ӘОК 004.42; 004.43; 004.6; 004.7

КОМПЬЮТЕРЛІК ЖЕЛІДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУГЕ АРНАЛҒАН ЖЕЛІЛІК БАРЛАУ ҚҰРАЛДАРЫ

Ешмұхаметов Е.Н., Күлімханов Ә.
yeshmukhametov.yn@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық қауіпсіздік жүйелері, Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – ф.-м.ғ.к., доцент м.а. А. Оспанова

Аңдатпа: Бұл мақалада кәсіпорындағы компьютерлік желілерді қорғауға арналған желілік барлау құралдары қарастырылып, талданады, осы құралдардың негізінде олардың тиімді қолданылуы туралы қорытынды жасалады. Күрделі хакерлік шабуылдарға қарсы тұру үшін вирусқа қарсы қорғау құралдарын, желіаралық экрандарды және басып кіруді болдырмау жүйесін қолдану жеткіліксіз, ең заманауи тәсілдерді ескеретін осалдықты анықтау үшін технологияларды пайдалану қажет.

Тақырыптың өзектілігі мен маңыздылығы ақпараттық технологиялардың кеңінен таралуына, қазіргі қоғамдағы және бизнестегі ақпараттың маңыздылығына және

компьютерлік желілерде өңдеу кезінде осы ақпаратты қорғау қажеттілігіне байланысты. Желілік барлау құралдары желілік қауіпсіздікпен байланысты және бұл желідегі осалдықтар мен әлсіздіктерді, кәсіпорынға зиян келтіруі мүмкін қажетсіз және әдеттен тыс мінез-құлықтан, ақшалай қаражат пен зияткерлік меншікті жоғалтудан қорғауға мүмкіндік беретін әрекет.

Кілттік сөздер: Ақпараттық қауіпсіздік, компьютерлік желі, желілік барлау құралдары, Auvik, Nessus, Nmap, Wireshark, OpenVAS, Advanced IP Scanner, Qualys Freescan.

Кіріспе

Қазіргі уақытта бағдарламалық жасақтама мен техникалық құралдардың алуан түрлілігі бар қазіргі компьютерлік желілердің қауіпсіздігін қамтамасыз ету үшін өте көп ресурстар жұмсалады. Сонымен қатар, жыл сайын бүкіл желіні басқару қиындай түсуде. Желіні сканерлеу ақаулықтарды жоюды жеңілдету арқылы құрылғылар мен өнімділік туралы маңызды ақпарат бере алады.

Желіні үнемі сканерлеу желінің және ондағы құрылғылардың дұрыс жұмыс істеуін қамтамасыз ету үшін маңызды. Желіде қандай құрылғылар бар екенін түсіну, олардың қалай жұмыс істейтінін көру және олардың арасындағы трафикті түсіну үшін желіні қалай сканерлеуге болады. Сондай-ақ, осы тапсырмаларды орындаудың қолдық әдістемелері бар, бірақ көпшілігі оңтайлы нәтижеге қол жеткізу үшін желік барлау құралын қолдануды ұсынады [1].

Желіні сканерлеу – бұл компьютерлік желідегі барлық белсенді құрылғыларды анықтауға мүмкіндік беретін процесс. Белсенді сканерлеу — бұл құрал желідегі әр құрылғыға эхо-сұраныс жіберіп, жауап күтеді. Содан кейін желілік барлау құралы сәйкессіздіктер мен осалдықтардың жауаптарын қарайды. Желіні сканерлеу пакеттерді ұстап алуды немесе желі арқылы деректер пакеті ретінде қозғалатын трафикті түсіретін және бақылайтын пассивті сканерлеуді де білдіруі мүмкін [1].

Желіні сканерлеудің мақсаты желілік барлау құралы анықтаған деректерді қолдана отырып, жүйені басқару, техникалық қызмет көрсету және қорғау. Желіні сканерлеу қол жетімді желілік қызметтерді тану, кез-келген орнатылған сүзу жүйелерін анықтау және тану, пайдаланылған операциялық жүйелерді қарау және желіні шабуылдардан қорғау үшін қолданылады. Оны желінің жалпы күйін анықтау үшін де қолдануға болады [1].

