**ЛЕКЦИЯ № 9. Жүйені қорғау және қауіпсіздік**

Кейбір адамдар үшін "қауіпсіздік" және "қорғау" ұғымдары бір-бірін алмастырады. Алайда, бір жағынан техникалық, әкімшілік, құқықтық және саяси мәселелер, екінші жағынан қауіпсіздікті қамтамасыз ету үшін қолданылатын операциялық жүйенің нақты тетіктері кіретін тиісті өкілеттіктері жоқ адамдар тарапынан оқу үшін файлдардың қолжетімсіздігін қамтамасыз етудің негізгі мәселелерін және өзгерістерді бір – бірінен ажырату пайдалы. Түсініспеушіліктерді болдырмау үшін жалпы жоспардың мәселелеріне сілтеме жасау үшін қауіпсіздік (қауіпсіздік) термині қолданылады, ал компьютерде бар ақпаратты қорғау үшін қолданылатын операциялық жүйенің нақты механизмдеріне сілтеме жасау үшін қорғаныс механизмдері (protectionmechanisms) термині қолданылады. Дегенмен, екеуінің арасында нақты белгіленген шекара жоқ. Зерттелетін мәселенің табиғатын зерттеу үшін алдымен қауіп-қатерлер мен крекерлердің әрекеттері жағдайында қауіпсіздік мәселелеріне жүгінейік. Содан кейін қауіпсіздікке қол жеткізуге қолайлы қорғаныс механизмдері мен модельдерін қарастырыңыз.

*Қауіптер*

Қауіпсіздікке арналған көптеген жұмыстарда ақпараттық жүйелердің қауіпсіздігі үш компонентке бөлінеді: құпиялылық, тұтастық және қол жетімділік. Барлық үш компонент бірге жиі CIA (құпиялылық, Интегралдылық, Қауіпсіздік) деп аталады. Олар 9.1-кестеде көрсетілген және біз басқа CIA (ЦРУ, АҚШ Орталық барлау басқармасы)тапсырмаларына ұқсас крекерлер мен тыңшылардан қорғануымыз керек қауіпсіздік қасиеттерінің негізін құрайды.

| Тапсырмалар | Қауіптер |
|---|---|
| Құпиялылық | Деректердің сенімсіздігі |
| Тұтастық | Деректерді бұрмалау |
| Қол жетімділік | Қызмет көрсетуден бас тарту |

Кесте 9.1. Қауіпсіздік міндеттері мен қауіптері

Бірінші қасиет-құпиялылық (құпиялылық) – деректердің құпиялылығын сақтауға бағытталған. Нақтырақ айтсақ, егер белгілі бір деректердің иесі бұл мәліметтер қатаң анықталған адамдар тобына қол жетімді болуы мүмкін деп шешсе, жүйе оған құқығы жоқ адамдардың деректерге қол жеткізе алмауына кепілдік беруі керек. Кем дегенде, иесі кімді және нені көре алатынын анықтай алуы керек және жүйе жеке файлдарға қатысты осы талаптардың орындалуын қамтамасыз етуі керек.

Екінші қасиет-тұтастық (integrity) – қажетті құқықтары жоқ пайдаланушылар иелерінің рұқсатынсыз кез келген деректерді өзгерте алмауы керек дегенді білдіреді. Бұл тұрғыда деректерді өзгерту оларға өзгерістер енгізуді ғана емес, оларды жоюды немесе оларға жалған деректерді қосуды да қамтиды. Егер жүйе иесі оны өзгерту туралы шешім қабылдағанға дейін оған енгізілген деректердің өзгермейтініне кепілдік бере алмаса, онда ол деректерді сақтау рөлін жоғалтады.

Үшінші қасиет-қол жетімділік (availability) – бұл жүйенің жұмысын ешкім бұза алмайтындығын және оны бұза алмайтындығын білдіреді. Қызметтен бас тартуды тудыратын шабуылдар (denial of service, (DOS)) жиі кездеседі. Мысалы, егер компьютер интернет-сервер ретінде жұмыс істесе, оны үнемі сұраулармен лақтыру оның орталық процессорының барлық жұмыс уақытын кіріс сұрауларын зерттеуге және қабылдамауға бағыттай отырып, оның жұмысын тоқтатуы мүмкін. Егер кіріс веб-бетті оқу сұрауын өңдеу үшін, айталық, 100 ХҒС қажет болса, секундына 10 000 сұрау жібере алатын кез келген адам серверді өшіре алады. Деректердің құпиялылығы мен тұтастығын бұзуға бағытталған шабуылдармен күресу үшін Сіз өте қолайлы модельдер мен технологияларды таңдай аласыз, бірақ қызмет көрсетуден бас тартуды тудыратын шабуылдарға қарсы тұру әлдеқайда қиын.

