**1Kibertəhlükəsizlik anlayışı** “Kibertəhlükəsizlik” anlayışının vahid tərifi yoxdur (Bu kursda “kibertəhlükəsizlik” və “informasiya təhlükəsizliyi” ekvivalent anlayışlar kimi işlənəcək). Bəzən “kibertəhlükəsizlik” anlayışına ”informasiyanın konfidensiallığının, tamlığının və əlyetənliyinin təmin olunduğu vəziyyət” kimi tərif verilir (Bu tərif “informasiyanın təhlükəsizliyi” məsələsini əks etdirir). “Kibertəhlükəsizlik” anlayışı həmişə müəyyən şəraitdə (mühitdə) olan (fəaliyyət göstərən) konkret subyekt ilə bağlı olur (məsələn, hər hansı sistemin və ya təşkilatın kibertəhlükəsizliyi). Ümumiyyətlə, təhlükəsizlik subyektin müəyyən vəziyyətidir və onu müvafiq keyfiyyət xarakteristikalarını göstərməklə müəyyən etmək olar. Təhlükəsizlik haqqında danışarkən subyektin mövcudluğunun müəyyən məqsəd funksiyası (maraqları) nəzərdə tutulur və təhlükəsizlik subyektin bu funksiyanı reallaşdırmaq qabiliyyəti kimi başa düşülür. Buradan çıxış edərək, bu mühazirədə “kibertəhlükəsizlik” anlayışına belə tərif verilir: “Kibertəhlükəsizlik informasiya qarşılıqlı münasibətlərində iştirak edən tərəflərin informasiya maraqlarının təmin edildiyi vəziyyətdir.” Hər bir sosial subyekt “kibertəhlükəsizlik” anlayışına öz maraqlarına cavab verən məna verir. Dövlətin kibertəhlükəsizliyi sosiumun elə vəziyyətidir ki, bu zaman şəxslər, cəmiyyət və dövlət təbii və süni meydana çıxan, ictimai və fərdi şüurun qəsdən deformasiya olunmasına, şəxsiyyətin, cəmiyyətin və dövlətin mövcudluğu üçün vacib əhəmiyyəti olan informasiya infrastrukturunun məhv edilməsinə yönəlmiş təhdidlərdən etibarlı şəkildə qorunur. Cəmiyyətin kibertəhlükəsizliyi dedikdə, cəmiyyətin informasiya mühitinin vətəndaşların, təşkilatların və dövlətin maraqları naminə formalaşmasını və inkişafını təmin edən vəziyyəti başa düşülür. Şəxsin kibertəhlükəsizliyi anlayışının məzmununa onun informasiya almaq hüququnun təmin edilməsi, fərdi məlumatlarının etibarlı qorunması və müxtəlif mənbələrdən aldığı informasiyanın onun şəxsiyyətinin azad formalaşmasına və inkişafına mane olmaması məsələləri daxildir. Təşkilat səviyyəsində kibertəhlükəsizlik informasiyanın icazəsiz girişlərdən qorunması, əlyetənliyinin və tamlığının təmin edilməsi məsələlərini əhatə edir. İnformasiyanın mühafizəsi – kibertəhlükəsizliyin təmin edilməsinə yönəlmiş tədbirlər kompleksidir.

**Kibertəhlükəsizliyə əsas təhdidlər** Təhdid dedikdə (geniş mənada) – kiminsə maraqlarına ziyan vura bilən potensial mümkün hal, hadisə, hərəkət (və ya hərəkətsizlik), şərait, proses və s. nəzərdə tutulur. Təhdidi reallaşdırmaq cəhdi hücum (kiberhücum), belə cəhdlərə baş vuran şəxslər isə bədniyyətli adlandırılır. Təhdidi iki parametrlə xarakterizə edirlər – təhdidin baş verməsi ehtimalı və təhdid baş verdikdə vurulan ziyan.

Adətən, təhdidlər informasiya sisteminin layihələndirilməsi, yaradılması və ya istismarı zamanı buraxılan boşluqlar (səhvlər) nəticəsində meydana çıxır (məsələn, proqram təminatında səhvlər). Kibertəhlükəsizliyə təhdidlərin sayı olduqca çoxdur və onları müxtəlif siniflərə ayırırlar. Meydana çıxma səbəblərinə görə təhdidləri təbii və süni xarakterli təhdidlərə bölürlər. Süni xarakterli təhdidlər də öz növbəsində bilməyərəkdən və qəsdən törədilən təhdidlərə bölünür. Təbii xarakterli təhdidlərə misal olaraq təbii fəlakətləri və qəzaları (yanğın, daşqın, zəlzələ və s.) və avadanlıqda baş verən imtina və qəzaları göstərmək olar. Süni xarakterli təhdidlərin aşağıdakı növlərini göstərmək olar: ο proqram təminatı yaradılarkən buraxılan səhvlər; ο proqram təminatının istismarı zamanı istifadəçilərin səhvləri; ο bədniyyətlilərin qəsdli əməlləri. Qəsdən törədilən təhdidlər təhdid mənbəyinin sistemə nəzərən yerləşməsinə görə xarici və daxili (ingilis dilində insider – insayder) təhdidlərə bölünür. Bəzi müəlliflərə görə, təhdidlərin böyük əksəriyyəti (80 %-i) sistemin öz daxilindəki mənbələrdən qaynaqlanır. Təhdidlər digər əlamətlərinə görə də təsnif oluna bilər: − Baş vermə ehtimalına görə (böyük ehtimallı, ehtimallı, az ehtimallı); − Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər); − Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi); − Təsir xarakterinə görə (aktiv, passiv); − Obyektə münasibətinə görə (daxili, xarici); Təsir məqsədlərinə görə təhdidlərin üç əsas növü ayırd edilir: − İnformasiyanın konfidensiallığının pozulmasına yönələn təhdidlər; − İnformasiyanın tamlığının pozulmasına yönələn təhdidlər; − Əlyetənliyin pozulmasına yönələn təhdidlər (DoS hücumlar (Denial of Service) – xidmətdən imtina hücumları).

**2) KONFIDENSIAL INFORMASIYANIN TESNIFATI**

Konfidensial informasiya İnformasiyanı konfidensiallıq əlamətinə görə aşağıdakı kimi təsnif etmək olar: – açıq informasiya; – konfidensial informasiya. Açıq informasiya – əldə olunması, işlənməsi, verilməsi və ya istifadəsi Azərbaycan Respublikasının qanunvericiliyi ilə məhdudlaşdırılmayan və ümumi istifadə üçün nəzərdə tutulmuş informasiyadır. Açıq informasiya üçün tamlığın və əlyetənliyin təmin edilməsi vacibdir. Açıq informasiyaya aiddir: − kənara verilmək üçün rəhbərlik tərəfindən imzalanmış informasiya, (məsələn, konfranslar, təqdimatlar və s. üçün); − açıq xarici mənbələrdən alınmış informasiya; − təşkilatın açıq veb-saytında yerləşdirilən informasiya. Sənədləşdirilmiş informasiya (sənəd) − maddi daşıyıcıda qeyd olunmuş və identikləşdirilməsinə imkan verən rekvizitlərə malik informasiya; Konfidensial informasiya − əldə olunması, işlənməsi, verilməsi və ya istifadəsi Azərbaycan Respublikasının qanunvericiliyinə müvafiq olaraq məhdudlaşdırılan sənədləşdirilmiş informasiya; Konfidensial informasiyanın dövlət sirri, hərbi sirr, kommersiya sirri, xidməti sirr (dövlət təşkilatları üçün), peşə sirləri (bank, istintaq, müalicə, rabitə, ...), fərdi məlumatlar, şəxsi sirr və s. kimi siniflərini göstərmək olar. Konfidensial informasiyasının mühafizəsi üçün konfidensiallığın, tamlığın və əlyetənliyin təmin edilməsi zəruridir. Fərdi məlumatlar – vətəndaşın şəxsi həyatının faktları, hadisələri və şəraitləri haqqında onun şəxsiyyətini identikləşdirməyə imkan verən məlumatlardır. Təşkilat əməkdaşlarının fərdi məlumatları adətən kadrlar şöbəsində saxlanır. Bu halda qanunvericiliyə uyğun olaraq təşkilat vətəndaşlar qarşısında bu informasiyanın qorunması, emalı rejiminin və istifadə qaydasının pozulmasına görə məsuliyyət daşıyır. Kommersiya sirri – dövlət sirri olmayan, istehsalat, texniki, texnoloji informasiya ilə, müəssisənin maliyyə və digər fəaliyyətinin idarə edilməsi ilə əlaqədar olan informasiya, açılması (verilməsi, sızması) onun maraqlarına ziyan vura bilən. Peşə sirri – peşə fəaliyyəti ilə əlaqədar olan və girişi Konstitusiyaya və qanunlara uyğun olaraq məhdudlaşdırılan məlumatlar.

Dövlət sirri – dövlətin hərbi, xarici-siyasi, iqtisadi, kəşfiyyat, əks-kəşfiyyat və əməliyyat-axtarış fəaliyyəti ilə bağlı olub, dövlət tərəfindən mühafizə edilən və yayılması Azərbaycan Respublikasının təhlükəsizliyinə ziyan vura bilən məlumatlardır; Məlumatların dövlət sirrinə aid edilməsi və onların məxfiləşdirilməsi prinsipləri:. • Qanunilik – dövlət sirrinə aid edilən və məxfiləşdirilən məlumatların Azərbaycan Respublikasının dövlət sirri haqqında qanunvericiliyinə müvafiqliyidir. • Əsaslılıq – dövlətin, cəmiyyətin və vətəndaşların həyati maraqlarının balansı nəzərə alınmaqla, konkret məlumatın dövlət sirrinə aid edilməsinin və məxfiləşdirilməsinin mümkün iqtisadi, siyasi, hərbi və digər nəticələrinin ekspertlər tərəfindən qiymətləndirilməsi yolu ilə məqsədəuyğunluğunun müəyyənləşdirilməsidir. • Məlumatların vaxtında dövlət sirrinə aid edilməsi və onların məxfiləşdirilməsi - bu məlumatların yayılmasına və onların daşıyıcıları ilə tanış olmağa buraxılmağa qabaqcadan və ya onların əldə edildiyi (hazırlandığı) andan məhdudiyyət qoyulmasıdır. Aşağıdakı məlumatlar dövlət sirrinə aid edilmir və məxfiləşdirilmir: – insanların həyat və sağlamlığı üçün təhlükə törədən fövqəladə hadisələr və qəzalar, onların nəticələri, habelə təbii fəlakətlər, onların rəsmi proqnozları və nəticələri haqqında; – ekologiya, səhiyyə, sanitariya, demoqrafiya, təhsil, mədəniyyət və kənd təsərrüfatının, habelə cinayətkarlığın vəziyyəti haqqında; – dövlətin vətəndaşlara, vəzifəli şəxslərə, müəssisə, idarə və təşkilatlara verdiyi imtiyazlar, güzəştlər və kompensasiyalar haqqında; – insan və vətəndaş hüquqlarının və azadlıqlarının pozulması faktları haqqında; – Azərbaycan Respublikasının ali vəzifəli şəxslərinin səhhəti haqqında; – dövlət hakimiyyəti orqanları və onların vəzifəli şəxsləri tərəfindən qanunvericiliyin pozulması faktları haqqında. Dövlət sirri təşkil edən məlumatların üç məxfilik dərəcəsi və müvafiq olaraq, bu məlumatların daşıyıcıları üçün üç məxfilik qrifi müəyyənləşdirilir: "xüsusi əhəmiyyətli", "tam məxfi" və "məxfi". Dövlət sirri təşkil edən məlumatların məxfilik müddəti 30 ildən artıq olmamalıdır. Bu müddət müvafiq icra hakimiyyəti orqanının rəyi ilə uzadıla bilər.

3) ***Kibertəhlükəsizliyin təmin edilməsi metodları*** Kibertəhlükəsizliyin təmin olunmasına kompleks yanaşma tələb edilir. Onun həlli üçün tədbirləri aşağıdakı səviyyələrə bölmək olar: ♦ Qanunvericilik tədbirləri (informasiya ilə davranış qaydalarını müəyyən edən və bu qaydaların pozulmasına görə məsuliyyəti müəyyənləşdirən qanunlar, fərmanlar, standartlar və s.)

♦ İnformasiya təhlükəsizliyi siyasəti. İnformasiya təhlükəsizliyi rəhbərlik tərəfindən müvafiq kibertəhlükəsizlik siyasətinin həyata keçirilməsi ilə əldə edilir. Kibertəhlükəsizlik siyasəti dövlətin, idarənin, təşkilatın ali idarəetmə orqanları tərəfindən rəsmi rəhbər sənəd kimi işlənir və təsdiq edilir. Sənəddə kibertəhlükəsizlik siyasətinin məqsədləri və kompüter sistemlərində (KS-də) kibertəhlükəsizlik məsələlərinin həllinin əsas istiqamətləri göstərilir. Kibertəhlükəsizlik siyasətində KS-də kibertəhlükəsizlik sisteminin qurulmasının ümumi tələbləri və prinsipləri də verilir.

♦ Təşkilati tədbirlər − təhlükəsizlik təhdidlərinin reallaşmasını maksimum çətinləşdirmək və ya istisna etmək məqsədilə KS-in fəaliyyət prosesini və istifadəçilərin hərəkətlərini reqlamentləşdirir: a) istifadəçilərin işinə aşkar və ya gizli nəzarətin təşkili; b) sənədlərin və informasiya daşıyıcılarının saxlanmasının, istifadəsinin və məhv edilməsinin uçotunun təşkili; v) mühafizənin (ərazi) və etibarlı buraxılış rejiminin təşkili; q) kadrların seçilməsi və hazırlanması zamanı həyata keçirilən tədbirlər; d) informasiyaya giriş qaydalarının işlənməsi üzrə tədbirlər; e) sistemin texniki vasitələrinin layihələndirilməsi, işlənməsi, modifikasiyası zamanı tədbirlər.

