**Сабақ тақырыбы:** Хакерлік әдістер

Бағытсыз хакерлік шабуылдардың әдістерін анықтау

Бағытсыз шабуыл әдістерін қолданатын хакерлер нақты ақпаратты немесе ұйымды іздемейді: кез келген жүйе бұзуға жарамды. Олардың шеберлік деңгейі өте төменнен жоғарыға дейін өзгереді, ал мотив - бұл ең алдымен жүйені бұзу арқылы назар аударуға деген ұмтылыс. Мүмкін пайда табуға деген құмарлық бар шығар, бірақ олар осылай алуға тырысқандары құпия болып қала береді.

**Шабуылдардың нысандары**

Бағытсыз шабуыл әдістерін қолданатын хакерлер кез келген жүйені іздейді. Әдетте олардың нақты мақсаты жоқ. Кейде іздеу үшін желі немесе домен атауы таңдалады, бірақ бұл таңдау әдетте кездейсоқ болады. Хакер сымсыз желіге қосыла алатын кез келген ұйым шабуыл объектісі бола алады.

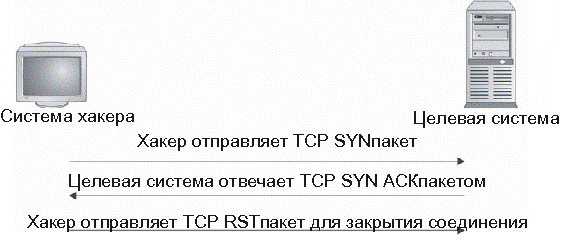
**Алдын ала зерттеу**

Хакер әртүрлі әдістермен алдын ала зерттеулер жүргізеді. Кейбіреулер желіге қосылған жүйені тапса, ешқандай «барлаусыз» және дәл нысанаға алусыз дереу шабуыл жасайды. Алдын ала тергеуден кейін шабуыл әдетте бұзылған жүйелерден жүзеге асады, осылайша хакер «ізін жабады».

**Интернет арқылы алдын ала зерттеу**

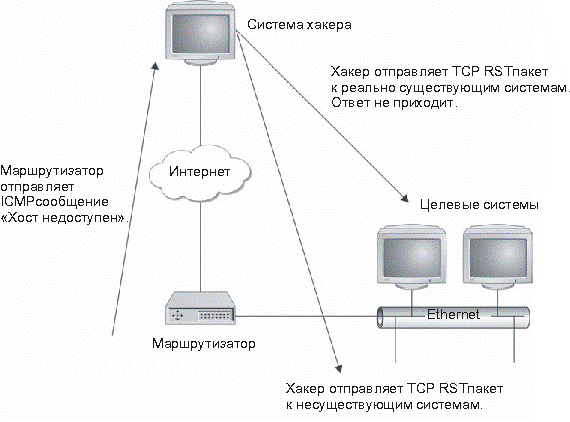
Көбінесе хакерлер IP -жартылай сканерлеу деп аталатын мекенжай диапазонында жасырын сканерлейді. Ол берілген ауқымдағы жүйелерді және сол жүйелерде қол жетімді қызметтерді анықтайды. Жасырын сканерлеу сонымен қатар осы мекенжай диапазонында кеңейтілген пинг сұрауларын орындайды, яғни әр адреске пинг сұранысын жіберу және алынған жауаптарды қарау.

Жасырын қарап шығу кезінде хакер әдетте TCP SYN пакетін IP мекенжайына жібереді және TCP SYN ACK жауабын күтеді. Жауап алған кезде, ол TCP RST пакетін байланыстың жабылуына дейін қалпына келтіру үшін жібереді (3.8 -сурет). Көптеген жағдайларда бұл мақсатты жүйедегі оқиғалар журналынан кіру әрекеттерін жасыруға мүмкіндік береді.



