ОӘЖ 004.771

УНИВЕРСИТЕТТІҢ ҚАШЫҚТЫҚТАН ОҚЫТУ ПОРТАЛЫНЫҢ ҚАУІПСІЗДІГІ

Кемербаева Раушангүл Қайратқызы
kemerbayeva@gmail.com
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан
Ғылыми жетекшісі-т.ғ.к., доцент м.а. Омарбекова А.С.

Аннотация. Көптеген жағдайларда желіге шабуыл әрекеттері желідегі кез-келген мүмкін жерге қосылу әрекеті орындалатын желіні сканерлеуден немесе белгілі бір мақсаттағы әр портқа қосылу әрекеті орындалатын портты сканерлеуден басталады. Мұндай сканерлеуді анықтау мүмкіндігі желіге қауіпті,осалдығын анықтауға көмектеседі. Бұл мақалада Nmap-ті қолдана отырып, қашықтықтан оқыту порталының қауіпсіздін сканерлеу арқылы осал тұстарын анықтау мүмкіндіктері қарастырылған.

Түйінді сөздер: ақпараттық қауіпсіздік; операциялық жүйе; осалдықтар; осалдықтарды анықтау; шабуыл жасау.

Кіріспе.

Желілер мен порттарды сканерлеуді қауіпсіздік сарапшылары көбінесе оларды жою үшін өз желілерінде қауіпсіздікке төнетін қауіптерді іздеу үшін пайдаланады. Өкінішке орай, дәл осындай қауіптерді- шабуылдаушы өз мүддесіне қарай тауып қолдануға болатын шабуыл іс-әрекеттерін жасай алады. Сондықтан компьютерлерді мақсатты желіде немесе мақсатты компьютердің порттарында сканерлеу-бұл желіге кіруге тырысудың өте кең таралған алғашқы қадамы. Шын мәнінде, интернетке қол жетімді кез-келген желі автоматты түрде де, қолмен де үнемі сканерленіп, шабуылға ұшырауы ықтимал.

Осылайша, желі сарапшыларына шабуылдың қайдан келуі мүмкін екенін анықтау немесе алдын алу шараларды қолдану осындай сканерлеу арқылы анықтай алу өте тиімді болып келеді.

Сонымен қатар, шабуылдаушының сканерлеу арқылы желі туралы ақпарат алуға және шабуылдаушы туралы ақпарат алу үшін пайдалануға болады. Яғни, шабуылдаушының ерекшеліктерін анықтау үшін сканерлеуді талдауға болады, мысалы
шабуылдаушының операциялық жүйесін, қолданылатын сканерлеу құралы немесе шабуылдаушының нақты жабдықтары туралы мәләметтерді алуға болады. Уақытша ақпарат тіпті IP мекенжайын өзгерткен жағдайда шабуылдаушының нақты орналасқан жерін анықтай алатын маршруттаудың кідірістерін талдау үшін де қолданыла алады.

Сканерлеу- бүгінгі таңда интернетте жиі кездесетін әрекет, мысалы, дәлелді қарсылас туралы ақпарат жинау немесе осал хосттарды іздеудің автоматтандырылған құралдары сияқты зиянды әрекет. Сканерлеуді анықтаудың көптеген әдістері жасалды, дегенмен, олардың негізгі бағыты пакет деңгейіндегі ақпарат қол жетімді немесе желінің ішкі сипаттамалары белгілі болатын шағын желілерге бағытталған. Интернет-провайдерлер, ірі корпорациялар немесе мемлекеттік ұйымдар сияқты ірі желілер үшін бұл ақпарат қол жетімді болмауы мүмкін.

Сканерлеу- мақсатты зерттеу әдісі. Сканерлеудің мақсаты-белгілі бір хосттарда белгілі бір хосттардың немесе белгілі бір қызметтердің болуын анықтау. Ол белгілі бір мақсатты объектіге зондтау пакетін жіберуден тұрады, онда мақсаттың жауабы хосттың немесе қызметтің болуын көрсетеді.

Сканерлеу көбінесе зиянды әрекеттің көрсеткіші болып табылады. Олар белгілі бір құрттардың болуын көрсетуі мүмкін, осы уақытқа дейін байқалған құрттардың көпшілігі сканерлеу құрттары болған..

Сканерлеу зиянды әрекетті көрсетуі мүмкін болғандықтан, олардың болуын анықтау өте маңызды. Алайда, сканерлеуді анықтаудың көптеген тәсілдері желінің сипаттамалары толығымен белгілі немесе пакеттік деңгейдегі трафик туралы ақпарат бар шағын желілерде сканерлеуді анықтауға бағытталған.