♦ Mənəvi etik tədbirlər.

♦ Fiziki təhlükəsizlik tədbirləri: sistemə nüfuzetmə yollarında fiziki maneələrin yaradılması üçün müxtəlif növ texniki mühafizə vasitələrinin tətbiqi.

♦ Proqram-texniki tədbirlər – müəyyən təhlükəsizlik funksiyalarını yerinə yetirən texniki qurğuların və proqramların istifadəsinə əsaslanır. Onlara təhlükəsizlik servsləri deyilir. Adətən, aşağıdakı təhlükəsizlik servisləri nəzərdə tutulur: ‒ identifikasiya və autentifikasiya; ‒ girişin idarə olunması (avtorizasiya); ‒ protokollaşdırma və audit; ‒ şifrləmə; ‒ rəqəmsal imza; ‒ tamlığa nəzarət; ‒ ekranlaşdırma; ‒ virtual xüsusi şəbəkələr; ‒ imtinalara dayanıqlığın təmin edilməsi; ‒ təhlükəsiz bərpanın təmin edilməsi; ‒ kibertəhlükəsizliyin idarə edilməsi.

**4)5)*“Cyber kill chain” modeli***Kiber-hücumların mərhələlərini təsvir etmək üçün Lockheed Martin şirkəti tərəfindən “Cyber kill chain” ─ “Kiber ölüm zənciri” modeli təklif edilmişdir. Kiber ölüm zəncirində olan 7 mərhələ aşağıdakılardır: 1. Kəşfiyyat (Reconnaissance). Araşdırma, identifikasiya və hücum üçün hədəf sistemin seçilməsi. 2. Silahın qablaşdırılması (Weaponization). Hücum üçün alətlərlə və zərərli proqramlarla təchizat 3. Çatdırma (Delivery). Zərərli kontentin hədəf sistemə çatdırılması (məs., e-poçt, veb-sayt və ya USB daşıyıcılar vasitəsilə) 4. Yoluxdurma (Exploitation). Zərərli kodun işə salınması və ya sistemdəki boşluğun istismarı 5. Quraşdırma (Installation). Zərərli proqram təminatı bədniyyətliyə əlyetər olan giriş nöqtəsi (məs., "backdoor") quraşdırır. 6. İdarəetmənin ələ alınması (Command and Control). Yoluxdurulmuş sistemin idarə edilməsi. 7. Əməliyyatların yerinə yetirilməsi (Actions on Objective). Hücum edən öz məqsədlərini reallaşdırmaq üçün hərəkətə keçir: verilənlərin toplanması, oğurlanması, göndərilməsi, faylların şifrlənməsi, verilənlərin dəyişdirilməsi, silinməsi və s.

***6)*** ***Etik hakinq anlayışı***. Kibertəhlükəsizlikdə “hakinq” termini sistemdəki boşluqları istismar etmə və sistem resursları üzərində nəzarəti (idarəetməni) ələ keçirmə prosesini bildirir. Etik hakinq təşkilatda informasiya təhlükəsizliyinin səviyyəsini qiymətləndirməyin ən etibarlı yollarından biridir. Etik hakinq ona görə etik hesab edilir ki, yalnız sistemin sahibinin xahişi ilə yerinə yetirilir və arzuolunmaz müdaxilələrin qarşısını almaq məqsədi güdür. Etik hakinq boşluqları və nöqsanları aşkarlamaqla və aradan qaldırmaqla, səhvləri düzəltməklə təşkilatlara kibertəhlükəsizlik səviyyəsini yüksəltməyə imkan verir. Kibertəhlükəsizlikdə ağ şlyapalı hakerlərin xidmətindən 1990-cı illərdən istifadə edilir (məsələn, red teams). Etik hakinq risklərin qiymətləndirilməsi, kibertəhlükəsizliyin auditi, kiberhücumlarla mübarizədə əsas və vacib komponentdir. Etik hakinq hücumlar əleyhinə dərhal tədbir görmək üçün boşluqların, risklərin müəyyən edilməsində sızma testi kimi geniş istifadə olunur. Təşkilat sızma testini həyata keçirən şəxsi işə cəlb edərkən son dərəcə ehtiyatlı olmalıdır, çünki həmin şəxs(lər) bədniyyətli ola bilər. Etik haker profili (texniki): Etik haker geniş istifadə olunan Windows, Linux, Unix, Macintosh kimi demək olar ki, bütün əməliyyat sistemləri haqqında geniş və dərin məlumatlı olur; Şəbəkə, texnologiyalar, aparat və proqram təminatı imkanlarını tədqiq edə bilir. Etik hakerin qeyri-texniki profilinə öyrənmə qabiliyyəti, problem həlletmə bacarıqları və kommunikasiya bacarıqları daxildir.

**Etik hakinqin tədrisi ilə bağlı problemlər.** Etik hakerliyin öyrədilməsi ilə bağlı bir sıra etik və hüquqi məsələlər mövcuddur. Bəzi tələbələrin öyrəndikləri hücum metodlarını və alətlərini məsuliyyətsiz şəkildə tətbiq edəcəkləri ehtimalı var. Etik hakinq üsullarının öyrədilməsinə görə təşkilatların və pedaqoqların məsuliyyətini azaltmaq üçün bir sıra addımlar atılmalıdır. Etik hakinq üsullarıını öyrədən hər bir kursda hüquqi nəticələr və etika məsələləri müzakirə edilməlidir. Tələbələr başa düşməlidirlər ki, hücum metodlarının öyrədilməsinin məqsədi kiber hücumların necə işlədiyini başa düşməklə müdafiə metodlarını təkmilləşdirmək və müvafiq təhlükəsizlik həllərini tətbiq etməkdir. Etik hakinq kursunu öyrənmək istəyən tələbələr davranış kodeksini imzalamalıdırlar. Davranış kodeksində tələbənin davranış sərhədləri göstərilir və qəbuledilməz hərəkətlərin hüquqi nəticələri şərh olunur.

7***) Kali Linux Kali Linux*** Kali Linux – Linux nüvəsində əməliyyat sistemidir (distributivdir). Onun əsası kimi Debian distributivi çıxış edir. Kali Linux 2013-cü ildə xüsusi olaraq, sızma testləri və rəqəmsal kriminalistika üçün yaradılmışdı. Kali Linux kibertəhlükəsizlik tədrisi sahəsində lider təşkilatlardan olan Offensive Security şirkəti tərəfindən işlənir, maliyyələşdirilir və dəstəklənir.

Kali Linuxda 600-dən artıq alət vardır, onlar kibertəhlükəsizliyin sızma testləri, təhlükəsizliyin tədqiqi, kompüter kriminilastikası və tərs mühəndislik kimi müxtəlif məsələlərinə yönəlib. Kali Linux menyüsünə aşağıdakı bloklar daxildir:

1. Information Gathering İnformasiyanın toplanması
2. Vulnerability Analysis Boşluqların analizi
3. Web Application Analysis Veb tətbiqlərin analizi
4. Database Assessment Verilənlər bazalarının qiymətləndirilməsi
5. Password Attacks Parol hücumları
6. Wireless Attacks Naqilsiz şəbəkələrə hücumlar
7. Reverse Engineering Tərs mühəndislik
8. Exploitation Tools Eksployt alətləri
9. Sniffing & Spoofing Sniffinq və spufinq
10. Post Exploitation Eksployt sonrası
11. Forencics Kriminalistika alətləri
12. Reporting Tools Hesabat alətləri
13. Social Engineering Tools Sosial mühəndislik alətləri
14. System Services Sistem servisləri

***8) Sosial mühəndislik üsulları***

İnsanlarda belə rəy formalaşıb ki, kibercinayətkarlar kompüter sistemlərinin sındırılması üçün yalnız mürəkkəb haker alətlərindən və texnologiyalarından istifadə edirlər. Bu heç də belə deyil. Kibercinayətkarlar çoxdan başa düşüblər ki, informasiyanı oğurlamaq və ya informasiya sisteminə hüçum etmək üçün ən asan üsul insan faktorunun zəifliklərindən istifadə etməkdir. Bir çox tədqiqatçıya görə, sosial mühəndislik adlanan bü üsullar XXI əsr hakerlərinin əsas alətlərindən biridir. Sosial mühəndislik (ing. social engineering) – tətbiqi sosiologiyanın insanın davranışını müəyyən edən və ona nəzarəti təmin edən təşkilati strukturların məqsədyönlü dəyişdirilməsinə yönəlmiş yanaşmalar məcmusudur. İnformasiya texnologiyaları sahəsində sosial mühəndisliyi çox vaxt informasiyaya icazəsiz giriş əldə etməyə yönəlmiş tədbirlər kimi qəbul edirlər. Sosial mühəndislik psixologiyanın və sosiologiyanın qanunlarına əsaslanır, digər insanları manipulyasiya etmək bacarığı ilə həyata keçirilir. Öz növbəsində, manipulyasiya insanın elementar zəifliklərinə əsaslanır: maraq, lovğalıq, şöhrətpərəstlik, qorxu, mərhəmət, qulluq göstərmə və s. Sistemli yanaşma baxımından sosial mühəndislik ondan çıxış edir ki, orta statistik istifadəçi müəyyən ortabab xarakteristikalara malik olur. Sosial mühəndislik insana sistemin bir hissəsi kimi baxır, insan həmin sistem haqqında fundamental biliklərə malik olmur. Əks halda, sosial mühəndislik işləmir – insan onu əhatə edən mühit haqqında nə qədər çox məlumatlıdırsa, sosial mühəndislik üsullarının işləməsi ehtimalı bir o qədər azdır. Sosial mühəndislik hücumu informasiyanın toplanması, senarinin qurulması və hücumun həyata keçirilməsi mərhələlərindən ibarətdir. İnformasiyanın toplanması mərhələsində fərdin profili (ünsiyyət dairəsi, maraqları, hobbisi, sosial şəbəkələrdə yazışmaları və s.) və ya təşkilatın profili (fəaliyyət dairəsi, tərəfdaşları, veb-saytdakı məlumatlar, əməkdaşlarının siyahısı, e-poçt ünvanları, telefonlar və s.) yaradılır. Senari ideyalarına sosial şəbəkələrdə dostluq münasibətləri yaratmaq, epoçtla məktub göndərmək, telefonla zəng etmək və s. daxildir. Əks-sosial mühəndislik (ing. reverse social engineering) – məqsəd hücum hədəfini “kömək” üçün bədniyyətlinin özünə müraciət etməyə məcbur etməkdir. Bunun üçün bədniyyətli, məsələn, reklamdan: “əgər kompüterinizdə nasazlıq olarsa, bu nömrəyə zəng edin” tipli elandan istifadə edə bilər.

***9) İnformasiya toplanmasının metodologiyası.*** İntenretdən, sosial mediadan, rəsmi veb-saytlardan və digər mənbələrdən lazım olan məlumatların toplanması böyük problem deyil. Aşağıda hakerlər tərəfindən tez-tez istifadə olunan informasiya mənbələri verilmişdir:

* Axtarış sistemlərinin istifadəsi
* Google geniş (ing. advanced) axtarış üsulları
* Google Hacking Database (GHDB)
* Sosial şəbəkələrdən informasiyanın toplanması
* Veb-saytlardan informasiyanın toplanması
* Poçt sistemlərindən informasiyanın toplanması
* Rəqabət kəşfiyyatı
* DNS verilənlərinin toplanması
* Şəbəkə informasiyasının toplanması
* Sosial mühəndislikdən istifadə

**Axtarış sistemlərindən istifadə** ən sadə və çox sürətli seçimdir. Google, Bing, Yahoo kimi internet axtarış sistemlərindən istifadə etməklə hədəf haqqında internetdə olan bütün mümkün məlumatları üzə çıxarmaq olar. Aşağıdakı əmrlər vasitəsilə Google-da hədəf sistem haqqında müəyyən məlumat toplamaq (Google Hacking) olar:

* site: spesifik vebsayt və domen axtarmaq üçün istifadə olunur. İki nöqtədən sonra saytın adı yazılır.
* filetype: xüsusi fayl tipinin yalnız daxilində axtarış aparır. İki nöqtədən sonra fayl tipi yazılır.
* link: axtarış termininə görə hiperlinklərdə axtarış edir.
* cache: veb səhifənin versiyasını müəyyən edir. İki nöqtədən sonra veb səhifənin URL-i yazılır.
* intitle: sənəd başlığında axtarış sözünü axtarır.
* inurl: sənədin URL-də axtarış sözünü axtarır.

İnformasiyanın toplanması mərhələsində hücumedən şirkətin açıq və məhdudlaşdırılan veb sayt URL-lərini də tapmağa çalışır. Məhdudlaşdırılmış URL-ləri tapmaq üçün «trial and error» metodu istifadə edilir ([www.netcraft.com](http://www.netcraft.com/))

Hədəf sistemin yerləşdiyi fiziki ünvan haqqında onlayn yerləşmə və xəritə servislərindən istifadə edərək məlumat toplamaq olar: Google Earth; Google Map; Wikimap; Yahoo Map.

İnsanlar, telefon nömrələri, ünvanlar (ABŞ) haqqında məlumat toplamaq üçün bir neçə onlayn servis mövcuddur.

İş saytlarından təşkilatın yerləşdiyi yer, əlaqə məlumatları, iş tələbləri, aparat və proqram təminatı haqqında biliklər əldə etmək mümkündür (məsələn, LinkedIn-dən)

GHDB təşkilatın sistem və şəbəkələrində təhlükəsizlik boşluqlarını tapan kompüter hakinq üsullarının kombinasiyasından ibarətdir. İlk dəfə Conni Lonq tərəfindən məşhurlaşdırılmışdır.

