Etik hakerlər və nüfuzetmə testləri üçün alətlər

Tural Yunusov
AMEA İnformasiya Texnologiyaları İnstitutu
turaly@mail.ru

***Xülasə*— Məqalədə kompüter şəbəkələrinin təhlükəsizliyi, kiber hücum metodları, kiber hücum vektorları, hakerlər, haker növləri və məqsədləri, etik haker, etik haker bacarıqları, Kali Linux əməliyyat sistemi, kali test alətləri olan websploit, nmap, webspoit və istifadəsi, nüfuzetmə test metodologiyası, praktiki olaraq kompüter şəbəkəsi üzərində nüfuzetmə testi haqqında informasiya verilmişdir.**

Açar sözlər— təhlükəsizliyin qiymətləndirilməsi, haker, etik haker, CEH, Kali Linux, Nikto, Nmap, webspoit, test metodologiyaları, OWASP, OSSTMM, ISSAF.

I. GİRİŞ

Şirkətlərdə, bütün kompüterlər şəbəkə üzərindən bir-biri ilə bağlıdırlar və bu şəbəkə vasitəsi ilə İnternetə çıxış əldə edə bilirlər. İnternetə çıxışın əldə edilməsi, kompüter şəbəkələrində böyük təhlükəsizlik problemləri yaradır. Hakerlər İnternet üzrərindən kompüterlərə girə bilir və bununla kompüter şəbəkələrində olan digər kompüterlərə giriş əldə edə bilirlər. Son illərdə hakerlər tərəfindən edilən məşhur hücumlardan bir neçəsi nümunə gətirə bilərik.

Ebay dünyada məşhur online alış-veriş saytıdır. Bu saytda günlük milyonlarla insan qeydiyyatdan keçir və alışlar edirlər. 2014-cü ildə Ebay–a edilən hücum nəticəsində 145 milyon istifadəçinin şifrələri, email ünvanları, doğum tarixləri və şəxsi məlumatları oğurlanmışdı. Google Play, Google şirkətinin yaratdığı android əməliyyat sistemlərində olan aplikasiya yükləmə bazasdır. Google Play bazasında 2014-cü ildə Türk hakeri tərəfindən sistemdə nasazlıq yaradılaraq sistemin əlyetənliyinə xələl yetirildi, haker hazırladığı aplikasiyanı android verilən bazasına yükləyərək, aplikasiya vasitəsi ilə boşluqları test etdi və bu hadisə google play-in xidmətdən imtinası ilə nəticələndi. 2015-ci ildə haker qrupu Sony şirkətinə hücum edərək böyük maddi zərər vurdular. Sony şirkətinin məlumatına əsasən hakerlər korporativ şəbəkəyə girərək, gizli biznes sənədlərini oğurlayıb, şəbəkədə olan bütün kompüterləri nasaz vəziyyətə gətirərək şirkətə 15 milyon dollar maddi ziyan vurublar. Breachlevelindex.com saytına əsasən son 2017-ci ildə dünyada 1.901.866.611 çox məlumat itirilir və ya oğurlanır. Bu hər gün üçün 10.507.550 məlumat, hər saat üçün 437.815 məlumat, hər dəqiqə üçün 7297 məlumat, hər saniyə üçün 122 sayda məlumatın itməsi və ya oğurlanması deməkdir [1]. Bu məlumatların 56.59% -i pərakəndə, 9.63% -i texnologiya, 5.13% -i təhsil, 4.23% -i hökümət və 20.55% maliyyə sahəsini əhatə edir.

II. KİBER HÜCUM METODLARI

Bu gün çox hücum metodları mövcuddur və texnologiyanın inkişafı bu tip metodlarında inkişafına səbəb olmuşdur. Hakerlər əsasən aşağıdakı hücum metodlarını istifadə edərək istədiklərini əldə etməyə çalışırlar.

Zero-day Attack (0-gün) – əsasən bir proqramda boşluğun aşkar etdikdən gün və ya zəyiflik tapıldıqdan sonra proqram yaradıcı şirkət tərəfindən yeniləmə tətbiq edilənə qədər istifadə edilən boşluq növüdür [2].

Daisy Chaining – bir kompüter şəbəkəsinə və ya kompüterə daxil olmaq imakanını əldə edərək digər kompüter şəbəkələrinə və ya kompüterlərinə daxil olmaqdır .