Кейінірек барлық мүмкін сценарийлер үшін үш негізгі қасиет жеткіліксіз деп шешілді және шынайылық (authenticity), сәйкестендіру (accountability), бас тарту (nonrepudiability), жабықтық (құпиялылық) және т.б. сияқты қосымша қасиеттер қосылды. Дегенмен, үш бастапқы қасиет әлі де көптеген (құрметті) қауіпсіздік сарапшыларының санасы мен жүрегінде ерекше орын алады.

Жүйелерге крекерлерден келетін тұрақты қауіп төніп тұр. Мысалы, крекер жергілікті желі трафигіне қосылып, ақпараттың құпиялылығын бұзуы мүмкін, әсіресе егер деректер алмасу хаттамасында шифрлау қолданылмаса. Сондай-ақ, шабуылдаушы дерекқорды басқару жүйесін бұзып,

базаның тұтастығын бұза отырып, кейбір жазбаларды жоя немесе өзгерте алады. Ақырында, техникалық қызмет көрсетуден бас тартуды тудыратын ақылды орналастырылған шабуылдар бір немесе бірнеше компьютерлік жүйелердің қолжетімділігін бұзуы мүмкін.

Бөгде адамның жүйеге шабуыл жасауының көптеген жолдары бар.Қазіргі уақытта көптеген шабуылдарға өте жақсы құралдар мен қызметтер қолдау көрсетеді. Бұл аспаптардың кейбіреулері қара қалпақ хакерлері (black-hathackers), ал кейбіреулері ақ қалпақ (whitehats) деп аталады. Ескі батыстықтарға ұқсас, цифрлық әлемдегі жағымсыз кейіпкерлер қара шляпалар киіп, трояндық атқа мінеді (Трожанхорс), ал жақсы хакерлер ақ шляпалар киіп, бағдарламаларды өз көлеңкесінен жылдамырақ жасайды.

Айтпақшы, танымал ақпараттық басылымдарда "хакер" деген жалпы терминді тек қара шляпаларға қатысты қолдану әдетке айналған. Бірақ компьютерлік әлемде хакер - ұлы бағдарламашыларға берілген құрметті атақ. Олардың кейбіреулері, әрине, жағымсыз істермен айналысады, бірақ көпшілігі өте лайықты адамдар. Олардың баспасөзі мүлдем әділетсіз деп санайды. Нағыз хакерлерді құрметтеу үшін біз бұл ұғымды өзінің бастапқы мағынасында қолданамыз, ал оларға тиесілі емес компьютерлік жүйелерді бұзуға тырысатын адамдар крекер немесе крекер (крекер) немесе қара шляпалар деп аталады.

Хакерлік құралдарға оралу. Таңқаларлықтай, олардың көпшілігі ақ шляпалармен жасалған. Мәселе мынада, оларды раскальдар да пайдалана алады (және қолдана алады), бірақ бұл құралдар бастапқыда компьютерлік жүйелердің немесе желілердің қауіпсіздігін тексерудің ыңғайлы құралы болды. Мысалы, Nmap сияқты құрал портты сканерлеу (portscan) арқылы крекерлерге компьютерлік жүйе ұсынатын Желілік қызметтерді анықтауға көмектеседі. Nmap ұсынатын қарапайым сканерлеу технологияларының бірі-компьютерлік жүйедегі әрбір ықтимал порт нөміріне TCP қосылуға тырысу. Сәтті қосылу жүйеде осы портты тыңдайтын қызметтің бар екендігін көрсетеді. Сонымен қатар, көптеген қызметтер кеңінен танымал порт нөмірлерін қолданатындықтан, қауіпсіздікті тексеретін адам (немесе крекер) машинада қандай қызметтер жұмыс істейтінін дәл анықтай алады. Басқаша айтқанда, nmap крекерлер үшін де, қорғаушылар үшін де пайдалы құрал болып табылады, яғни оның қос мақсатты (dualuse) деп аталатын қасиеті бар. Dsniff жалпы атауы бар тағы бір құралдар жиынтығы желілік трафикті бақылаудың және желілік пакеттерді қайта бағыттаудың әртүрлі тәсілдерін ұсынады. "Төмен орбиталық иондық зеңбірек" – LowOrbitIonCannon (LOIC)-бұл алыс галактикалардағы жауларды жойып жіберетін ғылыми-фантастикалық кітаптардың қаруы ғана емес, сонымен қатар қызмет көрсетуден бас тартуға әкелетін шабуылдарды бастау құралы. Көптеген әртүрлі мақсаттарға қарсы зиянды коды бар жүздеген қолайлы құралдармен алдын ала орнатылған Metasploit ортасымен бұзу ешқашан оңай болған емес. Бұл қаражаттың барлығы екі мақсатқа ие екені түсінікті. Бірақ олар абсолютті зұлымдық деп айтуға болмайды, мысалы, пышақтар мен балталарды еске түсіріңіз.

