osobę, która korzysta z trybu prywatnego w przeglądarce?	75
Do czego używa się MITRE ATT&CK?	75
Czym jest modelowanie zagrożeń?	76
Do czego wykorzystuje się tęcze tablice?	76
Czym jest exploit?	77

Czym jest DAST?	77
Na czym polega zasada najmniejszego uprzywilejowania?	78
Jakie widzisz różnice pomiędzy DDoS a DoS?	78
Co oznacza pojęcie „insider threat“?	78
Jakie znasz metodyki prowadzenia testów penetracyjnych?	79
Czym charakteryzują się testy black box, grey box i white box?	80
Dlaczego każdy program bug bounty ma zakres?	
Do czego on służy?	80
Czym są honeypoty i honeynety? Do czego można je wykorzystać?	81
Gdzie można znaleźć informacje o gotowych exploitach?	81
Do czego wykorzystuje się narzędzie nmap?	81
Czym jest cyber kill chain?	82
Czym są podatności typu IDOR?	83
Czym jest steganografia?	84
Co powinien zawierać raport z pentestu?	84
Po co przeprowadza się skanowanie portów?	85
Czy można podszyć się pod nadawcę wiadomości SMS?	86
Na czym polega vishing?	86
Do czego można wykorzystać narzędzie Burp Suite?	86
Na czym polega credential stuffing?	86
Jak wygląda atak SIMSWAP?	87
Jakie znasz metody socjotechniki?	88
Na czym polega rekonesans i dlaczego jest ważny dla pentestera?	88
Po co firmowe laptopy są szyfrowane?	88
Na czym polega google hacking/google dorking?	89
Jakie popularne rodzaje cyberataków można wymienić?	89
Jak zapobiegać atakom typu brute force?	89
Czym różni się responsible disclosure od full disclosure?	90
Na czym polega atak clickjacking i jak się przed nim obronić?	90
Czym jest przechwytywanie sesji?	91
W jakim celu pentesterzy korzystają z serwerów proxy?	93
Czym jest Cyber Threat Intelligence (CTI)?	93
Na czym polega podatność SSRF?	93
W jaki sposób atak DoS na stronę firmową może zagrozić organizacji?	94
Czym jest OWASP Top 10?	94
Jakim narzędziem modyfikujesz ruch HTTP?	94
Czy CSS można wykorzystać do ataków?	95
Jakie projekty OWASP inne niż Top 10 można wymienić?	95
Do czego można wykorzystać portal Shodan?	96
Jak chronić się przed atakami phishingowymi?	96

Bibliografia

99