Vulnerability – kompüter şəbəkələrində olan sistemlərin təhlükəsizliyinə olan gözlənilməz hadisəyə səbəb ola biləcək mövcud zəiflik, struktur dizaynında və ya tətbiqdə olan səhv [3].

Exploit – ingilis sözü olub “nəyisə öz xeyrinə istifadə etmək” mənası daşıyır. Exploit proqram təminatının, məlumat yığınının və ya əmrlər sətrinin bir hissəsi olub proqram səhvlərindən və boşluqlardan istifadə edərək kompüter proqramlarında, texnikasında və ya hər hansı elektron cihazlarda gözlənilməz hadisələrə səbəb olur [4].

Payload – kompüter təhlükəsizliyində *payload,* hücumu həyata keçirən soxulcanlar və ya viruslar kimi ziyanverici proramların bir hissəsi olub informasiya silmə, spam göndərmə və şifrləmə məqsədi ilə istifadə edilir [5].

Hack value – Hackerlər arasında hücum edəcəkləri obyektin vacibiliyini və ya maraqlı olduğunu göstərmək üçün bir dəyərdir (rəqəm).

Doxing – (dox, dokument sözünün qısaldılmasıdır), doxxing və ya docxing İnternet əsasında fərdi və ya təşkilat haqqında müəyyənləşdirilə bilən informasiyanın (xüsusilə şəxsi məlumatları) tədqiq edilməsidir [6].

Bot – istifadəçi kompüterində gizli quraşdırılan və yoluxmuş kompüterin resurslarından istifadəçinin xəbəri olmadan istifadə etməklə, müəyyən əməlləri yerinə yetirməyə imkan verən uzaqdan idarə oluna bilən zərərli proqramdır [7].

III. KİBER HÜCUM VEKTORLARI

Texnologiyanın inkişafı ilə əlaqədar yeni texnoloji sahələr yaranmaqdadır və bu inkişaf yeni hücum vektorlarının yaranmasınada səbəb olmuşdur, hazırda hakerlər tərəfindən geniş şəkildə istifadə olunan hucum vektorları aşağıdakı kimidir.

Cloud Texnologiyası təhdidləri üzrə - cloud texnologiyası, təşkilatların və müştərilərin həssas məlumatlarının saxlanıldığı və İnformasiya texnologiyaları (İT) imkanlarının, tələb əsasında verilməsidir.

DOI: 10.25045/NCInfoSec.2017.21

Qabaqcıl inadkar təhdidlər üzrə – bu hücum növünün əsas hədəfi istifadəçinin xəbəri olmadan seçilmiş hədəf sistemdən informasiyaların oğurlanmasıdır.

Virus və Soxulcanlar ilə - Virus proqramları və soxulcanlar texniki vasitələrlə bir kompüterdən digər kompüterə keçməyə cəhd edən, verilənlərin korlanmasına (dəyişdirilməsi və ya silinməsi) gətirən və ya istifadəçinin işinə mane olan, digər proqramlarda gizlənmiş kiçik həcmli proqramlardır

Mobil təhdidlər üzrə – iş və şəxsi məqsədlər üçün mobil telefonlara olan tələbatın artması və nisbətən daha az təhlükəsizlik nəzarəti ilə əlaqədar hakerlərin marağına səbəb olmuşdur [8].

Botnet – “robot” və “network” sözlərinin birləşməsindən yaranmışdır, xüsusi bot proqramlarla yoluxmuş kompüterlərin şəbəkəsini bildirir. Botnet şəbəkələrini çox vaxt verilmiş əmrləri avtomatik yerinə yetirən zombi-kompüter şəbəkələri də adlandırırlar [7].

Daxili hücum ilə – şəbəkəyə giriş imkanı olan şəxs (insider) tərəfindən korporativ şəbəkə və ya bir kompüterdə həyata keçirilən hücumdur [9].

IV. ETİK HAKERLƏR HAQQINDA

"Haker" (Hacker) sözü öz ilkin mənasında İT-nin yüksək inkişafı nəticəsində Massaçusets Texnologiya İnstitutunda 1960-cı illərdə meydana gəlmişdir. Termin meydana çıxdığı zaman heç də kütləvi şəkildə istifadə olunmamışdır. Buna səbəb isə kompüterlərin geniş yayılmaması idi. Termin ilkin olaraq lokal söz kimi işlənmişdir və mənası hər hansısa bir problemin sadə, ancaq kobud şəkildə həlli tələbələrin hədsiz hiyləgərlik işlətmələri (əksər halda bu şəkildə qaydaları pozanları məhz haker adlandırmışlar) demək idi. İlkin olaraq “to hack” (sındırmaq, kəsmək) kimi istifadə olunmağa başlamışdır. Bu o mənada işlədilir ki, hər-hansısa bir proqrama "ayaqüstü" düzəliş edilsin. Tədricən “to hack” hacker sözü kimi istifadə edilməyə başlandı. Əsl haker kiminsə proqramındakı səhvi tapıb deməklə yanaşı onun həlli üsulunu verməyi çox lazımlı hesab edirdi. "Haker" sözü məhz buradan törəmişdir [10].