Бүгінгі күні ақпараттық қауіпсіздік бойынша ISO/IEC 27001, 15408, 13335 халықаралық стандарттары бар, олар компьютерлік желідегі ақпараттық қауіпсіздікті қамтамасыз ету үшін желілік барлау құралын пайдалану бойынша кәсіпорынға немесе ақпараттық жүйеге қойылатын талаптарды белгілейді. Сондай-ақ, Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен, ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар бекітілген (бұдан әрі – БТ). БТ 37 тармақтың 2 тармақшасында, ақпараттық-коммуникациялық технологиялар саласындағы тәуекелдерді басқару мақсатында, қатерлердің іске асырылуына әкеп соғуы мүмкін осалдықтарды айқындау және БТ 98 тармақтың 1 тармақшасында, ақпараттық қауіпсіздікті қамтамасыз ету үшін бағдарламалық және аппараттық қамтамасыз етудің осалдықтарын анықтау және жою, осы заңнамалар мен стандарттарда жазылған ақпараттарға сілтеме жасай отырып желілік барлау құралдарының маңызды рөл атқаратына көз жеткізуге болады [3-6].

Зерттеу әдістері. Желілік барлау құралын пайдалану желіде бірнеше құрылғы болса және желі бірнеше ішкі желіні қамтуға жеткілікті үлкен болса қажет. Үлкен желіні қолмен басқаруға тырысу қиын және корпоративтік желіні қауіпсіздіктің елеулі тәуекелдеріне ұшыратуы мүмкін. Нарықта бірнеше түрлі желілік барлау құралдары бар, олардың әрқайсысында тапсырмаға сәл өзгеше көзқарас бар.

Әдетте желілік барлау құралы іздеуге арналған:

a. Желіде іске қосылған барлық хосттар;
b. Осы хосттардағы ашық порттар;
c. Осы порттарда іске қосылған қызметтер;

d. Егер бұл қызметтер соңғы жаңартулармен түзетілсе;
e. Егер желі дұрыс реттелген болса [2].

Желілік осалдықтарды анықтау үшін кеңінен қолданылатын ең жақсы желілік барлау құралдарына шолу.

Auvik – таратылған ақпараттық технологиялар активтерін автоматты түрде табу мүмкіндігі бар желіні басқару шешімі. Бұл қосылатын құрылғылардың көрінісін береді [8,9].

Негізгі ерекшелігі:

a. Avia Traffic Insights желілік трафикті тексеруге көмектесетін трафик туралы ақпарат береді;
b. Бұл желіні кез-келген жерден қол жетімді етеді және сіз auvix түгендеуінде желілік құрылғыларды қоса аласыз;
c. Auvix желіні шарлауды жеңілдетеді және сіз желінің үлкен суретін көре аласыз;
d. Ол таратылған сайттарды тиімді басқаруға мүмкіндік береді;
e. Желінің көрінуін Автоматтандыру және АТ активтерін басқару мүмкіндігі бар.

OpenVAS – толықтай жұмыс істейтін осалдық сканері, өзін интеллектуалды жеке сканерлеуі бар желілік осалдықтарды сканерлеудің қуатты құралы ретінде көрсетті [8, 10].

Негізгі ерекшелігі:

a. Open Vulnerability Assessment System (OpenVAS) — бұл желілік қауіпсіздікті сканерлеудің тегін құралы;
b. OpenVAS-тың көптеген компоненттері GNU General Public License лицензиясы бойынша таратылады;
c. OpenVAS-тың негізгі компоненті-тек Linux ортасында жұмыс істейтін қауіпсіздік сканері;
d. Осалдық тесттерін жазу үшін осалдықтарды бағалаудың ашық тілімен (OVAL) біріктіруге болады.

Wireshark – бұл ашық бастапқы кодты құрал, желілік протоколдардың мультиплатформалық анализаторы ретінде белгілі [8, 11].

Негізгі ерекшелігі:

a. Ол белсенді клиент пен сервер арасындағы қолданыстағы желідегі деректер осалдықтарын сканерлейді;
b. Желілік трафикті көруге және желі ағынын бақылауға мүмкіндік береді;
c. Wireshark Windows, Linux және OSX жүйелерінде жұмыс істейді;
d. Ол TCP сеансы ағынының құрылысын көрсетеді және tcpdump консольдік нұсқасы болып табылатын tshark – ты қамтиды (tcpdump – бұл пәрмен жолынан басталатын пакеттік анализатор).

