Ташкинов Ж.
2 курс студенті, академик Е.А. Бөкетов атындағы Қарағанды университеті
Сегізбаева М.С.
оқытушы, академик Е.А. Бөкетов атындағы Қарағанды университеті

ҚАУІПТЕР МЕН ОСАЛДЫҚТАРДЫ АНЫҚТАУ ЖӘНЕ АЛДЫН АЛУ

Бүгінгі таңда Интернеттің жылдам дамуы кезеңінде көптеген шабуылдар желі арқылы орын алады. Ақпараттық қауіпсіздік жағынан ең қауіпті желілік компьютерлер болып табылады. Олардың қауіпсіздігі ең өзекті тақырыптардың біріне жатады. Сондықтан ақпарттық қауіпсіздікді сақтауда алдымен ықтимал қауіп-қатерлер мен осалдықтарды зерттеу қажет. Осы мақсатқа жету үшін зертеу жұмысын Nmap арқылы жүзеге асырамыз.

Nmap ("Network Mapper") - бұл желіні зерттеуге арналған бастапқы коды бар ақысыз утилита. Көптеген жүйелер мен желі әкімшілері оны желіні түгендеу, қызметтерді жаңарту кестесін басқару және хосттың немесе қызметтің жұмыс уақытын бақылау сияқты тапсырмалар үшін пайдалы деп санайды [1].

Ол үлкен желілерді жылдам қарап шығуға арналған, бірақ жалғыз хосттарға қарсы күшті жұмыс жасайды. Nmap барлық негізгі компьютерлік операциялық жүйелерде жұмыс істейді, консольдік және графикалық нұсқаларыда қол жетімді.

Linux жүйелеріне арналған Nmap қосымшасын Гордон Лион жасаған болатын. Оның жұмысы шикі, өңделмеген IP пакеттерін қолдануға негізделген. Бұл желідегі қол жетімді хосттарды табуға және осы хост деректерін пайдаланатын сервистерді анықтауға ықпал етеді. Сонымен қатар, утилита бұл процестердің қандай операциялық жүйелерде орындалғаны туралы деректерді қайтарады.

Осы қосымшаның көмегімен сіз келесі сипаттағы ақпаратты ала аласыз:

* сіздің желіңізге қанша және қандай машиналар қосылған;
* онда қандай IP мекенжайлары бар;

* іске қосылған машиналарда қандай операциялық жүйелер және қандай нұсқалар орнатылған;

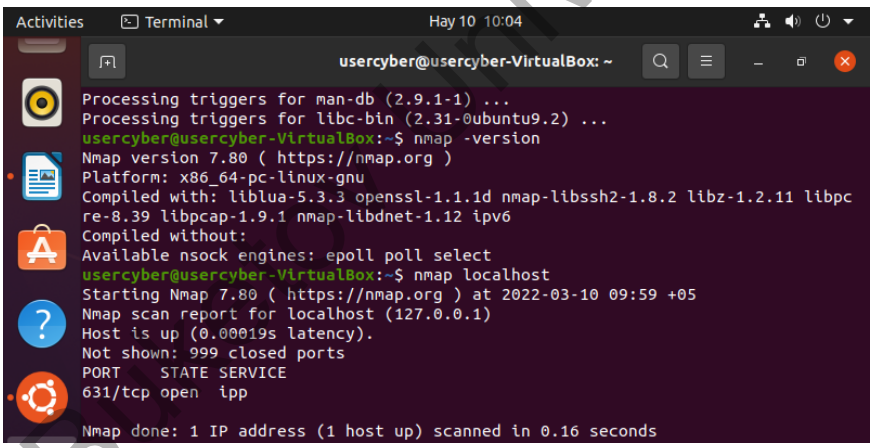
* сіздің инфрақұрылымыңызда ашық порттар бар ма және олар қандай;

* жүйені ықтимал зиянды бағдарламалық жасақтамамен жұқтыру бар ма;

* рұқсат етілмеген хосттар немесе қызметтер желіге қосылған ба;

* желіңіздегі барлық компьютерлер қауіпсіздік өлшемдерінің көрсетілген жиынтығына сәйкес келе ме (сәйкес келмейтіндерді бұғаттау мүмкіндігімен).

Осы зерттеу жұмысында ашық порттарды және осылдылықтарды анықтаймыз. Ол үшін Ubuntu жүйесінің пәрмен жолына nmap localhost негізгі сканерлеуді орындайтын пәрменді енгіземіз(1 сурет).