Kömpüter şəbəkələrində isə haker o şəxsdir ki, şəbəkənin elementlərinə və kompüterə girişə nəzarət edir, lazım gəldikdə onları məhdudlaşdırır. Bu şəxslər fərdi şəkildə şəbəkələrin normal fəaliyyətini nizamlayırlar. Bu cür hakerlər həmçinin İnternet vasitəsilə açılmaz kodları sındırmaqla və kiber müharibələrin iştirakçısı kimi də iştirak edir. Hakerlərin bu cür fəaliyyət cəmiyyətdə digər fəaliyyətlərə nisbətən daha dərin iz buraxır.

İT sahəsində hakerlərin məqsədini göstərmək üçün ağ şlyapalı və ya qara şlyapalı terminindən istifadə edilir. Bu termin məşhur amerika mədəniyyətinin qərb janrıdır və burada ağ şlyapalı kavboylar qəhrəmanlığı, qara şlyapalı kavboylar isə cinayətkarlığı, pisliyi təbliğ edir [11].

Bu gün hakerləri gördükləri iş və məqsədləri daxilində aşağıdakı kateqoriyalara bölmək olar [12]:

Qara şlyapalı (Balack Hat) – Qara şlyapalı hakerlar əsasən qeyri qanuni olaraq özlərinə aid olmayan və səlahiyyətlərinə aid olmayan sistemlərə daxil olub müxtəlif tipli zərərli işlərlə məşğul olurlar.

White hat (Ağ şlyapalı) - Ağ şlyapalı haker qara şlyapalı hakerdən fərqli olaraq təhlükəsizlik üçün işləyirlər və məsul olduqları sistemlərə dəyə biləcək zərərlərin qarşısını almaq və sistemin özünü müdafiə qabiliyyətini artırmaqla məşğul olurlar.

Boz şlyapalı (Gray hat) – boz şlyapalı hakerlər müxtəlif vaxtlarda həm hücum, həm də müdafiə üçün işləyən şəxslərdir.

Suicide Hackers – Fərdi olaraq əsas fikri kritik infrastrukturlarda nasazlıq yaratmaq olan və hər hansı növ cəzadan qorxmayan şəxslərdir.

Script Kiddies – Haker bacarıqları olmayan və real hakerlər tərəfindən yaradılmış proqramlardan, alətlərdən və skriptlərdən istifadə edən şəxslərdir.

Kiber terorist (Cyber Terrorist) – Fərdi şəkildə geniş bacarıqlara malik olub, dini və siyasi motivasiya olunaraq, kompüter şəbəkələrində böyük zərərə səbəb olan şəxslərdir.

Dövlətə işləyən hakerlər (State Sponsored Hackers) – dövlətə işləyən və gizli məlumatlar əldə etmək üçün digər dövlətlərin informasiya sistemlərinə girən və ya zərər verməkk üçün istifadə edilən şəxslərdir.

Haktivist – Hakinq yoluyla siyasi gündəmi təşviq edən, xüsusilə veb saytları sındıran və ya silən şəxslərdir.

Etik hakerlər təhlükəsizlik sistemləri haqqında sahib olduqları bilik və təcrübələrini məsul olduqları sistemlərin zəifliklərini tapmaq və boşluqlarını bağlamaq üçün istifadə edirlər. Onlar kompüter şəbəkələrinə ediləcək hücumlara qarşı hansı tədbirləri yerinə yetirəcəyini, təhlükə yarandıqda və hətta təhlükə yaranmamışdan qabaq şəbəkələr arası ekranın yaradılması ilə atılacaq addımları və prosedurları planlaşdıran, sistemə girmək istəyən hakerlərin qarşısına almaq vəzifəsini yerinə yetirirlər [13].