**Sosial şəbəkələrdən informasiyanın toplanması.** Sosial şəbəkələr digərlərinə nisbətən daha yaxşı informasiya mənbəyi hesab olunur. Hücumçu hədəfin fotosu, əlaqə məlumatları, şəxsi informasiya, fəaliyyətlər və digər məlumatları asanlıqla əldə edə bilə və fərdin əleyhinə istifadə edə bilər. Hücumedən sosial şəbəkə vasitəsilə yaxınlaşan tədbir barədə məlumatları və kritik verilənləri əldə edə bilər, saxta hesab aça, qrupları izləyə, maliyyə məlumatlarını ələ keçirə bilər və s.

**Veb saytlardan informasiyanın toplanması.** Hücumedən Burp Suite, Web Spiders, Zaproxy, Website Informer, Firebug, netcraft.com kimi vasitələrlə hədəf təşkilatın işlətdiyi proqram təminatı haqqında, əməliyyat sistemləri, altdirektoriyalar və digər faydalı məlumatları ələ keçirir.

**Poçt sistemlərində informasiyanın toplanması.** Partnyorlar, əməkdaşlar və digər şəxslərlə əlaqə üçün email ən çox işlənən vasitədir. Belə e-mail məktublarının kontentini ələ keçirmək hücumçular üçün daim maraqlı olmuşdur. Bu mənada aşağıdakı alətlər istifadə edilməkdədir: Polite Mail, Email Tracker Pro, Email Lookup, Who Read Me, Yesware və s.

**Rəqabət kəşfiyyatı.** Rəqabət kəşfiyyatı rəqiblər haqqında informasiya toplama, analiz və statistika metodudur. Bir neçə sadə mənbə bunlardır: rəsmi veb-saytlar, iş elanları, pres-relizlər, illik hesabatlar, məhsul kataloqları, analiz hesabatları, agentlər, distribüterlər.

Rəqabət kəşfiyyatı alətləri: Google Alerts, Monits, Trackur, Rankur, Alexa, Webb-stat və s.

**DNS verilənlərinin toplanılması.** Domen adı ilə əlaqədar informasiya (IP ünvanlar, DNS, IP yerləşmə, domen statusu və s.) əldə etmək məqsədilə müxtəlif vasitələrdən istifadə edirlər: Whois ([http://whois.domaintools.com](http://whois.domaintools.com/)), DNS Tools, Ultratools və s.

**Şəbəkə informasiyasının toplanması.** Hücumedən şəbəkə informasiyasının toplanması alətləri ilə şəbəkədən aşağıdakı məlumatları çıxara bilər:

* Şəbəkə ünvanlarının diapazonu;
* Host adları;
* Əməliyyat sistemi və tətbiqlərin versiya məlumatları;
* Tətbiqlərin strukturu və s.

# *10) Şəbəkənin inventarlaşdırılması*

İnventarlaşdırma fazasında hücum edən hədəf sistemlə aktiv qoşulmalara təşəbbüs edir. Daha çox informasiya almaq üçün bu aktiv qoşulmalar ilə birbaşa sorğular generasiya edilir. Bu informasiyalar sistemə hücum nöqtələrini müəyyənləşdirməyə kömək edir. Hücum edən hücum nöqtələrini aşkarladıqdan sonra o, toplanmış bu informasiyadan istifadə edərək aktivlərə icazəsiz giriş əldə edə bilər. İnventarlaşdırılan məlumatlara daxildir:

* + Marşrutlama məlumatları
  + SNMP məlumatları
  + DNS məlumatları
  + Kompüter adı
  + İstifadəçi məlumatları
  + Qrup məlumatları
  + Tətbiqi proqramlar və bannerlər
  + Şəbəkə paylaşma məlumatları
  + Şəbəkə resursları

Əvvəlki fazalarda axtarışlar hüquqi problemlərlə çox da əlaqəli deyildi. İnventarlaşdırma üçün alətlərdən istifadəsi hüquqi sərhədləri keçə bilər və hədəflə aktiv qoşulmalardan istifadə edilməsinə görə izlənilə bilərsiniz. Siz bu fəaliyyətləri həyata keçirmək üçün müvafiq icazələr almalısınız.

# İnventarlaşdırma üsulları

**EmailID istifadə etməklə inventarlaşdırma.** Email ID istifadə etməklə informasiyanın çıxarılması istifadəçi adı, domen adı və s. kimi faydalı məlumatlar təmin edə bilər. Email ünvanında istifadəçi adı və domen adı olur.

**Defolt parol istifadə etməklə inventarlaşdırma.** İnventarlaşdırmanın başqa bir yolu defolt parollardan istifadə edilməsidir. Hər bir qurğunun və proqram təminatının öz defolt parametrləri və identifikasiya məlumatları olur. Bu defolt parametrləri və konfiqurasiyanı dəyişmək tövsiyə olunur. Lakin bəzi administratorlar onları dəyişmədən istifadə etməkdə davam edirlər. Bu halda hücum edən defolt identifikasiya məlumatlarından istifadə etməklə asanlıqla icazəsiz giriş əldə edə bilər. Qurğunun defolt parametrlərini, konfiqurasiyasını və parolunu tapmaq o qədər də çətin iş deyil.

**DNS zona transferi vasitəsilə inventarlaşdırma.** DNS zona transferi prosesi vasitəsilə inventarlaşdırmaya DNS server, DNS yazıları, host adı, IP ünvan, istifadəmi adı və s. kimi digər qiymətli şəbəkə məlumatlarının əldə edilməsi daxildir. Zona transferi DNS serverin yenilənməsi prosesidir; Zona faylında hücum edənin axtardığı qiymətli informasiya olur. DNS serverlərə yönələn DNS sorğularda UDP 53 istifadə edilir. DNS zona transferində transferin normal keçməsini təmin etmək üçün TCP 53 istifadə edilir.

# NetBIOS inventarlaşdırma

NetBIOS (Network Basic Input/Output System – şəbəkə baza giriş/çıxış sistemi) proqramı lokal şəbəkə daxilində müxtəlif sistemlərdə işləyən müxtəlif tətbiqi proqramlar arasında kommunikasiyaya imkan verir. NetBIOS servisi şəbəkə qurğularını TCP/IP üzərindən identifikasiya etmək üçün unikal 16-ASCII hərfli sətirdən istifadə edir. İlk 15 hərf qurğunu, 16-cı hərf servisi identifikasiya etmək üçündür. NetBIOS servisi TCP port 139-u istifadə edir. TCP üzərindən NetBIOS (NetBT) aşağıdakı TCP və UDP portlarını istifadə edir:

* + UDP port 137 (ad servisləri)
  + UDP port 138 (dataqram servisləri)TCP port 139 (seans servisləri)

NetBIOS inventarlaşdırmadan istifadə edərək hücumedən aşağıdakıları aşkarlaya bilər:

* + Domen daxilindəki maşınların siyahısı
  + Fayl paylaşımları
  + Printer paylaşımları
  + İstifadəçi adı
  + Qrup məlumatları
  + Parol
  + Siyasətlər

***nbtstat*** komandası TCP/IP üzərindən NetBIOS statistikaları haqqında məlumatları göstərmək üçün faydalı alətdir. O həmçinin NetBIOS ad cədvəlləri, ad keşi və digər məlumatları da göstərə bilər. nbstat utilitindən istifadə edən komandaya misal aşağıda göstərilir:

nbtstat.exe –a "NetBIOS name of the remote system." nbtstat -A 192.168.1.10

**nbtstat** komandası bir neçə opsiya ilə istifadə edilə bilər.

NetBIOS inventarlaşdırma üçün digər faydalı alətlər: Hyena; Winfingerprint; NetBIOS Enumerator; Nsauditor Network Security Auditor.

# SNMP inventarlaşdırma

SNMP (Simple Network Management Protocol) inventarlaşdırma çox geniş istifadə edilən şəbəkə idarəetmə protokolu SNMP-dən istifadə edilməklə inventarlaşdırma üsuludur. SNMP inventarlaşdırmada istifadəçi hesabları və avadanlıq məlumatları hədəflənir.

Texniki baxımdan, SNMP-nin şəbəkədə tətbiqində üç komponent iştirak edir:

**SNMP Menecer:** İdarəetmə stansiyasında işləyən proqram təminatıdır, şəbəkə qurğularından toplanmış məlumatların anlaşıqlı şəkildə göstərilməsinə xidmət edir. PRTS, Solarwinds, OPManager və s. geniş istifadə edilən SNMP proqram təminatıdır.

**SNMP Agent:** Müxtəlif komponentləri monitorinq edilən şəbəkə qovşaqlarında işləyən proqram təminatıdır. Komponentlərə CPU/RAM istifadəsi, interfeysin status və s. missal ola bilər. SNMP agenti ilə SNMP meneceri arasında kommunikasiya üçün UDP port 161 istifadə edilir.

**Management Information Base (MIB):** MIB virtual verilənlər bazasında iyerarxik təşkil olunmuş informasiya toplusudur. Onlara SNMP kimi protokollar vasitəsi ilə müraciət edilir.

# LDAP inventarlaşdırma

LDAP (Lightweight Directory Access Protocol) açıq standartdır, Internet protokoludur. LDAP iyerarxik və məntiqi strukturlu paylanmış kataloq informasiya servislərinə giriş və idaəetmə üçün nəzərdə tutulub. Kataloq servisi istifadəçi, sistem, şəbəkə, servis və s. məlumatlarını şəbəkə üzrə paylaşmasına imkan verməklə vacib rol oynayır. LDAP istifadəçi adlarını və parolları saxlamaq üçün mərkəzi yer təmin edir. Proqramlar və servislər istifadəçiləri təsdiqləmək üçün LDAP serverinə qoşulur. Kliyent LDAP seansını başlatmaq üçün TCP port 389 istifadə edərək DSA agentinə (Directory System Agent) bir əməliyyat sorğusu göndərir. Kliyent və Server arasındakı kommunikasiyada BER (Basic Encoding Rules) kodlaşdırması istifadə edilir.

LDAP kataloq servislərinə daxildir:

* + Active Directory
  + Open Directory
  + Oracle iPlanet
  + Novell
  + eDirectory
  + OpenLDAP

# LDAP inventarlaşdırma alətləri:

* Jxplorer
* LDAP Admin Tool
* LDAP Account Manager
* Active Directory Explorer
* LDAP Administration Tool
* LDAP Search
* Active Directory Domain Services Management Pack
* LDAP Browser/Editor

# NTP inventarlaşdırma

NTP (Network Time Protocol) şəbəkədəki hostlarda və şəbəkə qurğularında saatları sinxronlaşdırmaq üçün istifadə edilir. NTP vacib protokoldur, çünki kataloq servisləri, şəbəkə qurğuları və hostlar login məqsədləri və hadisələrin protokollaşdırılması üçün saatdan istifadə edirlər. NTP protokolu UDP port 123-dən istifadə edir və onun bütün kommunikasiyası UTC-ə (Coordinated Universal Time) əsaslanır.

İnformasiya toplanmasının digər vacib aspekti müəyyən hadisənin baş verdiyi zamandır. Hücum edənlər ruterin zaman parametrlərin dəyişdirə və ya şəbəkəyə saxta NTP server daxil edə bilərlər ki, məhkəmə ekspertizası komandalarını çaşdırsınlar. NTP protokolunda dəstəklənən mexanizm zamanı həqiqi qəbul etməzdən əvvəl NTP serverin autentifikasiyasını həyata keçirir.

NTP-dən informasiya toplamaq üçün NTP komandaları, Nmap və NSE skripti kimi müxtəlif alətlərdən istifadə etmək olar. NTP inventarlaşdırma prosesində hücumedən aşağıdakı faydalı məlumatları əldə edə bilər:

* + NTP serverə qoşulmuş host məlumatları
  + Kliyentin IP ünvanı
  + Maşın adı
  + Əməliyyat sistemi məlumatları
  + Daxili IP-lərkimi şəbəkə məlumatları (əgər NTP server DMZ-də yerləşirsə)

**NTP inventarlaşdırma alətləri:** Nmap; NTP server Scanner; Wireshark, NTPQuery

# SMTP inventarlaşdırma

SMTP (Simple Mail Transfer Protocol) inventarlaşdırma hədəf barədə məlumat almaq üçün SMTP protokolundan istifadə edən üsuldur. SMTP protokolu e-poçt serverləri və istifadəçilər arasında 25-ci port üzərindən poçt kommunikasiyası təmin edir. SMTP əksər e-poçt serverləri tərəfindən istifadə edilən populyar TCP/IP protokollarından biridir.

İnventarlaşdırma üçün, məsələn, VRFY, RCPT TO və EXPN kimi SMTP komandalarını istifadə etmək olar. Bu komandalara SMTP serverin cavabları müxtəlifdir. SMTP serverlə telnet vasitəsilə qarşılıqlı əlaqədə olaraq həqiqi və saxta istifadəçilər üçün cavabları yoxlayıb müqayisə etməklə həqiqi istifadəçiləri müəyyən etmək olar.

**SMTP inventarlaşdırma alətləri:** NetScan Tool Pro; SMTP-user-enum; Telnet

# *11)Boşluqların idarə edilməsinin həyat dövrü*

Boşluqların idarə edilməsinin həyat dövrü aşağıdakı mərhələlərdən ibarətdir:

* 1. Planlaşdırma;
  2. Boşluqların qiymətləndirilməsi;
  3. Risklərin qiymətləndirilməsi;
  4. Aradan qaldırma.
  5. Verifikasiya;
  6. Monitorinq.

**Planlaşdırma –** şəbəkə inzibatçısı və ya pentester korporativ şəbəkənin təbiətini, tətbiqləri və servisləri müəyyən edir və bütün resurs və aktivlərin qiymətləndirməni prioritetləşdirməyə və idarə etməyə imkan verən «xəritə» yaradır.