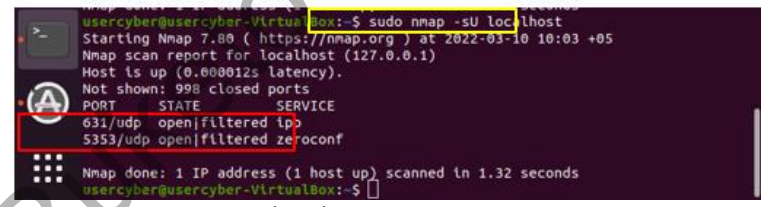
1-сурет негізгі сканерлеу

Бұл команда арқылы маршрутизатордағы портты тексеріп олардың ашық немесе жабық екенін анықтаймыз. Басқа қандай порттар бар? Порттар-бұл компьютерден компьютерге ақпарат берілетін виртуалды жолдар. Таңдау үшін барлығы 65536 порт бар.. 0-ден 1023-ке дейінгі порттар-ең танымал порт нөмірлері. Порттарда жұмыс істейтін ең танымал қызметтер: MS SQL де-рекқоры (1433), POP3 пошта қызметтері (110), IMAP (143), SMTP

(25), HTML веб-қызметтері (80). 1024 - тен 49151-ке дейінгі порттар-бұл сақталған порттар; бұл оларды бағдарламалық жасақтаманың нақты протоколдары үшін сақтауға болатындығын білдіреді. 49152 - 65536 порттары-динамикалық немесе жеке порттар; бұл оларды кез-келген адам пайдалана алады дегенді білдіреді[1].

Портты айдау дегеніміз не? (Port Forwarding) Портты бағыттау (Port Forwarding) маршрутизаторда деректер пакеттерін жергілікті желідегі (Lan) құрылғыларға немесе компьютерлерге сырттан (интернеттен) жіберуге мүмкіндік беретін арнайы функция бар. Әдепкі бойынша, маршрутизатордағы барлық порттар жергілікті желідегі компьютерлердің бұзылуына жол бермеу үшін жабық. Бірақ маршрутизатордағы порт арқылы қосылу үшін қызметті пайдаланған кезде оны ашу керек. Мысалы: Yahoo! Messenger Сізге келесі порттардың біреуі ашық болуы керек: 5061, 443, 80. Сонымен алғашқы TCP порттарын сканерлеу нәтижелері көрсетілді. Қазіргі уақытта 631 TCP портты ашық(1 сурет).

Әкімші құқығымен Nmap пайдалану. Сканерлеуді орындау үшін терминалдың пәрмен жолына келесі *sudo nmap –sU localhost* команданы енгізу арқылы компьютердің UDP порттарын анықтай аламыз



2 сурет. Әкімші құқығымен Nmap пайдалану.

TCP/IP стекінде екі негізгі Протокол бар — бұл TCP және UDP. Олардың арасындағы айырмашылық деректерді жеткізу кепілдігінде. TCP алушыдан деректер пакеттерін алғанын растауды талап етеді және ол үшін түйіндер арасында бастапқыда орнатылған байланыс қажет. Сондай — ақ, ол деректердің жоғалуын болдыртпайды, кідірістерді жояды, логикалық қосылысты қолданады және т.б. Ал UDP мұндай қызметтерді

жасамайды, сондықтан оны жиі "сенімсіз датаграммалар протоколы"деп атайды.

Мынадай кемшіліктері қарастырылған

1. Сенімсіз хаттама. Деректердің берілуін және, тиісінше, тұтастығын бақыламайды, бірақ оларды жай ғана жібереді, сондықтан деректер үзіліп немесе қайталануы , жоғалуы мүмкін.

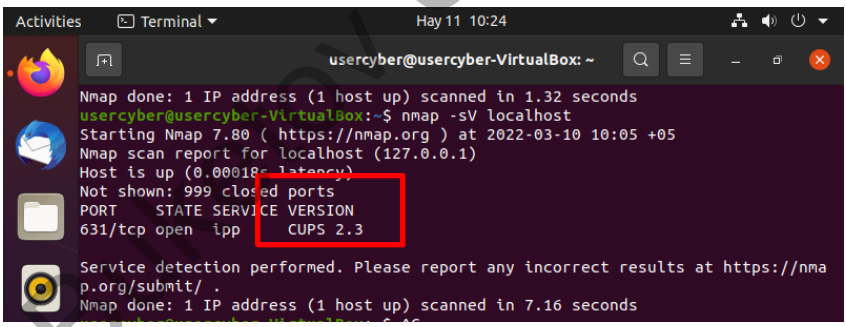
2. Деректерді тәртіппен жібермейді. Егер сіз деректерді бірнеше адресатқа жіберсеңіз, олар бірінші кімге келетіні белгісіз.

4. Пакеттің тұтастығын тексеру, егер ол жеткізілсе және оны алушы тексерсе ғана жүзеге асырылады, ал пакеттің жеткізілгенін жіберуші де білмейді.