CEH (Certified Ethical Hacker) sertifikatlı etik haker şəbəkə təhlükəsizliyi sahəsində ixtisaslaşmış mütəxəssisdir, hakerlərin istifadə etdiyi bilik və alətlərdən istifadə edir, hədəf sistemlərində zəif yerləri və boşluqları necə axtarmağı bacarır. CEHv9 sertifikat imtahanı şəbəkə protokollarının, əməliyyat sistemlərinin, tətbiqi proqramların boşluqları, troyanlar, viruslar, rutkitlər, informasiyanın toplanması, şəbəkənin axtarılması və resursların inventarlaşdırılması, veb-serverlərin, simsiz şəbəkələrin sındırılması, informasiya təhlükəsizliyi vasitələrinin aldadılması, nüfuzetmə testləri, DoS hücumların, SQL-inyeksiya hücumlarının həyata keçirilməsi, seansların ələ keçirilməsi və s. kimi sahələri əhatə edir [14].

Etik hakerdən tələb olunuan texniki bacarıqlar aşağıdakılardır:

- Əsas əməliyyyat sistemləri, windows, unix, linux və makintoş üzrə dərin biliklərə malik olmalıdır;
- Şəbəkə konsepsiyaları, texnologiyaları, mövcud texnikaları və proqramları üzrə dərin biliklərə malik olmalıdır;
- Texniki sahələrdə peşəkar kompüter eksperti olmalıdır;
- Təhlükəsizlik sahəsində və mövcud problemlər üzrə biliklərə malik olmalıdır;
- Mürəkkəb hücumlar üçün “yüksək texniki” bacarığa malik olmalıdır;

Etik hakerin qeyri-texniki bacarıqlarından bəziləri aşağıdakılardır:

- Yeni texnologiyaları öyrənmə və uyğunlaşma bacarığı;
- Yüksək iş etikası, problem həll etmə və ünsiyyət bacarığı;
- Təşkilatın təhlükəsizlik siyasətinə riaət etməli;
- Standartlardan və qanunlardan xəbərdar olmalıdır.

V. KALİ LİNUX ƏMƏLİYYAT SİSTEMİ

Kali Linux Debian əsaslı təhlükəsizliyin yoxlanılması üçün nəzərdə tutulmuş əməliyyat sistemidir. Kali Linux BackTrack tərtibatçıları olan Offensive Security tərəfindən 2013-cü ildə yaradılmışdır. Hal-hazırda da dəstəklənməkdədir. BackTrack-dəki bütün alətlər və sonradan əlavə olunanlarla birlikdə Kali Linux-da işləmək üçün 600-dən çox alət var.

Offensive Security komandası 2007-ci ildə yaradılıb. Komanda üzvləri hücum sistemləri sahəsində geniş təcrübəsi olan təhlükəsizlik mütəxəssislərindən ibarətdir. Onlar hücum ssitemləri ilə bağlı informasiyaları, təlimləri, pulsuz alətləri bölüşürlər. Kali linux əməliyyat sisteminin yaradıcıları aşağıdakılardır.

Mati Aharoni (muts) Kali əməliyyat sisteminin əsas proqramçısı, təlimçisi və Offesive Security-nin yaradıcısıdır. 10 illik peşəkər nüfuzetmə testeri və təhlükəsizlik sahəsində kritik boşluqları aşkarlamışdır:

Devon Kearns (dookie) Offensive Security təlimatçısı, Kali Linux proqramçısı, Exploit bazası inzibatçısı, Metasploit (test hücumu üçün istifadə edilən alət) proyektinin ortaq yaradıcısıdır.

Raphaël Hertzog (buxy) təcrübəli Debian proqramçısı və məsləhətçi, çox tanınan “Debian Administrator’s Handbook” kitabının müəllifidir.

Kali Linux əməliyyat sistemində verilənlər bazasının qiymətləndirilməsi, informasiyanın toplanması, exploit alətləri, skanerlər, şifrələrə hücum, stres test, snifinq, simsiz şəbəkələrə hücumlar, texnikanın hakinqi, backtrack xidmətləri və “reverse engineering” kateqoriyalar üzrə yoxlamalar aparmaq mümkündür [15].

VI. NÜFUZETMƏ TESTLƏRİNİN METODOLOGİYASI

Kompüter şəbəkələrinin təhlükəsizliyini qiymətləndirmək üçün müxtəlif üsullar mövcuddur. Bunlar kompüter şəbəkələrinin təhlükəsizliyinin auditi, boşluqlarıının qiymətləndirilməsi və nüfuzetmə testləridir. Onlar arasındakı fərqlər aşağıdakı kimi göstərmək olar:

Təhlükəsizliyin auditi – təşkilatda qəbul edilmiş standart, təhlükəsizlik siyasəti və proseduralarının yerinə yetirilməsinin uyğunluğunu yoxlayır [16].