Сурет 3.8. Жасырын сканерлеу

Жасырын сканерлеудің бір түрі - хакер TCP RST пакетін IP мекенжайына жіберетін бастапқы қалпына келтіру сканері. Әдетте, бұл пакет қабылдаушы жүйеде ешқандай әрекет жасамайды және жауап алынбайды. Алайда, егер көрсетілген жүйе жоқ болса, онда алушының мекенжайы тиесілі желінің маршрутизаторы ICMP хабарламасымен жауап береді: «Хостқа қол жеткізу мүмкін емес» (3.9 -сурет). Ұқсас нәтиже беретін басқа да сканерлеу әдістері бар. Айта кету керек, қосылымды қалпына келтірумен сканерлеу желідегі жүйелерді анықтайды, бірақ жасырын сканерлеу сияқты оларда жұмыс істейтін қызметтерді анықтауға мүмкіндік бермейді.



Сурет. 3.9. Байланысты қалпына келтіру арқылы сканерлеу

Ескерту

Қандай порттар ашық екенін көрсету үшін жасырын сканерлеу әдістері бар. Олар әдетте трафикті белгіленген портқа жіберу арқылы жүзеге асады. Егер порт жабық болса, ол RST пакетімен жауап береді, әйтпесе жауап келмейді.

Кейде хакер бірнеше сатыда алдын ала зерттеу жүргізеді. Ол алдымен домен атауын таңдайды (әдетте ерікті) және сол доменге бағытталған DNS аймағын жіберуді бастайды. Аймақтық тасымалдау DNS -ке белгілі барлық жүйелер мен домендік IP -адрестерді тіркейді. Бұл тізіммен хакер ықтимал мақсатты операциялық жүйені анықтау үшін Queso немесе Nmap сияқты құралдарды іске қосады. Жасырын сканерлеу жүйеде жұмыс істейтін қызметтерді көрсетеді және бұл деректер нақты шабуылдар үшін қолданылады.

**Телефон арқылы алдын ала зерттеу**

Алдын ала зерттеулер тек интернет -адрестерді жинаумен шектелмейді. Қорқыту - бұл хакерлердің ықтимал құрбандарын анықтау және модемі бар және кіріс қоңырауларға жауап беретін жүйелерді анықтау үшін қолданатын тағы бір әдіс. Компьютердің көмегімен хакер бір түн ішінде модем желісінде табылған мыңдаған телефон нөмірлерін тереді. Қазіргі заманғы бағдарламалық құралдар модем мен факсты ажырата алады. Жауап беретін модемдерді анықтағаннан кейін, хакер жұмыс істейтін бағдарламаларды анықтай отырып, олардың әрқайсысымен байланысады. Кез келген жерде PC көмегімен (шабуылдаушыларға өте тартымды), хакер жауап беретін компьютерді басқарады.

**Сымсыз желілер бойынша алдын ала зерттеулер**

Ұйымдар мен үй пайдаланушыларына сымсыз желілердің тез таралуы хакерлерді іздеуге мүмкіндік береді. Жаңа «қамқоршылық» термині хакердің компьютер мен сымсыз адаптермен қаланы аралап, сымсыз желілердің кіру нүктелерін ашатынын білдіреді. Мұндай нүктелердің координаттарын жазу үшін GPS (Global Positioning System) құрылғысы қолданылады. Кейде мұндай барлау «соғысумен» бірге жүзеге асады. Хакер жаяу жүргіншілер жолындағы немесе ғимарат қабырғасындағы бор белгілерін басшылыққа алады, бұл аймақта ашық сымсыз желі бар екенін көрсетеді.

Сымсыз желі анықталғаннан кейін, хакер Интернет байланысын басқа сайттарға шабуыл жасау үшін қолданады. Бұл шабуыл әдісі хакерді керемет түрде жасырады, себебі жалған із ұйымның сымсыз желісіне әкеледі. Хакердің бар екендігі анықталса да, оның нақты орналасқан жерін білу өте қиын.

**Шабуыл әдістері**

Жалпы, бағдарланбаған шабуылдаушының бір немесе бірнеше (көп емес) ерлігі бар. Алдын ала барлау көмегімен ол осы ерліктерге осал жүйелерді табуға тырысады. Хакерлердің көпшілігі жүйені тауып, оны «бір уақытта» бұзуға тырысады. Жетілдірілген шабуылдаушылар бірнеше осал жүйелерді табу үшін арнайы сканерлеу құралдарын қолданады, содан кейін бір уақытта барлық жүйелерге қарсы шабуыл сценарийлерін жасайды.