**Boşluqların qiymətləndirilməsi –** bu mərhələ hədəfin qiymətləndirilməsinə fokuslanmışdır, təhlükəsizlik siyasətləri və yoxlamaları, fiziki təhlükəsizlik metrikalarının sınaqdan keçirilməsi və təftişi aparılır.

Boşluqların qiymətləndirilməsi sistem və tətbiqlərin təhlükəsizlik zəifliklərinin, səhvlərinin identifikasiyası, axtarılması

və yoxlanması prosesləri kimi təyin edilir. Boşluqların qiymətləndirməsinin növləri:

* **Aktiv qiymətləndirmə:** İşləməkdə olan şəbəkəyə aktiv sorğular göndərməklə cavabın yoxlanılması prosesidir.
* **Passiv qiymətləndirmə:** Boşluqları, işləməkdə olan servisləri, açıq portları və digər məlumatları öyrənmək üçün paketlərin tutulması prosesidir.
* **Xarici qiymətləndirmə:** Boşluqları aşkar etmək üçün xaricdən istismar etmə prosesidir.
* **Daxili qiymətləndirmə:** Boşluqları aşkar etmək üçün daxili şəbəkə və infrastrukturun daranması prosesidir. **Risklərin qiymətləndirilməsi –** aşkarlanmış boşluqları və onların təşkilatda və ya korporativ şəbəkədə təsirini qiymətləndirir. Boşluğun riskinin və (mümkün) nəticələrinin qiymətləndirilməsi üçün bir çox metodlar var. Riski

boşluğun istifadəsinin potensial mümkünlüyü (ehtimalı) kimi müəyyən etmək olar. Bir neçə vacib faktoru sadalayaq:

* Boşluq geniş məlumdurmu?
* Boşluq yayılıbmı?
* Boşluqdan istifadə etmək asandırmı?
* Boşluğu məsafədən istifadə etmək asandırmı?

Aşağıdakı düstur riskin qiymətləndirilməsinə sadə yanaşma ola bilər: 𝑁ə𝑡𝑖𝑐ə𝑙ə𝑟 = 𝑅𝑖𝑠𝑘 × 𝑃𝑜𝑡𝑒𝑛𝑠𝑖𝑎𝑙 𝑧𝑖𝑦𝑎𝑛𝑙𝑎𝑟. Potensial təhdidlər aşağıdakılar ola bilər:

* verilənlərə icazəsiz giriş;
* xidmətdən imtina (DoS);
* giriş hüququnun əldə edilməsi və ya artırılması və s.

Bu suallara cavab verərək, bülletenə potensial risk və nəticələr barəsində məlumat verən ümumi reytinq əlavə etmək

olar. Çox zaman, Aşağı, Orta və Yüksək kimi sadə terminlər istifadə edilir.

**Aradan qaldırma –** aşkar olunmuş boşluqlar prioritetlilik əsasında aradan qaldırılır.

**Verifikasiya –** bütün aşkar olunmuş boşluqların aradan qaldırılması yoxlanılır.

**Monitorinq –** Şəbəkə trafiki və sistemin davranışları daha geniş müdaxilələrə qarşı monitorinq edilir.

# *12)Boşluqların qiymətləndirilməsinə yanaşamlar*

## Boşluqların qiymətləndirilməsi sistemləri

Boşluğun risk dərəcəsi, bir qayda olaraq boşluq aşkarlanan sistemin istehsalçısı və ya informasiya təhlükəsizliyi vasitələri istehsal edən (boşluq skanerləri, IDS sistem və s.) şirkət tərəfindən müəyyən edilir. Bu zaman yol hərəkəti qaydalarında olan işıqfor sxemi istifadə edilir: aşağı dərəcədə risk (yaşıl), orta dərəcədə risk (sarı) və yüksək dərəcədə risk (qırmızı). Bəzən əlavə olaraq riskin dördüncü dərəcəsi – kritik boşluqlar da daxil edilir.

Belə yanaşmadan istehsalçıların əksəriyyəti istifadə edir. Məsələn, Microsoft proqram təminatı yenilənmələri haqqında elanlarında boşluqların kritikliyinin dörd səviyyəsindən istifadə edir.

Bu sadə yanaşma administratorun tələblərini həmişə ödəmir. Boşluğun risk dərəcəsi zaman keçdikcə dəyişə bilər.

İstifadəsinin detalları yalnız istehsalçı şirkətin mütəxəssislərinə məlum olan kritik boşluqla, istismar proqramı əlyetən olan boşluq arasındakı fərq böyükdür.

Boşluğun istifadə edilməsi ehtimalı ilə əlaqədar faktorları nəzərə almaq üçün standart “işıqfor” modelinə əlavə şərtlər daxil etmək lazımdır. Məsələn, SANS İnstitutu boşluqların analizi zamanı (SANS Critical Vulnerability Analysis) o

boşluqlara kritik səviyyəsi verir ki, bu boşluqdan istifadə edən, hamıya əlyetən və ya istismarı xüsusi vərdişlər tələb etməyən proqram mövcud olsun. Əks halda, hətta potensial olaraq çox təhlükəli boşluq kritik yox, yüksək səviyyəyə malik olacaq. SANS metodikasında istismarın sadəliyi ilə yanaşı, boşluğa həssas sistemlərin yayılması da nəzərə alınır. Microsoft şirkətinin PSS qrupu ziyankar proqram təminatı ilə bağlı riskin qiymətləndirilməsi metodikasında boşluğu

aradan qaldıran yenilənmənin mövcudluğu, hücum edənin istifadə edə biləcəyi hücum vektorlarının sayı, boşluğa həssas sistemlərin yayılması nəzərə alınır. Məsələn, “kritik təhlükəli soxulcan” yenilənmə olmayan Microsoft proqram təminatındakı lağım vasitəsilə, geniş yayılmış sistemlərdə iki və daha artıq hücum vektorundan istifadə etməklə

yayılmalıdır.

US-CERT-in istifadə etdiyi metodikada boşluğa aşağıdakı kriteriyalardan asılı olaraq qiyməti 0- 180 arasında olan risk

dərəcəsi müəyyən edilir.

* boşluq haqqında informasiya nə dərəcədə əlyetəndir?
* boşluqdan istifadə halları qeydə alınıbmı?
* şəbəkə üçün kritik İnternet-qovşaqlara təhlükə varmı?
* şəbəkənin boşluğa həssas qovşaqlarının sayı.
* boşluqdan istifadənin nəticələri necədir?
* boşluqdan istifadə nə dərəcədə asandır?
* boşluqdan istifadənin şərtləri necədir?

Təəssüf ki, kriteriyalar arasında onların mümkün çəkiləri və nəticədə alınan risk dərəcəsi formal müəyyən edilməyib, bu eyni boşluğun qiymətləndirilməsində ziddiyyətlər üçün geniş meydan verir. Bundan başqa, sadalanmış metodikalar konkret iş üçün yox, bütövlükdə İnternet üçün riskin qiymətini verir.

Yuxarıda qeyd edilənləri ümumiləşdirərək, boşluğun qiymətləndirilməsi metodikasına tələbləri aşağıdakıl kimi ifadə

etmək olar:

* boşluğun risk dərəcəsinin boşluğun istismarı imkanından asılı olaraq qiymətləndirilməsi imkanı olmalıdır;
* metodikanın tətbiqinin nəticəsi risklərin analizi zamanı istifadə üçün yararlı olan ədədi qiymət olmalıdır;
* metodikanın konkret informasiya sisteminə adaptasiyası imkanı olmalıdır;
* qiymətləndirmə zamanı istifadə edilən parametrlər minimum müxtəlif yozuma malik olmalıdır;
* yekun qiymətin hesablanması mexanizmi sadə və anlaşıqlı olmalıdır

# *13)Sistemin hakinq edilməsi metodologiyası, keyloqqerlər*

## Sistemin hakinqi

Sistemin hakinq edilməsi metodoloji yanaşmasında sosial mühəndislik və ya parol sındırma üsulu ilə girişə nəzarət sistemlərindən keçərək sistemə sızılır, imtiyazlar genişləndirilir, uzaqdan giriş üçün müxtəlif növ zərərli proqramlar hədəf maşında quraşdırılır. Təşkilatın kritik informasiya aktivlərini ələ keçirən şəxs öz kimliyini gizlətməlidir. Sistemin hakinq edilməsi metodologiyası aşağıdakı mərhələlərdən ibarətdir:

* Parolların qırılması;
* İmtiyazların genişləndirilməsi;
* Hazırlanmış tətbiqlərin icra olunması;
* Faylların gizlədilməsi;
* İzin itirilməsi.

**Parolların sındırılması -** parolu sındırma nəticəsində sistemə qanuni istifadəçi kimi giriş edilir. Adətən, identifikasiya/autentifikasiya üçün istifadəçi adı və parol üçün tələb olunur. Lakin iki və ya çox faktorlu giriş metodları da mövcuddur. O cümlədən, biometrik üsularla qorunma metodları da vardır. Parollar güman ediləbilən, qısa, zəif

şifrlənmiş, yalnız hərf və ya rəqəm ehtiva edən olduqda sındırılması asan başa gəlir.

**Parolların sındırılması alətləri –** pwdump7; fgdump; LophtCrack; Ophcrack; RainbowCrack; Cain and Abel, FlexySpy (mobil platformalar üçün), John the Ripper.

**Microsoft autentifikasiya –** Microsoft platformasında əməliyyat sistemi defolt autentifikasiya protokolları çoxluğundan istifadə edir: Kerberos; Security Account Manager; NT LAN Manager, LM və başqaları.

**İmtiyazların genişləndirilməsi –** Təkcə aşağı privilegiyalı istifadəçi hesabının əldə edilməsi məqsədə nail olmağa

kömək etməyə bilər. Yüksək səviyyəli giriş üçün imtiyazların genişləndirilməsi və ya məhdudiyyətlərin

kənarlaşdırılması tələb olunur. Imtiyazların genişləndirilməsi iki növə bölünür: Üfüqi imtiyaz genişləndirmə, Şaquli imtiyaz genişləndirmə.

**Tətbiqlərin icra edilməsi –** Zərərli proqram tətbiqlərinin icra edilməsində məqsəd sistem resurslarına avtorizasiyasiz giriş, parolların sındırılması və digər motivlərdir. Bu proses həm də «sistem mənimsəmə» adlanır. Hücumçu aşağıdakı fəaliyyətləri edir:

* 1. İnformasiya toplamaq üçün zərərli proqramları quraşdırır;
  2. Girişi istismar etmək üçün bekdor quraşdırır;
  3. Parol və skriptləri sındırmaq üçün kreker quraşdırır;
  4. Klaviatura kimi giriş qurğularından daxil edilən informasiyanı əldə etmək üçün keyloqqerlər quraşdırır Keyloqqerlər proqram və ya aparat təminatı olmaqla klaviatura kimi giriş qurğularından istifadə edərək daxil edilmiş məlumatların monitorinqi prosesini yerinə yetirir. Keyloqqerlər əleyhinə görülən tədbirlər:
  + Anti-keyloqqerlərin istifadəsi;
  + Kompüter əsaslı İDS-lər;
  + Fiziki monitorinq;
  + Şübhəli email və URL-lərə klikləməmək;
  + Kritik verilənləri daxil edərkən ekran klaviaturasından istifadə edilməsi;
  + Quraşdırmadan öncə faylın daranması.

**Anti keyloqqerlər –** keyloqqerlər əleyhinə istifadə olunan tətbiqi proqramlardır. Bu proqramlar SSL qoruma, keyloq qoruma, mübadilə buferinin keyloq prosesini qoruma, ekran loqlaşdırmasını qoruma kimi prosesləri təmin etməklə keyloq prosesini kənarlaşdırır.

Uzaqdan icraetmə (RemoteExec) – kod və skriptlərin, tətbiqlərin uzaqdan quraşdırılması üçün dizayn edilmiş proqram

təminatıdır. O, hədəf sistemdəki faylları şəbəkə üzərindən yeniləyə bilir. Proqramın əsas xüsusiyyətləri aşağıdakılardır:

* + Paketlərin hədəf sistemdə yerləşdirilməsi;
  + Proqram və skriptlərin uzaqdan icra edilməsi;
  + Xüsusi vaxt və zaman üçün icra edilmənin planlaşdırılması;
  + Uzaqdan konfiqurasiyanın idarə edilməsi;
  + Hədəf sistemin uzaqdan idarə edilməsi (söndürmə, yuxu, yenidən başlatma, kilitləmə və s.).

# Casus proqram təminatı, izlərin gizlədilməsi alətləri

**Faylların gizlədilməsi. Rutkitlər** - Rutkitlər hədəf sistem üzərindən uzaqdakı sistem istifadəçisinə imtiyazlı giriş üçün dizayn edilmiş poqramlar toplusudur. Rutkitlərin aşağıdakı növləri var:

* Tətbiqi səviyyə rutkitləri;
* Kernel (nüvə) səviyyəli rutkitlər;
* Aparat/İstehsalçı səviyyəli rutkitlər;
* Boot loader səviyyəli rutkitlər (butkitlər);
* Hipervizor səviyyəli rutkitlər.

Rutkit alətləri – Avatar, Necurs, Azazel, ZeroAccess. Rutkitlərin aşkarlanmasına yanaşmalar:

* Tamlıq əsaslı aşkarlanma
* Rəqəmsal imzalardan istifadə
* Fərq əsaslı aşkarlanma
* Davranışın aşkarlanması
* UNİX: Zeppoo, Chrookit;
* Windows: Microsoft Sysinternals RootkitRevealer, Avast, Sophos anti-rutkitləri istifadə edilir.