Boşluqların qiymətləndirilməsi - əsas hədəfi informasiya sistemlərində boşluqların tapılmasına istiqamətlənmişdir lakin boşluqlardan istifadə zamanı dəyə biləcək hər hansı zərərin indeksi göstərilmir.

Nüfuzetmə testləri – kompüter şəbəkələrinin təhlükəsizliyinin qiymətləndirilməsinə metadoloji yanaşmadır, təhlükəsizliyin auditini və boşluqarın qiymətləndirilməsini əhatə edərək hakerin müvəffəqiyyətlə boşluqlardan istifadə edərək sistemə vura biləcəyi zərəri nümayiş etdirir.

Nüfuzetmə testləri zamanı aşağıdakı test metodologiyalarından istifadə edilir [17]:

OWASP – The Open Web Application Security Project (Açıq veb aplikasiya təhlükəsizlik layihəsi) açıq mənbə kodlu layihədir və veb aplikasiyalarının təhlükəsizliyi üçün proqram alətlərini inkişaf etdirir, proqram aplikasiyaları və məlumat bazasına əsaslanan sənədlərlə köməklik göstərir.

OSSTMM – Open Source Security Testing Methodology Manual (Açıq mənbə kodlu təhlükəsizlik test metadologiyası) – bu metadologiya yüksək səviyyəli təhlükəsizlik testləri aparır: məlumatların idarə edilməsi, fırıldaqçılıq və sosial mühəndisliyə nəzarət səviyyəsi, kompüter şəbəkələri, simsiz qurğular, fiziki təhlükəsizliyə nəzarət və müxtəlif təhlükəsizlik proseslərini əhatə edir.

ISSAF – Information Systems Security Assessment, Framework– İnformasiya sistemlərinin təhlükəsizliyinin qiymətləndirilməsi mühiti – açıq mənbə kodlu lyihədir və əsas hədəfi peşəkarlara köməklik göstərməkdir.

EX-Council LPT Methodology – LPT metodologiyası informasiya sistemlərinin təhlükəsizlik auditini aparan və sənaye sistemlərində qəbul edilmiş əsas metadologiyadır.

VII. VEB SAYTLARIN NÜFUZETMƏ TESTİ

İstifadə edəcəyimiz əməliyyat sistemi Kali linux, alətlət isə NMAP, NİKTO və WebSploit olacaq. İlk olaraq domenin hansı İP ünvana bağlı olduğunu aydınlaşdıraq. Bunun üçün domenə ping əmri verməyimiz kifayət edir.(Şək.1)

```
root@kali:~# ping domeyn.com
PING domeyn.com (69.172.201.153) 56(84) bytes of data.
```

Şəkil 1. İP ünvanın müəyyənləşdirilməsi

Şəkil1 – dən də göründüyü kimi domeyn.com saytının İP ünvanı müəyyənləşdirildi. Bu İP ünvanına brauzer üzərindən giriş etsək əsasən aşağıdakı kimi səhifə açılacaq.(Şək.2)

Şəkil 2. “LAMP stack” Veb platforması

Şəkil 2 – dən göründüyü kimi açıq mənbə kodlu “LAMP stack” veb platforması istifadə edilir. Bu Linux, Apache, MySQL, and PHP/Python/Perl dəstəkləyir. Göstərilmiş platforma SSL sertifikatı dəstəkləsədə bu ünvanda SSL quraşdırılmayıb. SSL kompüter şəbəkələri üzərindən

informasiya ötürülməsi zamanı təhlükəsizlik və gizliliyi təmin edən Netscape tərəfindən yaradılan protokoldur. Bu platforma istifadə edilən veb saytların İP ünvanlarında, 12322 port vasitəsi ilə *mysql* verilən bazasının admin idarə etmə panelinə, 12321 portu vasitəsi ilə sistem idarə etmə paneli, 12320 portu ilə isə veb əsaslı əmrlər sətri olan terminala girmək mümkündür. Əgər bu portlar açıq olsa, müxtəlif növ şifrəyə hücum metodlarından istifadə edib bu panellərə girmək mümkün olardı.

NMAP ilə web platformada olan portların yoxlanılması.