5. Нашар қауіпсіздік. Көптеген брандмауэрлер UDP пакеттерін бұғаттайды, өйткені шабуылдаушылар оның порттарын нақты қосылыстар орнатпай - ақ пайдалана алады[2]

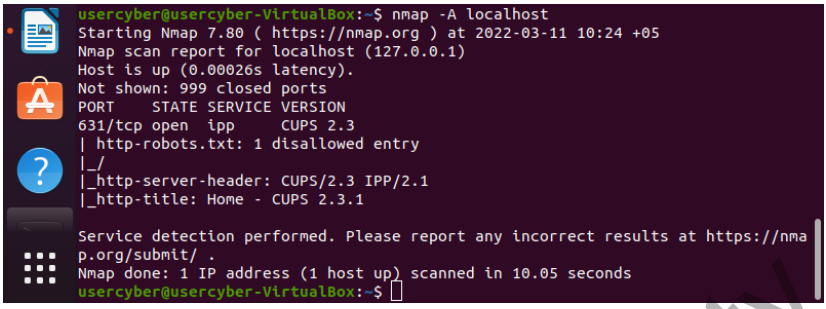
Біздің жағдайда екі 631 және 5353 UDP порттары анықталды(2сурет).

Келесі команда –sV параметрі көрсетілсе, онда Nmap командасы анықталғандардың версиясын көрсетеді, оның нәтижелері осалдықтарды іздеген кезде пайдаланылады.



3 сурет. Анықталғандардың версиясы

Сценарий негізінде сканерлеу үшін терминалдың пәрмен жолына келесі nmap –A localhost пәрмені енгізілді.



4 сурет Терең сканерлеу

Бұл команда белгілі бір осалдықтарды іздеуге арналған Nmap сценарийлерін орындайды сонымен қоса, хост жүйесіне арналған SSH кілттерін алуға болады.

Біздің жағдайд бұл жазба Disallow формасының robots.txt файлы: бұл кем дегенде кейбір пайдаланушы агентіне осы URI-ді сұрамауға нұсқау берілгенін білдіреді. Олардың осы жолдың астында тізімі көрсетілген.

Зертеу нәтижесінде алынған осалдылықтардың алдын алу үшін антивирус, Брандмауэрді қолдану. Яғни портты брандмауэр арқылы бұғаттау, оған қол жеткізуге мүмкіндік бермейді.

Сонымен қоса Nmap арқылы сканерлеуге қарсы қорғау шараларының бірі жақсы бапталған брандмауэр болып табылады. Брандмауэр шабуылдың көптеген жолдарын тиімді түрде бұғаттай алады.Егер күдікті трафикті байқаған жағдайда бәрін бұғаттау, содан кейін қажетті трафикке рұқсат беру үшін оны қайта анықтау. Брандмауэрлердің тағы бір қағидасы - терең қорғаныс. Егер порттар брандмауэрмен бұғатталған болса да, олардың жабық екеніне көз жеткізіңіз Қаскүнем брандмауэрді бұзса деп болжаймыз. Күшті қорғауды қамтамасыз ету үшін жеке машиналар бұғатталуы керек. Бұл әркім әр уақытта жіберетін қателіктердің көлемін және залалын азайтады. Шабуылдаушылаға брандмауэрде де, жеке машиналарда да әлсіз жерлерді табуы керек болады. Порт сканері жабық және сүзгіленген порттарға қарсы дәрменсіз. Жеке мекен-жай кеңістігін (мысалы, желілік мекен-жайларды тарату арқылы) және қосымша брандмауэрлерді пайдалану одан да көп қорғауды қамтамасыз етеді.

Пайдаланылған әдебиеттер:

1. https://nmap.org/book/toc.html
2. Kali Linux: Поиск уязвимостей на сайте. [Электронды мәлімет көзі].
Мына сілтеме бойынша қолжетімді:
http://t3i1t3.blogspot.com/2014/12/kalilinux.html

Шаяхметов Ж.М.
студент 2 курса, Костанайский региональный университет им. А.Байтурсынова
Бегалин А.Ш.
м.е.н., ст.преподаватель, Костанайский региональный университет им. А.Байтурсынова

СЕТЕВАЯ ПРОГРАММА МОНИТОРИНГА СЕТЕВОЙ И АППАРАТНОЙ КОНФИГУРАЦИИ КОМПЬЮТЕРОВ

Актуальность данного программного обеспечения для мониторинга конфигурации компьютера и сети определена поддержкой и обслуживание компьютеров и локальных сетей, а также за планирование и реагирование на перебои в обслуживании и другие проблемы в кратчайшие сроки.

Цель научной работы - разработка программы для мониторинга в реальном времени за локальной сетью, компьютерами в данной сети удалённо, что существенно сократит временные затраты и повысит качество обслуживания компьютеров в сети.

Для достижения данной цели нужно выполнить ниже приведённые задачи программного обеспечения:

1. Обеспечить разделение программного обеспечения на клиентскую и серверную части, с целью понижения нагрузки на компьютер конечных пользователей, это существенно уменьшит системные требования;

2. Построить базу данных, хранящую все данные о мониторинге;

3. Разработать программу которая будет выполнять функцию отправки данных компьютера в базу данных в реальном времени;