Nmap-кез-келген нысандар саны бар IP желілерін әр түрлі теңшелетін сканерлеуге, сканерленген желі объектілерінің күйін анықтауға арналған тегін қызметтік бағдарлама [8,13].

Негізгі ерекшелігі:

a. Nmap, аты айтып тұрғандай, желіні және оның порттарын сандық түрде көрсетеді, сондықтан ол портты сканерлеу құралы ретінде де белгілі;
b. Nmap NSE (Nmap Scripting Engine) сценарийлерімен бірге желілік қауіпсіздік мәселелерін және дұрыс емес параметрлерді анықтауға арналған;
c. Бұл IP пакеттерін зерттеу арқылы хосттың қол жетімділігін тексеретін тегін құрал;
d. Nmap – бұл GUI және командалық жол интерфейсі (командалық жол интерфейсі) нұсқаларында қол жетімді толық жиынтық;
e. Оған келесі утилиталар кіреді:

Жетілдірілген графикалық интерфейсі бар Zenmap;
Компьютерді сканерлеу нәтижелері үшін Diff;
Жауаптарды талдауға арналған NPing.

Nessus – ақпараттық жүйелерді қорғаудағы белгілі кемшіліктерді автоматты түрде іздеуге арналған бағдарлама. Ол осалдықтардың жиі кездесетін түрлерін анықтай алады [8,14].

Негізгі ерекшелігі:

a. Бұл UNIX жүйесімен жұмыс істейтін кеңінен қолданылатын желілік қауіпсіздік сканері;

b. Бұрын бұл құрал тегін және ашық болды, бірақ қазір ол коммерциялық бағдарламалық жасақтама ретінде қол жетімді;

c. Nessus-тің тегін нұсқасы шектеулі қауіпсіздік мүмкіндіктерімен қол жетімді;

d. Nessus бүгін 70 000-нан астам плагиндермен және зиянды бағдарламаларды анықтау, веб-қосымшаларды сканерлеу, жүйелік конфигурацияны тексеру және т. б. сияқты қызметтер / мүмкіндіктермен қол жетімді;

e. Nessus-тің жетілдірілген функциясы-автоматты түрде сканерлеу, бірнеше желіні қарап шығу және активтерді анықтау.

Advanced IP Scanner-қуатты және сонымен бірге оларға қосылу үшін қол жетімді желілік хаттамаларды анықтау үшін жергілікті желілерді және қашықтағы веб-серверлерді қарап шығуға арналған бағдарлама. Сондай-ақ, утилита компьютерді қашықтан басқару функцияларын ұсынады [8,15].

Негізгі ерекшелігі:

a. Бұл Windows ортасында жұмыс істейтін ақысыз, ашық бастапқы желіні сканерлеу құралы;

b. Ол желідегі кез-келген құрылғыны, соның ішінде сымсыз құрылғыларды анықтай және сканерлей алады;

c. Бұл қашықтағы компьютерде HTTPS, RDP және т.б. қызметтерді және FTP қызметтерін ұсынуға мүмкіндік береді;

d. Ол қашықтан қол жеткізу, жергілікті желіні қашықтан ояту және жұмысты тез аяқтау сияқты көптеген әрекеттерді орындайды.

Qualys Freescan-бұл қауіпсіздік жүйесіндегі саңылауларды анықтау үшін URL мекен-жайларын, интернет-кеңестерді және жергілікті серверлерді сканерлеуді қамтамасыз ететін ақысыз, ашық бастапқы желіні сканерлеу құралы [8,12].

Негізгі ерекшелігі:

a. Qualys Freescan тек 10 тегін айналдыруға мүмкіндік береді. Өкінішке орай, оны әдеттегі желіні сканерлеу үшін пайдалана алмайсыз;

b. Бұл олардан құтылу үшін желілік мәселелер мен қауіпсіздік түзетулерін анықтауға көмектеседі;

c. Qualys Freescan сканерлеудің 3 түрін қолдайды:

Осалдықтарды тексеру: зиянды бағдарламалар мен SSL-ге қатысты мәселелер;

OWASP: веб-қосымшалардың қауіпсіздігін тексеру;

SCALP check: компьютерлік желінің конфигурациясын қауіпсіздік жүйесінің мазмұнына сәйкестігін тексереді, яғни SCAPE.