NMAP, kompüter şəbəkələri mütəxəssisi Gordon Lyon (Fyodor) tərəfindən yaradılan təhlükəsizlik skaneridir. Yoxladığı şəbəkənin xəritəsini yarada bilir və həmçinin şəbəkəyə bağlı sistemlərin vəziyyətini, əməliyyat sistemlərini, portlarının vəziyyətini göstərir.

Nmap istifadə edərək kompüter şəbəkəsinə bağlı hər hansı kompüterin əməliyyat sistemini, işləmə vaxtını, proqramların hansı xidmətlərdən istifadə etdiyini, proqramların versiyalarını, kompüter sistemində şəbəkələrarası ekranın olub-olmadığını, şəbəkə interfeysinin hansı şirkətə aid olduğunu öyrənmək mümkündür. Kali Linux terminalında nmap yazaraq aləti çağırırıq.(Şək.3)

```
root@kali:~# nmap
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Şəkil 3. NMAP açılışı

İstifadə edəcəyimiz nmap 7.6 versiyasıdır, alət çağrılarkən kömək üçün istifadə əmrləri ilə birlikdə yüklənir (Şək.3). Biz sürətli port axtarışı üçün “nmap -vvv domeyn.com” əmrindən istifadə edirik.(Şək.4)

```
Host is up, received reset ttl 128 (0.047s latency).
Scanned at 2017-11-27 02:22:16 EST for 93s
Not shown: 998 filtered ports
Reason: 993 no-responses and 5 admin-prohibiteds
PORT     STATE SERVICE        REASON
80/tcp   open  http           syn-ack ttl 128
5631/tcp open  pcanywheredata syn-ack ttl 128
```

Şəkil 4. NMAP axtarış nəticəsi

Nəticə olaraq bütün portların bağlı olduğunu və ancaq 2 portunun açıq olduğu aydınlaşır. 80-cı port http portudur və istifadəçilər brauzerdən veb saytı yığdıqda sistem avtomatik olaraq bu porta istiqamətlənir və sayt açılır. Digər port 5631-ci portdur, bu port Symantec pcAnywhere–nin məsafədən qoşulmalar üçün istifadə etdiyi portdur. **CVE-1999-1028** (Common Vulnerabilities and Exposures) əsasən bu port sistemdə boşluq yaradır, məsafədən hücum edən şəxs bu porta böyük miqdarda verilənlər yollayarsa sistemin xidmətdən imtinasına gətirib çıxara bilər.

Websploit ilə mövcud giriş panellərinin yoxlanışı

Websploit açıq mənbə kodlu məsafədən idarə edilən sistemlərdə boşluqları axtararaq analiz edən alətdir. Websploit çağırmaq üçün terminalda “websploit” komandasl yığılmalıdır. Websploit alətindən istifadə edərək veb saytda daxili inizibatçı panellərini axtaraq. Bunun üçün Websploit-in “web/pma” modulundan istifadə edirik, modulu çağırmaq üçün “wsf > use web/pma” komandasından istifadə edilir. İndi isə hədəfin domeyn.com olduğunu “wsf:PMA > set target domeyn.com” komandası ilə göstərək.(Şək.5)

```
wsf > use web/pma
wsf:PMA > set target domeyn.com
TARGET =>  domeyn.com
wsf:PMA > show options

Options          Value
---------        --------------
TARGET           domeyn.com

wsf:PMA >
```

Şəkil 5. Websploit-də hədəfin seçilməsi

Göründüyü kimi hədəf domeyn.com saytı seçildi “wsf:PMA > run” komandası ilə axtarışa başlaya bilərik.(Şək.6)