**İzlərin itirilməsi –** izlərin itirilməsində məqsəd sübutların yox edilməsidir. Hücumedən bu mərhələdə bütün hadisələrin

loqlarını, xəta mesajlarını silir. Hücumedənin istifadə etdiyi ümumi üsullar aşağıdakılardır: Auditin deaktivasiyası, Loqların təmizlənməsi, Loqların manipulyasiyası.

İzlərin itirilməsi üçün aşağıdakılar tövsiyə olunur: Müvəqqəti faylların silinməsi; Keşin təmizlənməsi; Kukilərin təmizlənməsi; Auditin deaktivasiyası; Loq faylların təmizlənməsi; Loqların modifikasiyası; CCleaner, auditpol.exe, clearlogs.exe, MRU-Blaster kimi alətlərdən istifadə.

## ***15)Kompüter virusları və şəbəkə soxulcanlarının müxtəlif sinifləri***

Kompüter virusları informasiya təhlükəsizliyinin təmin olunmasının hər üç baza prinsipinin - konfidensiallığın, tamlığın və əlyetənliyin pozulmasının ən geniş yayılmış səbəblərindən biridir. Tarix. Kompüter virusları təxminən 1980-ci illərin əvvəllərində meydana çıxmışdır. Özüçoxalan süni konstruksiyaların ilk tədqiqatları riyaziyyatçılar fon Neyman və N. Viner tərəfindən 1950-ci illərdə aparılmışdı. Lakin «kompüter virusu» terminin özü 1984-cü ildə ABŞ-da keçirilən informasiya təhlükəsizliyi üzrə 7-ci konfransda Fred Koen tərəfindən işlədilmişdi.

**Kompüter virusları -** digər proqramlara yeridilmə yolu ilə müstəqil yayılan, müəyyən şərtlər yerinə yetirildikdə kompüter sisteminə mənfi təsir göstərən (kiçik) proqramlardır. Kompüter virusu – başqa proqramlara özünün sonradan yayılma qabiliyyətini saxlayan işlək surətlərini birləşdirmək qabiliyyəti olan proqramdır. Adətən virusun həyat müddəti iki fazadan ibarətdir:

* + **çoxalma –** virus zahirən üzə çıxmamağa çalışaraq müxtəlif yoluxdurma strategiyalarından istifadə etməklə mümkün qədər geniş yayılmağa çalışır;
  + **özünü göstərmə –** virus onda reallaşdırılmış, müxtəlif effektlər və dağıdıcı əməllər törədən proseduru yerinə yetirir.

**Virusların yayılması.** Şəbəkə və kommunikasiya texnologiyalarında hər bir yenilik virusların yaradılması və yayılması üçün yeni imkanlar, yollar açır. Əvvəllər viruslar disketlər və digər yaddaş daşıyıcıları vasitəsi ilə yayılırdı, İnternetin geniş yayılması viruslar üçün geniş magistral yol açmışdır. Bu səbəbdən kompüter virusları Internetdə real dünyada bioloji virusların yayılmasından daha sürətlə yayılır.

## Kompüter viruslarının təsnifatı:

1. Yaşayış mühitlərinə görə
2. Yoluxdurma üsullarına görə
3. Destruktiv imkanlarına görə
4. Alqoritmin özəlliklərinə görə
5. Faylları yoluxdurma üsullarına görə

**Yaşayış mühitlərinə görə** virusların aşağıdakı növləri var: Fayl, Yükləmə, Makroviruslar, Skript, Fayl-yükləmə virusları.

**Yoluxdurma üsullarına görə** viruslar rezident və qeyri-rezident olurlar.

**Destruktiv imkanlarına görə** virusları aşağıdakı siniflərə bölmək olar: zərərsiz, təhlükəsiz, təhlükəli, çox təhlükəli.

**Alqoritmin özəlliklərinə görə** virusların aşağıdakı qruplarını ayırmaq olar: tələbə, stels, polimorf.

**Faylları yoluxdurma üsullarına görə** virusların klassifikasiyas: Üstəyazan, Parazit, Kompanyon, Link,Virus-«soxulcanlar», Fayl-soxulcanlar.

## Soxulcanlar

**Soxulcanlar −** müstəqil, yəni başqa proqramlara yeridilmədən öz surətlərini kompüter sistemlərində yaymağa və onları işə salmağa qabil olan proqramlardır. Soxulcanların axın kimi yayılması rabitə kanallarının, yaddaşın həddən artıq yüklənməsinə və son nəticədə sistemin bloka alınmasına gətirib çıxarır.

Soxulcanların ilk nümunəsi Morris soxulcanıdır, bu soxulcan C dilində 4000 sətirdən ibarət proqram idi. Soxulcanlar həm müstəqil, həm də insanın müəyyən hərəkətləri nəticəsində yayıla bilərlər. Şəbəkə soxulcanı iki müxtəlif “infeksiya” və “faydalı” hissədən ibarət ola bilər. “İnfeksiya” hissəsi diskdə faylların və operativ yaddaşda proqramların yoluxdurulmasına cavabdehdir. “Faydalı” hissə isə digər əməlləri yerinə yetirir, məsələn, verilənləri oğurlayır, faylları korlayır və ya kompüteri DDoS-hücumlar üçün zombiyə çevirir. Poçtla yayılan soxulcanların

əksəriyyəti bir fayldan– yalnız “faydalı” hissədən ibarət olur. Ayrıca “infeksiya” hissəsi tələb edilmir, çünki istifadəçi

soxulcanı könüllü yükləyir və instalyasiya edir. Soxulcan sürətlə yayılsa, kompüterin işini yavaşıda və şəbəkə bağlantılarının sürətini azalda bilər.

Soxulcanların aşağıdakı növlərini ayırırlar.

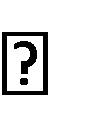
* + **Email-Worm –** elektron poçt kanalları ilə öz-özünə yayılma qabiliyyəti olan soxulcanlardır.
  + **IM-Worm –** ani məlumat mübadiləsi sistemlərinin (məsələn, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype və s.) kanalları ilə öz-özünə yayılma qabiliyyəti olan soxulcanlardır.
  + **IRC-Worm –** Internet Relay Chats (IRC) vasitəsi ilə öz-özünə yayılma qabiliyyəti olan soxulcanlardır;
  + **Net-Worm –** kompüter şəbəkələrində öz-özünə yayılma qabiliyyəti olan soxulcanlardır.
  + **P2P-Worm –** fayl mübadiləsi pirinq (ing. peer-to-peer, P2P) şəbəkələrinin (məsələn, Kazaa, Grokster, eDonkey, FastTrack, Gnutella və s.) kanalları ilə öz-özünə yayılma qabiliyyəti olan soxulcanlardır.

## ***16)Troyanlar və onların təsnifatı***

**Troyanlar -** funksional cəhətdən faydalı proqram kimi görünən zərərli proqramlardır. İşə düşdükdə troyanlar elan

edilmiş faydalı funksiyalarla yanaşı elan, olunmamış funksiyaları da yerinə yetirirlər.

“Troyan” termini ilk dəfə sonradan Milli Təhlükəsizlik Agentliyinin əməkdaşı olan haker Dan Edvars tərəfindən istifadə edilmişdir. Troyanlar qəsdən törədilən təhdidlərin reallaşdırılmasında xüsusi rol oynayırlar. Troyanların yazılmasının əsas məqsədi yoluxmuş kompüterdə icazəsiz hərəkətlərin həyata keçirilməsidir, buna görə troyanları etdikləri zərərli hərəkətlərin tipinə görə klassifikasiya etmək olar (Kaspersky Lab).

* + **Məsafədən administratorluq troyanları (Backdoor – bekdor) –** bu sinif troyan proqramları kompüterləri şəbəkədə məsafədən idarə etmək (administratorluq) üçün utilitlərdir. Öz funksional imkanlarına görə onlar bir çox cəhətdən proqram istehsalçıları tərəfindən yaradılan və yayılan müxtəlif administratorluq sistemlərini xatırladır.
  + **Trojan-PSW (PSW – Password-Stealing-Ware, parolların oğurlanması) –** bu ailə yoluxmuş kompüterdə müxtəlif konfidensial informasiyanı saxlayan (adətən, telefon nömrələrini və İnternetə giriş parollarını) sistem fayllarını axtarırlar və onu «troya atının» kodunda göstərilmiş elektron ünvana və ya ünvanlara göndərirl’r.
  + **Trojan-Clicker (internet-klikerləri) –** troyanların bu ailəsinin əsas funksiyaları internetresurslara (adətən veb- səhifələrə) sanksizyasız müraciətləri təşkil etməkdir. Bu ya brauzerə uyğun komandaların göndərilməsi, ya da internet-resursların «standart» ünvanları göstərilən sistem fayllarının dəyişdirilməsi (məsələn, MS Windows-da hosts faylı) ilə əldə olunur.
  + **Trojan-Downloader (digər zərərli proqramların çatdırılması) –** bu sinif troyan proqramları qurban-kompüterə zərərli proqramların yeni versiyalarının yüklənməsi və quraşdırılması üçün nəzərdə tutulub. Yüklənən proqramların adları və yerləri haqqında informasiya troyanın kodunda və verilənlərində olur və ya troyan tərəfindən «idarə edən» internet-resursdan (adətən veb-səhifədən) oxunur. Trojan-Dropper (digər zərərli proqramların quraşdırılması) – hədəf-kompüterə virusların və ya digər troya proqramlarının gizli quraşdırılması üçün istifadə edilir.
  + **Trojan-Proxy (troyan proksi-serverləri) –** müxtəlif Internet-resurslara anonim girişi gizli həyata keçirirlər. Adətən, spamın göndərilməsi üçün istifadə edilir.
  + **Trojan-Spy (casus proqramları) –** Bu troyanlar yoluxmuş kompüterin istifadəçisindən elektroin casusluq edirlər: klaviaturadan daxil edilən informasiya, ekranın şəkilləri, aktiv proqramların siyahısı və istifadəçinin onlarla hərəkətləri diskdə hər hansı faylda saxlanır və vaxtaşırı bədniyyətliyə göndərilir. Bu növ troya proqramları tez- tez müxtəlif onlayn ödəniş və bank sistemləri istifadəçilərinin informasiyasaını oğurlamaq üçün istifadə edilir.
  + **Trojan (digər troyan proqramları) –** bu sinfə troyan proqramların tərifinə düşən digər hərəkətləri, yəni verilənlərin məhv edilməsi və ya bəd niyyətlə dəyişdirilməsi, kompüterin iş qabiliyyətinin pozulması və başqa həyata keçirən proqramlar düşür. Bu kateqoriyaya həmçinin «çox məqsədli» troya proqramları da daxildir, məsələn, eyni zamanda istifadəçidən casusluq edən və məsafədəki bədəmələ proxy-servis göstərən troyanlar.
  + **Trojan-Notifier (uğurlu hücum haqqında məlumatlandırma) –** bu növ troyanlar öz «sahiblərinə» kompüterin yoluxdurulması haqqında məlumat vermək üçün nəzərdə tutulub. Bu zaman «sahibin» ünvanına kompüter haqqında məlumat göndərilir, məsələn, kompüterin IP-ünvanı, açıq portun nömrəsi, elektron poçtun nömrəsi və s. Göndərmə müxtəlif üsullarla yerinə yetirilir: elektron məktubla, «sahibin» veb-səhifəsinə xüsusi tərtib

olunmuş müraciətlə, ICQ-məlumatla və s..

**17)** ***Zərərli proqramların növləri.***

Kompüter sistemlərində informasiya təhlükəsizliyinə təhdidlərin əsas mənbələrindən biri "zərərli proqramlar" kimi ümumi ad almış xüsusi proqramlardan istifadə edilməsidir. “Zərərli proqramlar” (ing. malware sözü malicious – zərərli (bədniyyətli) və software – proqram təminatı) anlayışı icazəsiz və çox zaman zərərli əməllərin həyata keçirilməsi üçün yaradılan və istifadə edilən bütün proqramları birləşdirir. Nə vaxtsa bütün zərərli proqramları təsvir etmək üçün “virus” və “troya atı – troyan” anlayışları kifayət edirdi. Lakin həmin vaxtlardan kompüterlərin yoluxdurulması üsulları və texnologiyaları xeyli irəli gedib və bu iki anlayış zərərli proqramların bütün rəngarəngliyini təsvir etmək üçün kifayət deyil. Viruslar, backdoor-proqramlar (məsafədən icazəsiz administratorluq üçün yaradırlar), klaviatura casusları (ing. keylogger – key – klaviş və logger – loq yazan)), parolları oğurlayan proqramlar və troya atlarının digər növləri, Word və Excel üçün makroviruslar, yükləmə sektoru virusları, skript virusları (BAT-viruslar, windows shell-viruslar, java-viruslar və s.) və skript troyanları, casusluq (ing. adware − advertisement − reklam və software) və reklam proqramları (ing. spyware − spy − casus və software) – bu zərərli proqramlar kimi təsnif olunanların tam siyahısı deyil.