Киберқылмыскерлер сонымен қатар қызметтердің үлкен таңдауын ұсынады (көбінесе онлайн): зиянды бағдарламаларды тарату, ақшаны жылыстату, трафикті қайта бағыттау, хостингті сұрақтарсыз қамтамасыз ету және т.б. Интернеттегі қылмыстық әрекеттердің негізгі бөлігі ботнеттер немесе ботнеттер (botnets) деп аталатын инфрақұрылымдарға негізделген, олар мыңдаған (кейде миллиондаған) вирус жұққан компьютерлерден тұрады, көбінесе бұл туралы білмейтін пайдаланушылардың қарапайым компьютерлері болып табылады. Крекерлердің жеке машиналарды жұқтырудың көптеген жолдары бар. Мысалы, олар танымал бағдарламалардың ақысыз, бірақ зиянды кодпен толтырылған нұсқаларын ұсына алады. Ащы шындық - қымбат бағдарламалардың ақысыз (бұзылған) нұсқаларының уәдесі көптеген пайдаланушыларға қарсы тұра алмайды.

Өкінішке орай, мұндай бағдарламаларды орнату крекерлерге машинаға толық қол жеткізуге мүмкіндік береді. Бұл сіздің үйіңіздің кілттерін бейтаныс адамдарға беру сияқты. Компьютер крекердің бақылауына түскенде, ол бот (bot) немесе зомби (zombie) деп аталады. Әдетте пайдаланушы мұны байқамайды. Қазіргі уақытта ботнеттер көптеген қылмыстық істердің жұмыс күші болып табылатын жүздеген мың зомбилерден тұрады. Бірнеше жүз мың дербес компьютерлер банк деректемелерін ұрлау немесе спам жіберу үшін жеткілікті және LOIC қаруын күдікті нысанаға бағыттаған миллиондаған зомбилермен қандай шайқас өткізуге болатынын қарастырған жөн.

Кейде шабуылдың салдары компьютерлік жүйелердің өзінен асып түседі және физикалық әлемге тікелей зиян келтіреді. Бір мысал, Брисбенге жақын орналасқан Австралияның Квинсленд штатындағы MaroochyShire аймағының қалдықтарды басқару жүйелеріне шабуыл болуы мүмкін. Компанияның кәріз жүйелерін монтаждау жөніндегі бұрынғы қызметкері наразы болды, өйткені MaroochyShire кеңесі

оның қызметтерінен бас тартты және олармен бірге тұруға шешім қабылдады. Ол ағынды суларды кетіру жүйесін бақылауға алып, саябақтарда, өзендерде және жағалау суларында (барлық балықтар бірден өлген жерде), сондай-ақ басқа жерлерде миллиондаған литр ағынды сулардың төгілуін ұйымдастырды.

Жалпы, белгілі бір елге немесе этникалық топқа наразы адамдар бар немесе бүкіл әлемге ашуланған және зиянның сипаты туралы да, олардың әрекеттерінің құрбаны кім болатыны туралы да ойланбастан максималды қиратуды қалайтындар бар. Әдетте, мұндай адамдар жауларының компьютерлеріне шабуыл жасау жақсы нәрсе деп санайды, бірақ шабуылдардың өзі нақты мақсатты бола алмайды.

**Негізгі әдебиеттер: [1,2,3].**
**Қосымша әдебиеттер: [8,11].**
**Бақылау сұрақтары:**
1. "Қауіпсіздік" пен "қорғаныс" арасындағы айырмашылық неде? Түсіндіріңіз.
2. Бірінші қасиеттің мәні неде?
3. Екінші қасиеттің мәні неде?
4. Үшінші қасиеттің мәні неде?
5. Киберқылмыскерлер кімдер?