```
[*]Loading Path List ... Please Wait ...
[/phpMyAdmin/] ... [302 Found]
[/phpmyadmin/] ... [302 Found]
[/PMA/] ... [302 Found]
[/admin/] ... [200 OK]
[/dbadmin/] ... [302 Found]
[/mysql/] ... [302 Found]
[/myadmin/] ... [302 Found]
[/phpmyadmin2/] ... [302 Found]
[/phpMyAdmin2/] ... [302 Found]
[/phpMyAdmin-2/] ... [302 Found]
[/php-my-admin/] ... [302 Found]
[/phpMyAdmin-2.2.3/] ... [302 Found]
[/phpMyAdmin-2.2.6/] ... [302 Found]
[/phpMyAdmin-2.5.1/] ... [302 Found]
[/phpMyAdmin-2.5.4/] ... [302 Found]
[/phpMyAdmin-2.5.5-rc1/] ... [302 Found]
[/phpMyAdmin-2.5.5-rc2/] ... [302 Found]
[/phpMyAdmin-2.5.5/] ... [302 Found]
[/phpMyAdmin-2.5.5-pl1/] ... [302 Found]
```

Şəkil 6. Websploit axtarış nəticəsi

Nəticə olaraq alət müxtəlif inzibatçı panel girişlərini yoxladı və ancaq “/admin/” inzibatçı panelini tapdı. Bu panelə şifrə sındırıcı alətlərlə hücum edib inzibatçı şifrəsini aşkarlamaq mümkündür.

NİKTO ilə veb saytında boşluqların axtarışı

NİKTO təhlükəsizlik üzrə veb server skaneridir və 6700 potensial boşluq üzrə axtarış apara bilir. Həmçinin server konfiqurasiyalarını, plaqinləri və onların yeniləmə versiyalarını və vaxtlarını göstərə bilir.

Nikto alətini çağırmaq üçün terminalda “nikto” əmri yığılır (Şək.7)

```
root@kali:~# nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host specified

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
```

Şəkil 7. NİKTO əmrinin nəticəsi

Nikto açıldıqdan sonra hədəf hostu göstərmək və skaneri işə salmaq üçün “nikto -h domeyn.com” əmrindən istifadə edirik.(Şək.8)

```
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Debian)
+ Retrieved x-powered-by header: PHP/5.4.45-0+deb7u11
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agai
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the conten
+ Cookie PHPSESSID created without the httponly flag
+ Server leaks inodes via ETags, header found with file /robots.txt, inode: 718603, size: 134, mtime
+ Entry '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /class/: Directory indexing found.
+ Entry '/class/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /uploads/: Directory indexing found.
+ Entry '/uploads/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /includes/: Directory indexing found.
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /languages/: Directory indexing found.
+ Entry '/languages/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /template/: Directory indexing found.
+ Entry '/template/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 6 entries which should be manually viewed.
```

Şəkil 8. NİKTO boşluqların aşkarlanmasının nəsticəsi

Şəkil 8-dən göründüyü kimi Debian Linux əməliyyat sistemi üzərində versiyası 2.2.22 olan Apache server istifadə edilir. Göstərilmiş boşluqlar OSVDB (Open Source Vulnerability Database) əsaslanır. Bundan əlavə bir çox boşluqlar aşkarlandı və bunların bəzilərini analiz edək.

Axtarış saytları Google, Yahoo, Yandex, Mail.ru, Bing və.s saytların axtarış xəritəsini çıxartmaq üçün botlardan istifadə edir. Bu botlar sayt daxili bütün informasiyaları, faylları, onların yerləşdiyi yerlərini aşkarlaya bilir. Bu səbəbdən həsas informasiya olan qovluqları bu botlardan qorumaq üçün “robots.txt” yaradılır və botların baxmasını istəmədiyiniz qovluqlar əlavə edilir. Bu da hakerlərə sizin həssas informasiyanın hansı qovluqlarda olduğunu göstərir. Hər hansı veb saytda http://domeyn.com/robots.txt ünvanında botlardan gizlədilmiş qovluqların siyahısını əldə etmək mümkündür. (Şək.9)