***18) BOTNELƏR VƏ ONLARİN ARXİTEKTURASİ***

DDoS-hücumların təşkili üçün bədniyyətlilər yoluxmuş kompüterlərin xüsusi şəbəkəsindən – botnetdən istifadə edirlər. DDoS-hücumlar zamanı bədniyyətlilər çox vaxt “DDoS klasteri” adlanan üçsəviyyəli arxitekturadan istifadə edirlər. Bu iyerarxik struktura aşağıdakılar daxildir (şəkil 2.1): − idarəetmə konsolu (onlar bir neçə ola bilər) – məhz bu kompüterdən bədniyyətli DDoShücumun başlaması haqqında siqnal verir; − master-kompüterlər – bu kompüterlər idarəetmə konsolundan DDoS-hücum siqnalı alır və onu agentlərə ötürürlər. Hücumun miqyasından asılı olaraq bir idarəetmə konsoluna bir neçə yüzədək master-kompüter düşə bilər. agentlər – sorğularla hədəf-qovşağa bilavasitə hücum edirlər. Bir qayda olaraq, həm master-kompüterlər, həm də agent-kompüterlər «zombi»lərdir, yəni onların sahibləri kompüterlərinin DDoS-hücumların iştirakçıları olduqlarını bilmirlər. Qeyd etmək lazımdır ki, bütün agentlər bir-birindən və bədniyyətlidən asılı olmadan avtonom rejimdə fəaliyyət göstərirlər. Hər bir agentin avtonom hərəkət etdiyini və hücumun aktiv komponentlərindən asılı olmadığını nəzərə alsaq, hətta bir neçə agentin eyni zamanda neytrallaşdırılması bütün hücumu tam dayandıra bilməz, çünki bu agentlərin sayı masterlərin köməyi ilə daim artırılır. Bundan başqa, masterlərin və agentlərin sayı heç nə ilə məhdud deyil. Belə strukturu əks istiqamətdə izləmək praktiki olaraq mümkün deyil. DDoS hücumlarında masterlərin və zombilərin istifadəsi hücumun həqiqi təşkilatçısının kim olduğunu gizlədir. Hakermaster-zombi arasındakı əlaqənin şifrlənmiş olması, zombilərin göndərdikləri paketlərin mənbə ünvanının saxta olması hücumu həyata keçirən bədəməlin tapılması prosesini olduqca çətinləşdirir. Hücum edilən ən çoxu agentin ünvanını müəyyən edə bilər. Xüsusi tədbirlər ən yaxşı halda masterkompüterin üstünə çıxara bilər. Lakin həm agentlər, həm də masterlər bu hücumda zərərçəkənlərdir. Bu struktur hücumu təşkil edən qovşağın ünvanını izləyib tapmağı praktiki olaraq qeyri-mümkün edir.

# *19.DDoS-hücumların sinifləri*

Xidmətdən imtina hücumları (DoS attaks) – qanuni istifadəçilərin sistemə, şəbəkəyə, tətbiqi proqrama və ya informasiyaya girişini əngəlləmək üçün yerinə yetirilən bədniyyətli hərəkətlərdir. DoS-hücumlar müxtəlif formalara malikdir, onlar birmənbəli və ya paylanmış olurlar. DoS-hücum texniki və qeyri-texniki vasitələrlə yaradıla bilər.

Texniki vasitələrlə yaradılan DoS-hücumlar iki üsulla həyata keçirilə bilər. Birinci üsulda hücum edilən kompüterdə proqram təminatının müəyyən boşluğu istifadə edilir. Bu boşluğun köməyi ilə kompüterdə müəyyən kritik səhv yaratmaq və sistemin iş qabiliyyətinin pozulmasına səbəb olmaq olar.

İkinci üsulda hücum edilən kompüterə eyni zamanda böyük sayda paketlər göndərməklə həyata keçirilir. Hər bir paket müəyyən müddətə emal olunur. Əgər bu vaxt yeni paket daxil olursa, o, növbəyə qoyulur və sistemin müəyyən

resurslarını zəbt edir. Sistemə eyni vaxtda olduqca çox sayda paket göndərilsə, onda həddindən artıq yüklənmə

nəticəsində kompüter «boğula» və ya işini tam dayandıra bilər.

DoS-hücumun bir növü olan paylanmış DoS-hücum (DDoS) – çox böyük sayda kompüterin köməyi ilə təşkil edilir, bunun

sayəsində hətta İnternet-kanallarının buraxma imkanı olduqca böyük olan serverlər də bu hücuma təslim olurlar. DDoS-hücumları üçün bədniyyətlilər yoluxmuş kompüterlərin xüsusi şəbəkəsi botnetdən istifadə edirlər.

* DDoS-hücumlar zamanı bədniyyətlilər çox vaxt “DDoS klasteri” adlanan **üçsəviyyəli arxitekturadan** istifadə edirlər: **idarəetmə konsolu –** məhz bu kompüterdən bədniyyətli DDoS hücumun başlaması haqqında siqnal verir;
* **master-kompüterlər –** idarəetmə konsolundan DDoS-hücum siqnalı alır və agentlərə ötürürlər.
* **agentlər –** sorğularla hədəf-qovşağa bilavasitə hücum edirlər.

Bu kompüterlərin sahibləri kompüterlərinin DDoS-hücumların iştirakçıları olduqlarını bilmirlər.

Bütün agentlər avtonom rejimdə fəaliyyət göstərirlər. Bir neçə agentin eyni zamanda neytrallaşdırılması bütün hücumu tam dayandıra bilməz, çünki bu agentlərin sayı masterlərin köməyi ilə daim artırılır.

DDoS-hücumların bir növü olan paylanmış dolayı DoS-hücumları **(Distributed Reflection DoS, DRDoS)** – İnternet şəbəkəsinin “vicdanlı” hostları ilə dolayı həyata keçirilir. DRDoS hücumunun klassik sxemi ondan ibarətdir ki, TCP-paket hücum edilən obyektin ünvanına deyil, ixtiyari hostun (reflektorun) IP-ünvanına ötürülür. Bu paketdə qayıtma ünvanı hücum obyektinin ünvanı ilə əvəz edilir. Əgər birinci paketdə mənbənin ünvanı olaraq hücum obyektinin ünvanı göstərilsə, SYN-bayrağı olan TCP sorğusuna cavab verəcək server bu ünvana SYN+ACK bayraqlı bir neçə TCP-paket göndərəcək.

## DoS-hücumlara nümunələr.

DoS-hücumların ilk növləri birmənbəli hücumlar idi, yəni hücumun həyata keçirilməsi üçün yeganə bir sistem istifadə edilirdi. “SYN flood attack” adlanan hücumlar daha çox məşhurluq qazanmışdı. Sinxron hücumdan sonra daha ciddi, lakin qarşısının alınması nisbətən asan olan başqa hücumlar da meydana çıxdı:

**TCP SYN flooding hücumu.** Bu hücumun yerinə yetirilməsi zamanı göndərən-sistem alan-sistemə çox böyük sayda TCP SYN-paketlər göndərir. SYN paketlər yeni TCP-birləşmələrin yaradılması üçün istifadə olunur. TCP nəqliyyat protokolu birləşmənin iki subyekti arasında verilənlərin mübadiləsi başlayana kimi virtual rabitə kanalı yaradılmasını nəzərdə tutur. SYN-paketi aldıqda alan-sistem verilənlərin uğurla qəbulu haqqında xəbər verən ACK-paketlə cavab verir və birləşmə qurmaq üçün verilənləri SYN-paket göndərənə göndərir. Bu zaman alan-sistem yeni birləşmə haqqında informasiyanı birləşmələrin növbə buferinə yerləşdirir.

TCP SYN Flooding hücumuna şəbəkənin TCP-birləşmə qurmaq imkanı olan bütün hostları (serverlər, marşrutizatorlar) həssasdır. Bir qayda olaraq, TCP SYN Flooding IP-şəbəkənin nömrələri 25 (SMTP), 80 (HTTP) və 110 (POP3) olan xidmətlərinə qarşı aparılır. NetBIOS-un 139- cu portda fəaliyyət göstərən xidmətinə qarşı çox az səmərə ilə təsir edir.

**Smurf-hücumu.** Bu hücum ICMP exo-paketlərinin istifadəsinə əsaslanır. Smurf-hücumunun gerçəkləşdirilməsi zamanı

bədniyyətli hücum obyektinin adından ICMP-exo paketləri əvvəlcədən seçilmiş şəbəkəyə genişyayımla göndərir.

Genişyayımlı ICMP-exo sorğuları alan bütün kompüterlər hücum obyektinə exo cavab göndərəcək. Beləliklə, bir paket göndərməklə bədniyyətli həm hücum obyektinə münasibətdə, həm də genişyayımlı exo sorğunu alan şəbəkəyə münasibətdə böyük həcmdə trafik yaradır. Bu rabitə kanalının buraxma qabiliyyətinin əhəmiyyətli azalmasına, bəzi hallarda şəbəkənin tam təcrid edilməsinə gətirib çıxara bilər.

***20)DDoS-hücum alətləri***

Bədniyyətlilər DoS-hücumların müxtəlif növlərini kombinasiya edə bilərlər, belə hücumlar daha təhlükəli və aradan qaldırılması çətin olar. Bunun üçün onlar Trinoo, TFN, TFN2K, Stacheldracht, Mstream kimi instrumental vasitələrdən istifadə edə bilərlər. Bu instrumental vasitələr hakerdən yüksək hazırlıq səviyyəsi tələb edir, hakerə bir hədəfə yönəlmiş DDoS-hücumda çox sayda sistemin qüvvəsini əlaqələndirməyə imkan verir. Bəzi instrumental vasitələr hücum edən paketlərdə göndərənin ünvanını təsadüfi şəkildə dəyişdirir, bu onların aşkarlanmasını olduqca çətinləşdirir.

**TFN (Tribe Flood Network) paketi** UNIX sistemində istifadə üçün nəzərdə tutulmuşdur, DDoS-hücumların təşkili üçün ilk açıq əlyetən vasitə idi. Paketin tərkibinə kliyent və server komponenti daxildir. TFN paketinin köməyi ilə ICMP, UDP- paketlərinin istifadəsi ilə hücumları, həmçinin smurf hücumunu gerçəkləşdirmək olar. Bu komponentlərlə yanaşı TFN paketinin tərkibinə TCP-portla əlaqəli komanda örtüyünə giriş əldə etməyə imkan verən modul da daxildir.

**Trinoo paketi**nin də tərkibinə kliyent və server komponentləri daxildir. Kliyentlə əsas proqram arasında qarşılıqlı əlaqə 27665-ci TCP-portla bağlantı vasitəsilə həyata keçirilir. Əsas proqramın serverlə əlaqəsi 27444-cü UDP portu, əks istiqamətdə isə 31335-cü UDP portu ilə qurulur. Trin00 ilk dəfə 1999-cu ilin avqustunda meydana çıxıb. Master və agent rolunda Linux və Solaris ƏS-nin idarəsi altında işləyən şəbəkə qovşaqları çıxış edə bilər. Bu hücumun son mərhələsində kompüter agentlər PingFlooding hücumundan istifadə edir.

**Stacheldraht (“tikanlı məftil”) paketi** Trinoo və TFN-in imkanlarını birləşdirir, əsas və tabe modullar arasında şifrlənmiş telnet seansını gerçəkləşdirir. Bunun sayəsində IDS-i neytrallaşdırmaq olar. TFN kimi Stacheldraht ICMP-, UDP-, SYN- və Smurf-hücumları həyata keçirmək imkanı verir. Kliyentin serverlə qarşılıqlı əlaqəsi TCP- və ICMP-paketlərin

kombinasiyası olan EchoReplay vasitəsilə həyata keçirilir. Serverlə kliyent arasında qarşılıqlı əlaqə zamanı simmetrik açarlı şifrləmə alqoritmi tətbiq edilir. Bundan başqa, parolla mühafizə rejimi də aktivdir. Zəruri olduqda bədniyyətli server komponentini yeniləyə bilər (rcp komandasından istifadə etməklə).

**TFN2K (TFN 2000) paketi** TFN-in xələfidir, qarşılıqlı əlaqə prosesində ixtiyari seçilmiş nömrəli portlardan istifadə etməyə imkan verir. Bunun sayəsində sərhəd marşrutizatorlarında portların bloklanmasından yan keçmək olar. TFN kimi TFN 2000 də ICMP-, UDP-, SYN- və smurf-hücumları dəstəkləyir, bundan başqa, hücumun müxtəlif növlərinə təsadüfi şəkildə keçə bilir. Lakin Stachelhardt paketində istifadə edilən şifrləmə alqoritmindən fərqli olaraq nisbətən zəif Base 64

şifrləmə alqoritmi tətbiq edilir.

**WinTrinoo paketi** Trinoo-nun Windows sistemində istifadə üçün nəzərdə tutulan versiyasıdır. Wintrino troyan tipli proqramdır, adətən, servise.exe adlanır (əgər adı dəyişdirilməyibsə) və 23145 baytdır. (servise.exe-ni Windows-un services.exe-si ilə qarışdırmayın). Bu proqram işə salındıqdan sonra Windows reyestrinə yeni parametr yazılır və bundan sonra sistem işə düşdükdə troyan da avtomatik yüklənir:

**Mstream –** 2000-ci ilin aprelində aşkarlanmış DDoS alətidir, TCP və UDP protokollarından istifadə edir və paket flooding üsulu ilə işləyir. Hücum üçün Attacker -> Masters -> Agents -> Target(s) dördsəviyyəli sxemdən istifadə edir.

**DoS hücumların aşkarlanması.** Serveri yükləyən paketlərin trafikin həqiqi sorğuları, yoxsa DDoS hücumu olmasını təyin etmək çətindir. Bunun üçün müxtəlif DDoS hücumlarının mexanizmi öyrənilir, loq-fayllar analiz edilir. Lakin müasir DDoS hücumlarının davranışı o qədər mürəkkəbdir ki, onların necə hücum edəcəklərini əvvəlcədən demək mümkün deyil.

Aşkarlama metodları:

* **siqnatura –** trafikin keyfiyyət analizinə əsaslanır;
* **statistik –** trafikin kəmiyyət analizinə əsaslanır;
* **hibrid –** əvvəlki iki metodun üstünlüklərini birləşdirir.DDoS-hücumların aşkarlanması üçün DDOSPing, Zombie Zapper və find\_ddos alətlərindən istifadə etmək, nömrələri məlum portların açıq olmasını yoxlamaq olar.

