“Kibertəhlükəsizlik və sertifikatlı etikal haker” kursu üzrə tədris proqramı

S/s	Mövzuların adı
1	**Kibertəhlükəsizliyə giriş**
1.1	Kiber təhlükəsizlik haqqında ümumi anlayışlar
1.2	Eyniləşdirmə, doğrulama və avtorizasiya
1.3	Qanunlar və uyğunluqlar
1.4	Giriş nəzarəti
1.5	Kibertəhlükəsizlik üçün linux mühitinin qurulması və konfiqurasiyası
1.6	**Fundamental linux bilikləri**
1.7	Linux fayl sistemi və onun strukturu
1.8	Əsas Linux komandaları(pwd, cd, ls, touch, cat, mv …)
1.9	Fayllar üzərində əməliyyatlar
1.10	Əməliyyat sistemi, əlaqə növləri və servis kontrolu
1.11	Müxtəlif uzantılı arxiv fayllarının üzərində əməllər
1.12	SSH konfiqurasiyası
1.13	Fayl və qovluqlarda imtiyazların idarə olunması
1.14	Şəbəkə interfeysləri və onların konfiqurasiyası
1.15	İstifadəçi və qrup idarəetməsi
1.16	Sistem performans görüntüləmək
1.17	Proqram təminatının idarə olunması
1.18	İptables ilə linux fayrvol konfiqurasiyası
1.19	**Etik hakerliyin əsasları**
1.20	Etik hakerliyə ümumi baxış və metodologiya
1.21	**Şəbəkənin əsasları**
1.22	Kommunikasiya modelləri – OSİ modeli və TCP/İP arxitektuarsı
1.23	Şəbəkə topologiyaları (bus, star, ring, mesh, hybrid)
1.24	Fiziki şəbəkə
1.25	LAN, VAN və digər sahə şəbəkələrinin işləmə prinsipləri
1.26	İP adresləri (başlıqlar, ünvanlama, alt şəbəkələr)
1.27	TCP, UDP və İCMP protokolları
1.28	Şəbəkə arxitekturası (Şəbəkə növləri, izolyasiya, uzaqdan giriş) və bulud sistemləri
1.29	**Təhlükəsizliyin əsasları**
1.30	CIA (confidentiality, integrity, avalibility) üçlüyü və kibertəhlükəsizlikdə rolu
1.31	Kibertəhlükəsizlik riskləri (siyasətlər, standartlar və prosedurlar)
1.32	Təhlükəsizlik texnologiyaları (fayrvol, İDS, İPS, SİEM)
1.33	**Buraxılmış izlərin analizi və məlumatların toplanması**
1.34	OSİNT(açıq mənbə kəşfiyyatı)
1.35	DNS üzərindən məlumat toplama
1.36	Passiv məlumat toplama
1.37	**Şəbəkələrin skan edilməsi**
1.38	Ping sveeps(fping, MegaPing)
1.39	Portların skan edilməsi (nmap, masscan, MegaPing)
1.40	Zəifliyin skan edilməsi(OpenVAS, Nessus)
1.41	Paket saxtakarlığı və manipulyasiya(hping, packETH, fragroute)
1.42	Hücumlardan və saxtakarlıqlardan yayınma texnikaları

1.43	Sadalama (enumeration)
1.44	Server mesaj bloku (SMB), sadə şəbəkə idarəetmə protokolu (SNMP) və sadə mail transfer protokolu (SMTP)
1.45	Veb tətbiqi əsaslı sadalama (web based enumeration)
1.46	**Sistemlərin qırılmasının üsul və vasitələri**
1.47	İstismarlar (exploit) axtarılır
1.48	Sistem kompromisi (metasploit modulu, exploit-db)
1.49	Parolların toplanması və qırılması (John The Ripper, Göy qurşağı cədvəli)
1.50	Klient tərəfdə olan zəifliklər
1.51	İstismar sonrası (İmtiyazların artırılması, sistem daxilində sıçrama, davamlılıq, izlərin örtülməsi)
1.52	Metasploitable2 maşınına öyrənilən praktiki metodlarla sızılma
1.53	**Zərərli proqram (Malvare)**
1.54	Zərərli proqramın tipləri (virus, vorm, trojan, botnet, ransomvare, dropper)
1.55	Zərərli proqram analizi (statik analiz, dinamik analiz)
1.56	Zərərli proqramın yaradılması (özümüz yarada bilərik vəya metasploit alətini istifadə edə bilərik)
1.57	Zərərli proqram infrastrukturu və antivirus həlləri
1.58	**Şəbəkənin iylənilməsi (sniffing)**
1.59	Paketlərin ələ keçirilməsi (tcpdump, tshark, wireshark, berkeley packet filter, port mirroring/spanning
1.60	Paket analizi
1.61	Spoofing hücumları (ARP spoofing, DNS spoofing, sslstrip)
1.62	**Sosial Mühəndislik**
1.63	Pretexting, sosial mühəndislik vektorları, fiziki sosial mühəndislik(badge access, man traps, biometrics, phone calls, baiting)
1.64	Fişinq və veb sayt hücumları (klonlama, qeyri-qanuni hücumlar)
1.65	Simsiz şəbəkələrdə sosial mühəndislik və sosial mühəndisliyin avtomatlaşdırılması
1.66	Simsiz şəbəkələrin təhlükəsizliyi (simsiz şəbəkə tipləri, autentifikasiya, şifrələmə, BYOD, simsiz şəbəkə hücumları və istifadə olunan alətlər
1.67	Simsiz qulaqcıq (bluetooth) təhlükəsizliyi (zəifliyin skan edilməsi, bluejacking, bluesnarfing, bluebugging)
1.68	Mobil cihazlar (mobil cihazlara edilən hücumlar)
1.69	**Hücum və müdafiə**
1.70	Veb tətbiqinə edilən hücumlar (XML External Entity Processing, XSS, SQL injection, Command injection)
1.71	Xidmətdən imtina hücumu (bant genişliyi hücumu, yavaş hücumlar, miras)
1.72	Tətbiqlərin istismarı (Buffer Overflow, Heap spraying)
1.73	Yanal hərəkət (lateral movement)
1.74	Dərinlikdə müdafiə və genişlikdə müdafiə
1.75	Müdafiə edilə bilən şəbəkə arxitekturası
1.76	bVAPP veb tətbiqi ilə müxtəlif zəifliklərin aşkarlanması və onların istismar edilməsi
1.77	**Kriptoqrafiya**
1.78	Sadə şifrələmə (əvəzetmə şifrələri, Diffie-Hellman)
1.79	Simmetrik açar kriptoqrafiyası (DES, AES)

1.80	Asimmetrik açar kriptoqrafiyası (Hybrid cryptosystem, Non-Repudation, Elliptic Curve Cryptography)
1.81	Sertifikat təşkilatları və açaridarəetmə (sertifikat təşkilatı, etibarlı üçüncü tərəf, özünü imzalayan sertifikatlar)
1.82	Kriptoqrafik haşinq
1.83	**Təhlükəsizlik arxitekturası və dizaynı**
1.84	Məlumatların təsnifatı və təhlükəsizlik modelləri (state machine, Biba, Bell-LaPadula, Clark_Wilson Integrity Model)
1.85	Tətbiqlərin arxitekturası (n-tier application design, service-oriented architecture, cloud-based applications, database considerations)