Пайдаланушы интерфейсі және өнімді пайдалану ыңғайлылығы критерийлері кесте 1-де ұсынылған.

Кесте 1. Пайдаланушы интерфейсі және өнімді пайдалану ыңғайлылығы критерийлері

Параметрлері	**Nessus**	**Nmap**	**Auvik**	**OpenVAS**	**Wireshark**	**Advanced IP Scanner**	**Qualys Freescan**
Тестілеудің тегін нұсқасын қолдайды	-	+	-	+	+	+	-

Ыңғайлы интерфейс	+	+	+	+	+	+	+
Қолдау опциялары	+	-	+	-	-	-	+
Орналастыру және орнату	-	+	+	+	+	+	+
Мақсатты нарық	+	+	+	+	+	+	+
Икемділік-Windows, Linux және Mac жүйелерінде жұмыс істей алады	+	+	+	+	+	+	+

Желілік барлау құралдарын қысқаша салыстырмалы талдау

Компьютерлік желі мен кәсіпорындағы желілік барлау құралдары туралы ақпаратты салыстыру мен талдаудың барлығы беделді және құрметті көздерден алынған [7-15].

Қарастырылған осалдық сканерлері кейбір ұқсастықтарға ие – атап айтқанда, олар көптеген танымал операциялық жүйелерді қолдайды, ат ресурстарын түгендеуді және желілік порттарды, қызметтерді және веб-қосымшаларды сканерлеуді біледі, жеткілікті тұрақты емес және әдепкі парольдерді анықтайды, негіздерді қолдана отырып осалдықтарды іздейді cve.mitre.org және OVAL(Open Vulnerability and Assessment Language) стандарты, сондай-ақ SIEM(Security information and event management) – мен интеграцияны қамтамасыз етеді.

Қорытынды. Желіні бақылау кез-келген желіге кіруді болдырмау үшін маңызды әрекет болып табылады. Желіні сканерлеу құралдары бұл тапсырманы айтарлықтай жеңілдетеді. Желілік мәселелерді жылдам қарап шығу бізге желілік шабуылдардың болашақ әсері туралы білуге мүмкіндік береді және олардан аулақ болу үшін алдын-алу жоспарын дайындауға көмектеседі.

Қазіргі әлемде интернеттегі перспективада жұмыс істейтін бағдарламалық жасақтаманың кез-келген ірі индустриясы желілік шабуылдардың салдарынан өзінің жұмысын жоғалтпай, өз жүйесін желіде жұмыс істеуге дайындау үшін желілік сканерлеу құралдарын қолданады, бұл өз кезегінде пайдаланушыларды жүйеге сенуге мәжбүр етеді.

Бұл мақалада ең танымал және кеңінен қолданылатын Желілік сканерлеу құралдары қарастырылған. Олардан басқа көп нәрсе болуы мүмкін. Болашақта желілік мәселелерді жеңу үшін желілік мінез-құлыққа сәйкес ең қолайлы жүйені таңдауға болады.

Қолданылған әдебиеттер тізімі

1. Staff Contributor. Network Scanning How-To Guide, 2019, https://www.dnsstuff.com/network-scanning (accessed 12 August 2019).
2. Prajakta Subhash Jagtap, M.Tech Student, K J Somaiya, “Vulnerability Scanning,” International Journal of Engineering Development and Research, vol. 8, Issue. 1, 2020.
3. ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements. 2015.
4. ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security. 2017.
5. ISO/IEC 15408, Information technology. Methods and means of ensuring security. Information and Communication technology protection management. 2007.

6. Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы». 2016.
7. Tim Keary. 10 Best Network Scanners – Network Analysis & Management Tools. 2021.
8. 15 Best Network Scanning Tools (Network And IP Scanner). 2022
9. Auvik желілік сканерінің ресми парақшасы https://www.auvik.com
10. OpenVAS желілік сканерінің ресми парақшасы https://www.openvas.org
11. Wireshark желілік сканерінің ресми парақшасы https://www.wireshark.org
12. Qualys желілік сканерінің ресми парақшасы https://www.qualys.com
13. Nmap желілік сканерінің ресми парақшасы https://nmap.org
14. Nessus желілік сканерінің ресми парақшасы https://www.tenable.com
15. Advanced IP Scanner желілік сканерінің ресми парақшасы https://www.advanced-ip-scanner.com