## ***21)DoS-hücumlardan müdafiə mexanizmləri***

Müasir əməliyyat sistemlərində bir çox DoS-hücumların qarşısı alınmışdır. Qarşısı alınmış DoS hücumlara misal olaraq ping vasitəsi ilə həyata keçirilən hücumları göstərmək olar. Bu gün bir çox əməliyyat sistemlərində normal üsul ilə yanlış formatlı ICMP paketlərinin göndərilməsi mümkün deyil. Bundan başqa, bəzi əməliyyat sistemlərində böyük həcmli paketlərə qarşı davamlılıq artırılmışdır. Bir çox serverdə isə bu növ hücumların qarşısını almaq üçün ICMP xidmətini, ümumiyyətlə, söndürürlər.

TCP/IP əlaqəsinin yaradılması zamanı 3 mərhələli prosesdə yanlış formatlı paket göndərərək serverin yarımçıq sessiyalar siyahısının doldurulmasının da qarşısı alınmışdır. Əvvəllər TCP/IP əlaqəsinin yaradılması üçün 3 mərhələli prosesin hər bir addımının həyata keçirilməsi üçün sonsuz qədər gözlənilirdi. İndi bu vaxt bir neçə saniyəyə endirilib. Əgər müəyyən bir zaman müddətində verilmiş əlaqənin yaradılması üçün növbəti paketlər gəlməsə, həmin sessiya avtomatik olaraq bağlanır.

DDoS hücumları bütün digər hücum növlərinə nisbətən qarşısının alınması ən çətin hücum növüdür. Təəssüf ki, DDoS- hücumlardan mühafizənin universal metodları mövcud deyil. Bu hücumların qarşısını almaq üçün müxtəlif metodlar, alqoritmlər və proqram təminatları işlənmişdir. DoS-hücumlarla mübarizə tədbirlərini passiv və aktiv, həmçinin preventiv və reaktiv tədbirlərə bölmək olar.

Əsas müdafiə metodları aşağıdakılardır:

* + **Profilaktika.** DoS-hücum təşkil etməyə təhrik edən səbəblərin profilaktikası. Arzuolunmaz aktivliyi başlamağa imkan verən səbəblərin aradan qaldırılması (çox vaxt hücumlar şəxsi incikliyin, siyasi, dini fikir ayrılığının və s. nəticəsi olur) üçün tədbirlər görülür.
  + **Mümkün DDoS hücumlarının effektivliyinin azaldılması.** Bu məqsədlə şəbəkədə yükləmə balansının tənzimlənməsi (ing. Load Balancing), proksilərdən istifadə, giriş informasiyasının süzgəcdən keçirilməsi, DNS yazılarının bir neçə serverə bölüşdürülməsi və s. kimi işlər görülür.
  + **Blackhole.** DDoS-hücumların qarşısını almaq üçün operatorlar BlackHole (“qara deşik”) texnologiyasından istifadə edirlər, bu zaman kliyentin ünvan fəzasında hücum edilən ünvanlar operatorun şəbəkəsində tam bloklanır (bağlanır). Bu metodu da tam uğurlu saymaq olmaz, çünki hücum trafiki ilə yanaşı “xoşniyyətli” paketlər də atılır. Bədniyyətli faktiki olaraq operatorun köməyi ilə öz əsas məqsədinə çatır – hücum edilən resursa giriş bağlanır. Bundan başqa, BlackHole metodunda marşrutlama getdikcə daha incə olan müasir hücumlarla mübarizə üçün optimallaşdırılmayıb.
  + **Filtrasiya.** Filtrasiya və blackhole metodlarının effektivliyi hücum hədəfinə yaxınlaşdıqca azalır və hücumun mənbəyinə yaxınlaşdıqca artır.
  + **Boşluqların aradan qaldırılması.** Flood tipli hücumlara qarşı işləmir, bu hücumlarda «boşluq» bu və ya digər resursun məhdud olmasıdır.
  + **Resursların artırılması.** İzafi resursların tətbiqi – yükün istənilən pik artımı ilə bacaran əlavə buraxma zolağının və ya ehtiyat şəbəkə qovşaqlarının alınması iqtisadi cəhətdən həmişə özünü doğrultmur. Bədniyyətliyə bu əlavə resursları tükətmək üçün yalnız hücumun miqyasını artırmaq gərəkdir.
  + **Paylanma.** Paylanmış və ehtiyat (təkrarlanmış) sistemlərin qurulması, məsələn, bir-birindən asılı olmayan bir neçə serverin və güzgü saytın istifadə edilməsi. Onlar hücum səbəbindən bəzi elementləri əlyetər olmadıqda belə, istifadəçilərə xidməti davam etdirirlər.
  + **Yayınma.** Hücumların bilavasitə hədəflərinin (domen-adının və ya IP-ünvanın) digər resurslardan kənara

aparılması, bilavasitə hədəflə birlikdə onlar da çox zaman təsirə məruz qalırlar.

**Aktiv cavab tədbirləri.** Hücumun mənbələrinə, təşkilatçısına və ya idarəetmə mərkəzinə həm texniki, həm də təşkilati-hüquqi xarakterli təsir edilməsi.

***22) OWASP***

OWASP konsorsiumunun təklif etdiyi boşluqlar klassifikatoru daha məşhurdur. Aşağıda bu klassifikasiya haqqında qısa məlumat verilir. “*OWASP Top 10 Web Application Security Risks 2021*” siyahısına aşağıdakı 10 boşluq sinfi daxildir. Bu boşluqların qısa izahına baxaq.

**A01:2021- Sındırılmış girişə nəzarət** (Broken Access Control) – sındırılmış girişə nəzarət problemləri girişə nəzarət elementləri olmadıqda və ya müvafiq şəkildə reallaşdırılmadıqda meydana çıxır. Giriş nəzarət siyasəti elə tətbiq edir ki, istifadəçilər nəzərdə tutulan icazələrdən kənar hərəkət edə bilməsinlər. Girişə nəzarət səhvləri, adətən, informasiyanın icazəsiz əldə edilməsinə, verilənlənlərin modifikasiyasına və ya məhv edilməsinə, həmçinin istifadəçinin hüquqlarından kənara çıxan biznes funksiyalarının yerinə yetirilməsinə gətirib çıxarır.

**A02:2021- Kriptoqrafik xətalar** (Cryptographic Failure) – kriptoqrafiya həm ötürülən, həm də diskdə saxlanan verilənlərin təhlükəsizliyini təmin etmək üçün geniş tətbiq edilir və xətaların siyahısı xeyli genişdir. Məsələn, köhnə və ya zəif kriptoqrafik alqoritmlər və protokollar istifadə edilir (defolt olaraq və ya köhnə kodlarda); defolt kriptoqrafik açarlar və ya zəif kriptoqrafik açarlar generasiya edilir və təkrar istifadə edilir; açar menecmenti düzgün qurulmur; server sertifikatı və etimad zənciri düzgün verifikasiya olunmur və s.

**A03:2021- İnyeksiya (Injection)** – SQL, NoSQL, ƏS, LDAP, ORM (Object Relational Mapping), EL (Expression Language) və ya OGNL (Object Graph Navigation Library) inyeksiyaları yoxlanmamış verilənləri komanda və ya sorğunun hissəsi kimi interpretatora göndərildikdə baş verir. Bədniyyətlinin ziyankar verilənləri interpretatoru arzuolunmaz komandaları yerinə yetirməyə və icazəsiz məlumatlara girməyə məcbur edə bilər.

**A04:2021- Təhlükəsiz olmayan layihələndirmə** (Insecure Design) – müxtəlif zəif cəhətləri təmsil edən və “nəzarət elementinin olmayan və ya səmərəsiz dizaynı” kimi ifadə edilən geniş kateqoriyadır. Təhlükəsiz olmayan dizayn bütün digər Top 10 risk kateqoriyalarının mənbəyi deyil. Təhlükəsiz olmayan layihələndirmə ilə təhlükəsiz olmayan reallaşdırma arasında fərq var. Təhlükəsiz olmayan dizaynın yoxluğu – nəzarətin yoxluğudur. Məsələn, konfidensial verilənləri şifrləməli olan kod təsəvvür edin, lakin şifrləmə metodu yoxdur. Nəzatət elementinin səmərəsiz dizaynı – təhdid reallaşa bilər, lakin domen (biznes) məntiqinin yetərsiz yoxlanması hərəkıətə mane olur. Məsələn, biznes- məntiq pandemiya ilə əlaqədar vergi güzəştlərini gəlir kateqoriyaları əsasında emal etməlidir, lakin bütün giriş verilənlərinin düzgün imzalanmasını yoxlamır və nəzərdə tutulandan daha geniş vergi güzəştləri təmin edir.

**A05:2021-Təhlükəsizliyin səhv konfiqurasiyası** (Security Misconfiguration) – yaxşı təhlükəsizlik tətbiqi proqramlar, tətbiqi proqram serverləri, ver-serverlər, verilənlər bazası serverləri və platformalar üçün təhlükəsiz konfiqurasiyanın müəyyən edilməsini və tətbiq edilməsini tələb edir.

**A06:2021-Müdafiəsiz və köhnə komponentlər** (Vulnerable and Outdated Components) – bura birbaşa istifadə edilən, həmçinin iç-içə asılılıqları olan komponentlər daxildir. Proqram təminatında boşluqlar ola bilər, dəstəklənməyə bilər və ya köhnəlmiş ola bilər. Bura ƏS, veb-server/tətbiqlər serveri, verilənlər bazasını idarəetmə sistemləri (VBİS), tətbiqlər, API və bütün komponentlər, icra mühiti və kitabxanalar daxildir.

**A07:2021-İdentifikasiya və autentifikasiya səhvləri** (Identification and Authentication Failures) – tətbiqi proqramlarda autentifikasiyanın idarə edilməsi ilə əlaqəli funksiyalar çox zaman düzgün reallaşdırılmırlar və bədniyyətliyə parolları, açarları, sessiya tokenlərini əldə etməyə imkan verirlər.

**A08:2021- Proqram təminatı və verilənlərin tamlığı səhvləri** (Software and Data Integrity Failures) – Proqram təminatı və verilənlərin tamlığının pozulması müvafiq müdafiənin olmadığı proqram kodu və infrastruktur ilə əlaqəlidir. Buna misal tətbiqi proqramların plaqinləri, kitabxanaları və modulları etibar edilməyən mənbələrdən yüklədiyi hallar ola bilər. Belə mənbələr icazəsiz girişə, zərərli kodlara və kompüter sisteminin sındırılmasına gətirib çıxara bilər. Hazırda bir çox sistemdə avtomatik yenilənmə funksiyaları vardır, bu zaman yenilənmələri tamlığı yetərincə yoxlamadan yükləyirlər və əvvəl etimad edilmiş tətbiqi proqramı yeniləyirlər. Bədniyyətlilər, yayılmaq və bütün qurğularda quraşdırılmaq üçün öz yenilənmələrini yerləşdirə bilərlər.

**A09:2021-Təhlükəsizliyin protokollaşdırılması və monitorinqi səhvləri** (Security Logging and Monitoring Failures) – bu səhvlər səbəbindən birbaşa yarana biləcək boşluq yoxdur, lakin ümumilikdə, protokollaşdırma və monitorinq kifayət qədər kritikdir və onların olmaması və ya səhvləri görünürlüyə, insidentlər barədə xəbərdarlığa və məhkəmə ekspertizasına birbaşa təsir göstərə bilər. Beləliklə, loqları toplamaq və hər hansı nasazlıq və ya səhv baş verəndə xəbərdarlıq etmək üçün funksional protokollaşdırma və monitorinq sisteminə sahib olmaq olduqca vacibdir, əks halda bunlar uzun müddət diqqətdən kənarda qala və daha çox zərər verə bilər.

**A10:2021-Server-tərəf sorğunun saxtalaşdırılması** (STSS, Server-Side Request Forgery) – STSS səhvləri veb-tətbiq istifadəçinin təqdim etdiyi URL-ünvanı yoxlamadan veb resursu əldə etdikdə baş verir. Bu, bədniyyətliyə imkan verir ki, veb-tətbiqi yaradaılmış sorğunu nəzərdə tutulmamış təyinat yerinə göndərməyə məcbur etsin. Müasir veb-tətbiqlər istifadəçilərə rahat funksiyalar təqdim edirlər, buna görə URL-ünvanın təqdim edilməsi geniş yayılmış senaridir. Nəticədə STSS insidentləri çoxalır. Bundan başqa, STSS-in ciddiliyi bulud xidmətləri və arxitekturaların mürəkkəbliyi səbəblərindən də artır.

## ***23)Veb sistemlərə hücumların əsas sinifləri***

**Autentifikasiya hücumları**

Autentifikasiya hücumları veb-proqramın istifadə etdiyi istifadəçinin, xidmətin və ya proqramın identifikatorunu yoxlama metodlarına yönəlir. Autentifikasiya üç mexanizmdən (faktordan) ən azı birini istifadə edir: "malik olduğu nəsə", "bildiyi nəsə" və ya "olduğu nəsə". Aşağıda veb-serverin autentifikasiyasını reallaşdıran mexanizmlərində olan boşluqların istismarına yönəlmiş iki hücum təsvir edilir.

**Kobud güc:** istifadəçinin adını, parolunu, kredit kartının nömrəsini, kriptoqrafik açarı və s. tapmaq üçün istifadə edilən avtomatlaşdırılmış sınaq-səhv üsuludur. Sistemlərin bir çoxu zəif parollardan və şifrləmə açarlarından istifadə etməyə imkan verir və istifadəçilər çox vaxt asan tapılan və ya lüğətlərdə olan parollar seçirlər.

Çox vaxt veb-serverdə autentifikasiya istifadəçidən parolu yadda saxlamağı tələb edir. Vaxt keçdikcə parol unudulur. Vəziyyət onunla mürəkkəbləşir ki, istifadəçinin sistemdə yadda saxlamalı olduğu parolların sayı çoxalır. Beləliklə, parolu bərpaetmə funksiyası veb-serverlərin təqdim etdiyi servislərin vacib tərkib hissəsi olur.