```
User-agent: *

Disallow: /admin
Disallow: /class/
Disallow: /uploads/
Disallow: /includes/
Disallow: /languages/
Disallow: /template/
```

Şəkil 9. “Robots.txt” faylının açılışı

Apache Server sonuncu versiyası 2.4.29 (2017-10-23 tarixində buraxılıb) ancaq NİKTO ilə yoxlanış vaxtı nümunə veb saytın istifadə etdiyi apache 2.2.22 versiyadır. Bu versiya üzrə serverə 14 növ hücum etmək mümkündür ancaq onların ən kritikləri CVE üzrə (CVE-2017-7679, CVE-2017-7668, CVE-2017-3169, CVE-2017-3167) 4 növdür ki, bu da sistemin xidmətdən imtinasına gətirib çıxarır.

NƏTİCƏ

Kompüter sistemlərinin tətbiqi və istifadə sahələri artdıqca onlara olan təhlükələrin və hücumların sayı artır. Belə məsələlərə hazırlıqlı olmaq üçün kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi və boşluqların aşkarlanması əsas məsələlərdən birinə çevrilir.

Texnologiyanın inkişafı yeni IT sahələrinin yaradılması yeni növ hakerlərin inkişfına gətirib çıxarır. Bu səbəbdən texnoloji sahələrin təhlükəsizliyini və müdfiəsini təmin etmək üçün etik hakerlərə ehtiyyac olur. Hakerlərin aqresiv hücumlarının və informasiya oğurluğunun qarşısını almaq üçün daim inkişaf edən texnologiya ilə birlikdə yeni təhlükəsizlik sistemləri, bu sistemləri müdəfiə və konfiqusrasiya edən savadlı mütəxəssislərə, həmçinin boşluqların axtarılması üçün yeni metodların yaradılmasına ehtiyyac yaranır.

Müasir hücum alətlərindən istifadə edərək nüfuzetmə testləri vasitəsi ilə mövcud kompüter şəbəkələrinin cari təhlükəsizlik vəziyyəti öyrənmək mümkündür. Bu məqalədə veb saytlara edilən sadə nüfuzetmə test vasitəsi ilə sistemdə təhlükəsizlik boşluqları yoxlanılnışdır. Ancaq kompüter şəbəkələrində məqalədə yer alan boşluqlar aradan qaldırılmazsa bu gələcəkdə ciddi problemlərə gətirib çıxara bilər.

ƏDƏBİYYAT

[1] Breach Level Index, “2017 First Half Report”, http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf

[2] H. Tran, E. Campos-Nanez, “Cyber resilience recovery model to combat zero-day malware attacks,” Computers & Security, vol. 61, 2016, pp. 19-31

[3] J. N. Goel, B.M. Mehtre, “Vulnerability assessment & penetration testing as a cyber defence technology,” Procedia Computer Science, vol. 57, 2015, pp.710-715.

[4] F. Sano, T. Okamoto, I.Winarno, “A cyber attack-resilient server using hybrid virtualization,” Procedia Computer Science, vol. 96, 2016, pp.1627-1636.

[5] N. Hoque, M. H. Bhuyan, R.C. Baishya, “Network attacks: Taxonomy, tools and systems,” Journal of Network and Computer Applications, vol. 40, 2014, pp. 307-324.

[6] P. Khanna, P. Zavarsky, D. Lindskog, “Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks,” Procedia Computer Science, vol. 94, 2016, pp. 459-464.

[7] Y.N. İmamverdiyev, G.B. Qarayeva, “Botnetlər və onların aşkarlanması üsulları,” İnformasiya Texnologiyaları Problemləri, 2017, №1, s.100-111.

[8] K. Bicakci, D. Unal, “Mobile Authentication Secure Against Man-In-The-Middle Attacks,” Procedia Computer Science, vol. 34, 2014, pp. 323-329.

[9] Z. Mohd Yusop, J. Abawajy, “Analysis of insiders attack mitigation strategies,” Procedia - Social and Behavioral Sciences, vol. 129, 2014, pp. 581-591.

[10] Wikipedia, Haker,https://az.wikipedia.org/wiki/Haker

[11] W.Thomas; A.Jason, “Ninja hacking: Unconventional penetration testing tactics and techniques.” Elsevier. pp. 26-7.

[12] R. Seebruck, “A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model,” Digital Investigation, vol. 14, 2015, pp.36-45.

[13] T. Caldwell, “Ethical hackers: putting on the white hat,” Network Security, vol. 2011, no. 7, 2011, pp.10-13.

[14] Y.N. İmamverdiyev, “Kiberqoşunlar: funksiyaları, silahları və kadr potensialı,” İnformasiya Cəmiyyəti Problemləri, 2015, №2, s.15-25.

[15] Kali Linux, official website, https://www.kali.org/about-us/

[16] H.S.B. Herath, T.C. Herath, “IT security auditing: A performance evaluation decision model,” Decision Support Systems, vol. 57, 2014, pp. 54-63.

[17] G. Stergiopoulos, D. Gritzalis, “Hacking and penetration testing with low power devices,” Computers & Security, vol. 49, 2015, pp. 274-275.

ETHICAL HACKER AND PENETRATION TEST TOOLS

Tural Yunusov
Institute of Information Technology of ANAS, Baku, Azerbaijan
turaly@mail.ru

Abstracts – The article covers the security of computer networks, cyber attack methods, cyber attack vectors, hackers, hacker types and goals, ethical hackers, ethical hacking skills, Kali Linux operating system, pentesting tools - websploit, nmap, webspoit, penetration test methodology, practically penetration test on the network.

Keywords – security assessment, ethical hacker, CEH, Kali Linux, Nikto, Nmap, webspoit, test methodology, OWASP, OSSTMM, ISSAF.