Негізгі бөлім

Жалпы, сканерлеу дегеніміз-бірнеше мақсаттардың болуын анықтау үшін қолданылатын барлау әдісі, онда хосттар немесе белгілі бір хосттарда белгілі бір қызметтер болуы мүмкін. Сканерлеуді қарсыластар шабуыл жасайтынын анықтау үшін де, жүйелік әкімшілер де өз желісін тексеру үшін қолдана алады. Сканерлеу осалдықтарды іздеудің жанама әсері болуы мүмкін.

Жүргізілген зерттеулер бойынша желіні және порттарды сканерлеу жұмыстары қарастырылған болатын. Бұл әдістер, әдетте, жалпы порттарды тексеру арқылы

шабуылдаушының анықталған осал тұстарын өз мүдделеріне қарай қолданылмау үшін алдын алу үшін жүргізіледі.

Сканерлеу кезінде жеке осалдықтарды анықтауға болады. Бұл жағдайда ену тестілеуі анықталған осалдықтарды мақсатты ортада қолдануға болатындығын тексеруге тырысады. Біліктк маман иесі болу үшін сканерлеудің барлық түрлерін қарастырған жөн. Осалдықтарға анықтауға мүмкіндік беретін Nmap бағдарламасы мамандар арасында бүгінгі таңда жиі қолданылуда.

Nmap-бұл портты сканерлеу мен сараптаудағы құрал болып келеді. Nmap барлық параметрлері мен модульдерін сипаттауға мүмкіндік береді[1].

Nmap-та бізге келесі параметрлер қол жетімді:

- o-ОЖ анықтау;
- p-портты сканерлеу;
- p - - барлық порттарды сканерлеу (1-ден 65 535-ке дейін);
- p 80,443-80 және 443 порттарын сканерлеу;
- sV-қызметтерді анықтау;
- p 22-1024-22-ден 1024-ке дейінгі порттарды сканерлеу және де т.б. мүмкіндіктері бар.

Nmap-та ОЖ-ны анықтау үшін келесі параметрлерді қолдану қажет. Бұл параметр амалдық жүйенің түрі мен нұсқасын анықтау үшін әртүрлі әдістерді қолданады. Бұл осалдықтарды анықтау үшін өте пайдалы. ОЖ нұсқасын іздеу амалдық жүйеде белгілі осалдықтар мен эксплуатацияларды көрсетеді. Мақсатты желіміздің осалдығын анықтау үшін келесі команданы енгізу қажет:

nmap 00.000.000.000 **-o**

Nmap-та қызметтерді анықтау. ОЖ анықталғандай, бұл параметр қызмет пен нұсқаны анықтауға тырысады.

nmap 00.000.000.000 **–sV**

Қашықтағы желіні сканерлеу үшін тек бір параметр қажет. Бұл мақсатты IP мекенжайы немесе егер DNS дұрыс конфигурацияланған болса, мақсатты хост атауы болады. Бұл операция келесі команда арқылы орындалады:

nmap -sV ■.■.kz

Төменде бір мәнді сканерлеу нәтижесі келтірілген:

1-сурет. Қызметті анықтау

Нәтижисінде мақсатты порталдың шабуылға өте осал екенін көруге болады, себебі бірнеше ашық порттары бар.

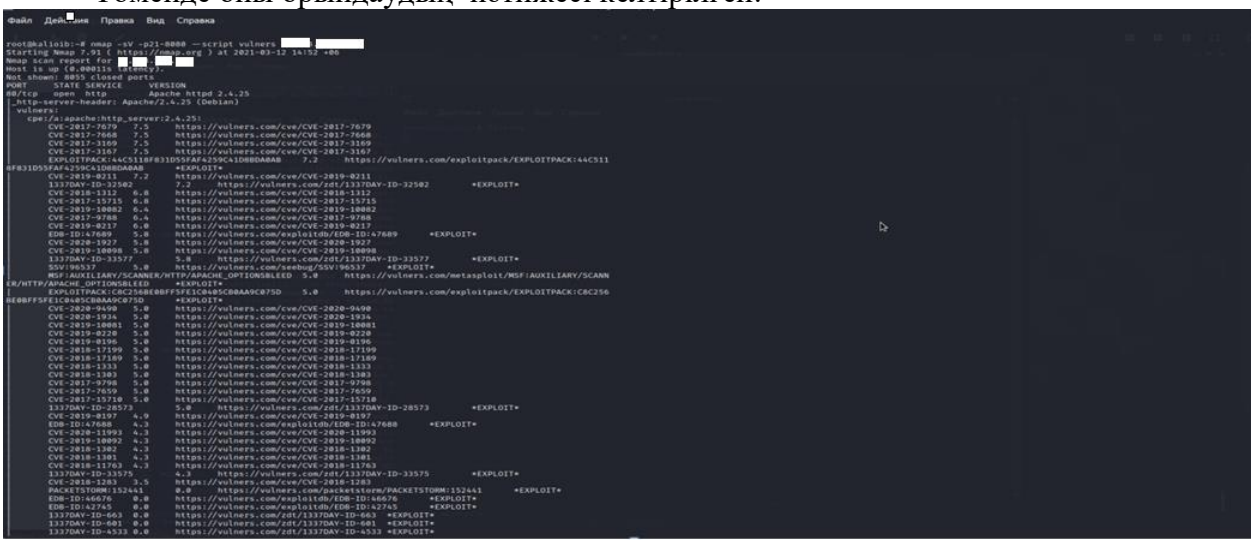
Nmap сканері анықтай алатын порттардың күйін қарастыру қажет. Порттардың келесідей түрлері бар:

- Open (ашық) — TCP қосылымын, UDP датаграммасын немесе SCTP қауымдастығын қабылдайтын қосымша бар екенін білдіреді.
- Closed (жабық) - порт қол жетімді болса да, оны ешқандай бағдарлама тыңдамайды.
- Filtered (сүзгі) - Nmap порттың ашылғанын немесе ашылмағанын анықтай алмайды, өйткені сұраныстарды бұғаттайтын пакеттік сүзу құрылғысы бар.
- Unfiltered (сүзілмеген) — порттың қол жетімді екенін білдіреді, бірақ Nmap оның ашық немесе жабық екенін анықтай алмайды.
- Open|Filtered (ашық|сүзілген) — Nmap порттың ашылғанын немесе сүзілгенін анықтай алмайды. Бұл ашық порттарды сканерлеу жауап бермеген кезде болады.
- Closed|Filtered (жабық|сүзілген) — Nmap порттың жабылғанын немесе сүзілгенін анықтай алмайды.

Әдепкі сценарийлерді қолдана отырып, мақсатты машинаның 10.123.255.184 портын сканерлеу үшін келесі пәрменді енгізу қажет:

nmap –sV 00.000.000.000

Төменде оны орындаудың нәтижесі келтірілген:



2-сурет. Nmap-та -sV командасы арқылы сценарийлерді анықтау

Зерттеу барысында, CVE-2019-0211 Apache Root Privilege Escalation осалдығы анықталған болатын.

Қорытынды

Қазіргі таңда қашықтан оқыту білім алудың басты және маңызды құралы болып отыр. Күн сайын білім беру қарқынды дамып келеді. Пандемия мен ұзақ мерзімді карантин себебінен қашықтықтан білім алатын студенттер мен оқушылардың саны күрт өсіп кетті, сол себепті қашықтан оқытудың порталының сапасын және де қауіпсіздігін қамтамасыздандыру басты өзекті мәселелердің бірі.

Қашықтықтан оқыту үздіксіз интернет желісімен, компьютермен және де басқада құрылғылармен үздіксіз жұмыс істеуді талап етеді. Интерактивті оқыту платформаларын, электронды журналдар мен бейнеконференция қызметтері,онлайн порталдар күнделікті үлкен сұранысқа ие. Сол себепті олардың ақпараттық қауіпсіздігін қарастырдым, солардың бірі "жалпы онлайн-курстарын білім беру онлайн-платформасы".

Бұл мақалада біз сканерлеуді пайдалана отырып порталдың осал тұстарын қарастырдым. Қазіргі уақытта желілер зиянды бағдарламалар, қызмет көрсетуден бас тарту, ақпаратты ұрлау және т.б. көптеген қауіптерге тап болады. Демек, сарапшылардың сканерлеу арқылы қауіптерді, зиянды бағдарламалар мен шабуылдарды анықтауда маңызды

рөл атқарады. Компьютерлік желінің шабуылдардан қауіпсіздігін қамтамасыз ету үшін Nmap құралы тиімді құралдың бірі болып келеді.[2]

Зерттеу барысында қашықтықтан оқыту порталының осал жақтары анықталған, ең басты осалдың бірі CVE-2019-0211 Apache Root Privilege Escalation болып шықты. Қашықтықтан оқыту порталының қауіпсіздігіне талдау жүргізіліп, ұсыныс шаралары ұсынылған болатын Қашықтан оқыту платформасының және қолданатын кез-келген басқа скриптердің жаңартылғанына көз жеткізу қажет. Тұрақты жаңартуды қамтамасыз ете отырып, қауіпсіздік осалдықтарын пайдалану мүмкіндіктері азаяды.

Қолданылған әдебиеттер тізімі

1. Kali Linux. Тестирование на проникновение и безопасность. — СПб.: Питер, 2020. — 448 с.: ил. — (Серия «Для профессионалов»).

2. Muelder, C., Ma, K.-L., & Bartoletti, T. (2006). Interactive Visualization for Network and Port Scan Detection. Recent Advances in Intrusion Detection, 265–283. doi:10.1007/11663812_14