**Parol bərpasının zəif yoxlanması (Weak Password Recovery Validation):** bu zəiflik veb-server hücum edənə digər istifadəçilərin parollarını icazəsiz əldə etməyə, modifikasiya və ya bərpa etməyə imkan verdikdə meydana çıxır.

## Avtorizasiya hücumları

Avtorizasiya hücumları istifadəçi, xidmət və ya proqramın əməliyyatları yerinə yetirmək üçün zəruri icazəyə malik olmasını yoxlamaq üçün veb-serverlərin istifadə etdiyi metodlara qarşı yönəlmiş hücumlardır. Veb-saytların çoxu müəyyən kontentə və ya proqramın funksiyalarına giriş əldə etməyi yalnız müəyyən istifadəçilərə icazə verir, digər

istifadəçilərə giriş məhdudlaşdırılır. Bədniyyətli müxtəlif üsullardan istifadə edərək öz imtiyazlarını artıra və mühafizə olunan resurslara giriş əldə edə bilər.

## Kliyentə hücumlar

**Kliyentə hücumlar (Client-side Attacks)** dedikdə, də veb-server istifadəçilərinə hücumlar nəzərdə tutulur. Sayta baş çəkdikdə istifadəçi ilə server arasında həm texnoloji, həm də psixoloji aspektlərdə inam münasibətləri yaranır. İstifadəçi gözləyir ki, sayt ona qanuni məzmunu təqdim edəcək. Bundan başqa, istifadəçi sayt tərəfdən hücum gözləmir. Bu inamı istismar edərək bədniyyətli serverin istifadəçilərinə hücum etmək üçün müxtəlif metodlardan istifadə edə bilər.

**Kontentin saxtalaşdırılması (Content Spoofing):** bədəməl bu hücumdan istifadə edərək istifadəçini səhifənin kənar mənbədən ötürüldüyünə deyil, veb-server tərəfindən generasiya edildiyinə inanmağa məcbur edir.

**Saytlararası ssenarilər (Cross-site Scripting, XSS):** Cross-site Scripting zəifliyinin olması hücum edənə istifadəçinin brauzerinə göndəriləcək icra olunan kodu serverə ötürməyə imkan verir. Bu kod adətən HTML/JavaScript dillərində yaradılır, ancaq VBScript, ActiveX, Java, Flash və ya brauzerin dəstəklədiyi digər texnologiyalar da istifadə edilə bilər. Ötürülmüş kod zəif serverin təhlükəsizlik kontekstində (və ya təhlükəsizlik zonasında) icra olunur. Bu imtiyazdan istifadə edərək kod brauzerin köməyi ilə əlyetən vacib verilənləri oxumaq, dəyişdirmək və ya ötürmək imkanı qazanır. Hücum edilən istifadəçinin akkauntu nüfuzdan salın bilər (cookie-nin oğurlanması), onun brauzeri başqa serverə yönəldilə bilər və ya serverin məzmunu dəyişdirilə bilər. Yaxşı planlaşdırılmış hücumun nəticəsində bədniyyətli hücum edilən istifadəçinin adından saytın səhifələrinə baxmaq üçün hədəfin brauzerindən istifadə edə bilər. Bədniyyətli kodu

URL-də, sorğunun HTTP başlıqlarında (cookie, user-agent, refferer), formadakı sahələrin qiymətlərində və s. ötürə bilər.

**HTTP-sorğunun parçalanması (HTTP Response Splitting):** bu zəiflik istifadə edildikdə bədəməl serverə xüsusi şəkildə formalaşdırılmış sorğu göndərir ki, ona cavab hücum hədəfi tərəfindən iki müxtəlif cavab kimi interpretasiya edilir.

İkinci cavaba bədniyyətli tamamilə nəzarət edir, bu ona sererin cavabını saxtalaşdırmaq imkanı verir.

## Kodun icrası hücumları

Kodun icrası hücumları (Command Execution) veb-serverdə kodun yerinə yetirilməsinə yönəlmiş hücumları nəzərdə tutur. Bütün serverlər sorğuların emalı zamanı istifadəçilərin ötürdüyü verilənlərdən istifadə edirlər. Çox vaxt bu verilənlər dinamik məzmunun generasiyası üçün tətbiq edilən komandaların tərtib edilməsi zamanı istifadə edilir. Əgər yaradılma zamanı təhlükəsizlik tələbləri nəzərə alınmırsa, bədniyyətli yerinə yetirilən komandaları modifikasiya etmək imkanı əldə edir.

Kodun icrası hücumlarına buferin daşması, stekdən verilənlərin oxunması, prosesin yaddaşından sətirlərin oxunması, prosesin yaddaşına tam ədəd qiymətlərin yazılması, sətrı formatlaşdırma funksiyalarına hücumlar və ƏS komandalarının yerinə yetirilməsi ilə yanaşı, bir sıra inyeksiya hücumları da daxildir.

İnyeksiya hücumlarına LDAP operatorlarının inyeksiyası, SQL operatorlarının inyeksiyası, server ssenarilərinin inyeksiyası (SSI Injection), XPath operatorlarının inyeksiyası aid edilir.

## İnformasiyanın açıqlanması hücumları

İnformasiyanın açıqlanması (Information Disclosure) sinfinin hücumları veb-proqram haqqında əlavə informasiya əldə edilməsinə yönəlib. Bu boşluqlardan istifadə edərək bədniyyətli proqram təminatının istifadə edilən distributivlərini, kliyentin və serverin versiya nömrələrini və sazlanmış yamaqları müəyyən edə bilər. Digər hallarda sızmış informasiyada müvəqqəti faylların və ehtiyat surətlərin yeri ola bilər. Bir çox halda bu verilənlər istifadəçinin işi üçün tələb edilmir. Serverlərin əksəriyyəti böyük həcmdə verilənlərə giriş təqdim edir, lakin xidməti informasiyanın həcmini minimum etmək lazımdır. Proqram haqqında bədniyyətlidə nə qədər çox məlumat olsa, ona sistemi nüfuzdan salmaq bir o qədər asan olar.

Bu sinif hücumlara direktoriyanın indekslənməsi, veb-serverin/tətbiqi proqramın identifikasiyası, informasiyanın sızması, direktoriyalarda tərs yol, resursların proqnozlaşdırılan yerləşməsi hücumları daxildir.

## Məntiqi hücumlar

Məntiqi hücumlar (Logical Attacks) proqramın funksiyalarının və ya onun fəaliyyət məntiqinin istismarına yönəlib. Proqramın məntiqi müəyyən əməliyyatların yerinə yetirilməsi zamanı proqramın gözlənilən fəaliyyət prosesindən ibarətdir. Misal olaraq parolların bərpasını, uçot yazılarının qeydiyyatını, elektron kommersiya sistemlərində

tranzaksiyaları göstərmək olar. Proqram müəyyən məsələnin yerinə yetirilməsi üçün istifadəçidən bir neçə ardıcıl əməliyyatın düzgün yerinə yetirilməsini tələb edə bilər. Bədniyyətli bu mexanizmərdən yan keçə və ya öz məqsədləri üçün istifadə edə bilər.

Bu sinif hücumlara funksional imkanlardan sui-istifadə, xidmətdən imtina, avtomatlaşdırmaya yetərsiz əks-təsir, prosesin yetərsiz yoxlanması kimi hücumlar aid edilir.

## ***24)SQL inyeksiyanın növləri***

Hücumedənlər veb tətbiqin bazasından verilənləri silmək, əlavə etmək, dəyişmək və baxmaq üçün müxtəlif üsul və hiylələrdən istifadə edirlər. SQL inyeksiyasının istifadə olunan üsullara görə, əsasən, üç növü vardır.

* + In-band SQL inyeksiya
  + Out-of-band SQL inyeksiya
  + Blind (inferential) SQL inyeksiya

**In-band SQL inyeksiya.** Bədniyyətli eyni qoşulma kanalından istifadə edərək nəticələri əldə edir. Ümumi və sadə hücum hesab olunur. Növlər aşağıdakılardır:

* + **rror-based –** bədniyyətli bilərəkdən girişə VB xətalarına səbəb olan uyğunsuz verilənlər daxil edir.
  + **Systemdə yerləşmiş prosedur –** Bədniyyətli VB-in saxlanmış prosedurlarından istifadə edərək öz hücumlarını başladırlar.
  + **Qanunsuz (məntiqi cəhətdən səhv) sorğular –** Bədniyyətli qəsdən VB-a səhv sorğu göndərir və bu növbəti

hücumlar üçün faydalı nəticələr verir.

* + **UNİON -** Bədniyyətli tələb olunan sorğuya zərərli sorğu əlavə etmək üçün UNİON-dan istifadə edir.
  + **Tautologiya –** Bədniyyətlinin şərti OR funksiyasından autentikasiya üçün istifadə etməyinə əsaslanır. Burada

Where ifadəsi həmişə doğru olacaq.

**Out-of-band SQL inyeksiya.** Hücumedən serverlə əlaqədə olmalı və veb tətbiqin işlətdiyi serverin xüsusiyyətlərini əldə etməlidir. Buna görə də çətin hücum hesab olunur. Hücum üçün müxtəlif əlaqə kanalları istifadə edilir və nəticələr əldə olunur. Bazadan verilənləri almaq üçün HTTP və DNS sorğularından istifadə edir. Məsələn, Ms SQL Serverdə hücumedən tərəfindən idarə olunan serverə DNS sorğuları göndərmək üçün xp\_dirtree əmri istismar edilir. Oracle-da isə hücumçu HTTP sorğularını serverə göndərmək üçün utl\_http paketindən istifadə edə bilər.

**Blind (inferential) SQL inyeksiya.** Bədniyyətli sistemdən xəta mesajı almır. Bunun əvəzinə VB-a zərərli SQL sorğuları göndərib, true və ya false qiymətləri alaraq VB strukturunu müəyyən edir ki, bu da uzun vaxt tələb edir. Hücumedən veb tətbiqdən çıxarılan həqiqi nəticələri görə bilmədiyi üçün «kor hücum» adı verilmişdir. Bu hücum ya VB-dan verilənlərin məhv edilməsi, ya da kritik verilənlərə daxil olmaq üçün istifadə edilir. Bədniyyətli müxtəlif SQL ifadələrindən istifadə edərək true və ya false sorğuları göndərərək həssas verilənləri ələ keçirə bilər.

## ***25)SQL inyeksiyanın metodologiyası***

* + İnformasiya toplama və SQL inyeksiya boşluğunun aşkarlanması
  + SQL inyeksiya hücumunun başladılması

## Təkmilləşdirilmiş SQL inyeksiya

**İnformasiya toplama.** Bu mərhələdə hücumedən hədəf VB haqqında onun adı, versiyası, növü, istifadəçilər, çıxış mexanizmi, istifadəçilərin imtiyaz səviyyəsi kimi məlumatları əldə etməyə çalışır. VB-dan informasiya çıxarmaq üçün ekrana çıxan xəta mesajlarından istifadə edirlər. İnformasiya toplamaq üçün aşağıdakı addımlar atılmalıdır.

1. Veb tətbiqin VB Serverə qoşulmağını yoxlamaq.
2. Giriş sahələrinin, gizli sahələrin və post sorğularının siyahısını tərtib etmək.
3. Səhvlərin generasiyası üçün giriş verilənlərinə kodun yoluxdurulmasına cəhd.
4. Giriş sahəsində ədəd gözlənilən yerə simvol veriləni daxil etməyə cəhd.
5. İki və daha artıq **SELECT** ifadəsini birləşdirmək üçün **UNİON** operatorundan istifadə etmək.
6. Xəta mesajlarından informasiya toplamaq.

**SQL inyeksiya aşkarlama.** Hücumedən kifayət qədər məlumat topladıqdan sonra veb tətbiqdə SQL inyeksiya boşluğunu aşkar etməyə çalışır. Bunun üçün veb tətbiqdəki bütün giriş sahələri, gizli sahələr və post sorğularını siyahıya alır və səhv generasiya etmək üçün giriş nöqtələrinə zərərli kodu inyeksiya etməyə çalışır.

**Verilənlərin girilmə sahəsinin müəyyən edilməsi.** Hücumedən giriş sahələri, gizli sahələr və kukiləri müəyyən etmək üçün veb Get və Post sorğularını analiz edir. Bunun üçün Tamper data, Burp Suite kimi alətlərdən istifadə edilir.

**Təkmilləşdirilmiş SQL inyeksiya.** Hücumedən troyan və ya keyloqerlər quraşdıraraq daxil olduğu hədəf şəbəkəni daha geniş ələ keçirə bilər. İnventarlaşdırma üçün, məsələn, MySQL-də mysql.user, mysql.host, mysql.db kimi VB obyektləri istifadə olunur.

## ***26)SQL inyeksiya alətləri***

1. BSQL Hacker
2. SQLMap
3. SQLninja
4. Safe3 SQL injector
5. SQLSus
6. SQL power injector
7. The Mole
8. jSQL injection
9. BBQSQL
10. Whitewidow

## ***27)SQL inyeksiyaya qarşı əks-tədbirlər***

Veb-tətbiqlərin SQL-inyeksiyadan müdafiəsi üzrə bəzi tövsiyələr vermək olar:

* + girişi ayrıca emal edin və sorğunu təhlükəsiz qiymətlərdən formalaşdırın;
  + “ağ” siyahılar yaradın;
  + yenilənmələri müntəzəm yerləşdirin;
  + istifadə edilməyən funksionalları silin;
  + cədvəl, sütun və bazaların adlarına konkret qiymətlər verin;
  + veb-tətbiqlərin təhlükəsizliyini periodik olaraq əllə və avtomatlaşdırılmış vasitələrlə analiz edin (məsələn, Wapiti)
  + veb-tətbiqlərin mühafizə vasitələrini istifadə edin (WAF)