Практикалық сабақ №1
Қауіпсіздік жүйесіндегі осалдықты анықтау

Осалдық сканерлері - бұл желілік компьютерлерді диагностикалау және бақылау үшін пайдаланылатын, оларға қауіпсіздіктің ықтимал проблемалары үшін желілерді, компьютерлерді және қосымшаларды сканерлеуге, бағалау және түзетуге мүмкіндік беретін бағдарламалық немесе аппараттық құралдар.

Осалдық сканерлері жүйеде жұмыс істейтін мүмкін қосымшалар мен протоколдарды анықтау және талдау үшін порт сканері сияқты төменгі деңгейлі құралдарды қолдана алады.

Осылайша, сканерлер келесі міндеттерді шешуге бағытталған:

- осалдықтарды анықтау және талдау;
- операциялық жүйе, бағдарламалық жасақтама және желілік құрылғылар сияқты ресурстарды түгендеу;
- осалдықтардың сипаттамасы және оларды жою нұсқалары бар есептер шығару.

Осалдық сканерлері өз жұмысында екі негізгі механизмді қолданады.

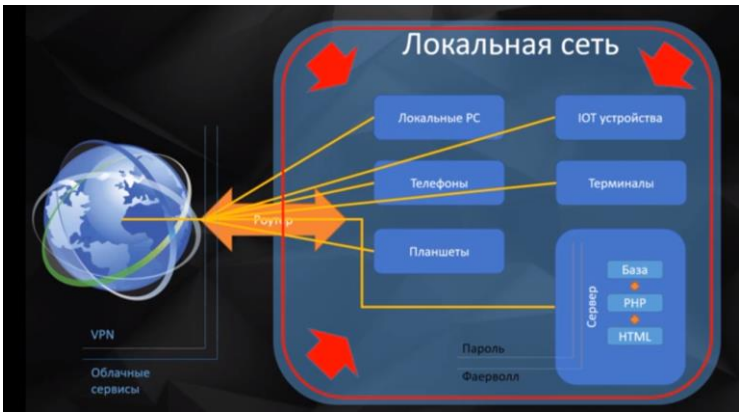
Біріншісі - дыбыстық - өте тез емес, бірақ дәл. Бұл имитациялық шабуылдарды басқаратын және осалдықтарды тексеретін белсенді талдау механизмі;

Зондта осалдықтың болуын растауға және бұрын анықталмаған «олқылықтарды» анықтауға көмектесетін шабуыл әдістері қолданылады.

Екінші механизм, сканерлеу жылдамырақ, бірақ дәлірек нәтиже бермейді. Бұл пассивті талдау, онда сканер жанама белгілерді қолдана отырып, оның бар екендігін растамай осалдық іздейді. Сканерлеу ашық порттарды анықтайды және олардың қатысты тақырыптарын жинайды.

Қарапайым әдістің бірі ретінде – Nessus Vulnerability Scanner негізінде желінің осалдығын анықтау жолдарын қарастырдық. Желі осалдығын анықтаудың негізгі мақсаты – желіні қорғаудағы әлсіз буынды анықтау.

1-суреттегі желі мысалында, роутер арқылы бүкіләлемдік байланысқа шығамыз, сонымен қатар, барлық ішкі құрылғылар өзара ешқандай құпия сөздерсіз (пароль) байланыс жасай алады.



1-сурет. Локальды желі байланысы

Осалдықты анықтаудағы міндеттер:

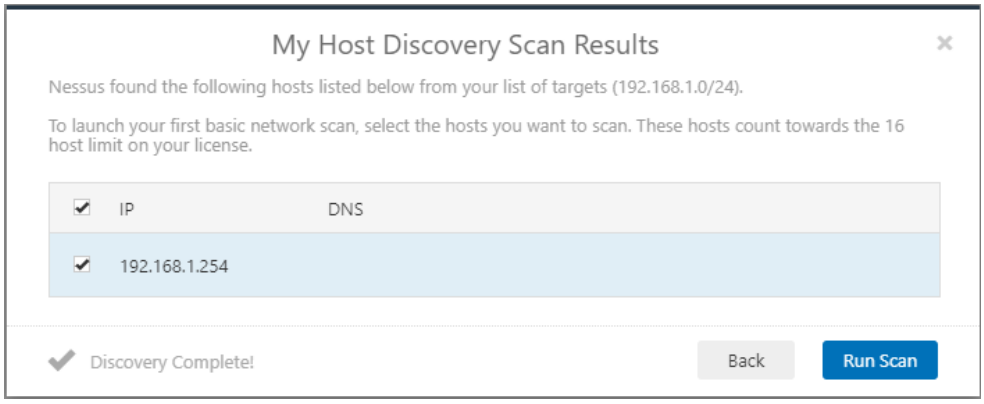
- желілік инфрақұрылымда, бағдарламалық және аппараттық құралдарда, қосымшаларда кездесетін осалдықтарды анықтау;

- анықталған «қауіпсіздік саңылауларының» гипотетикалық сценарийінің салдарын түсіндіру;

- анықталған қатерлермен күресу стратегиясын әзірлеу;

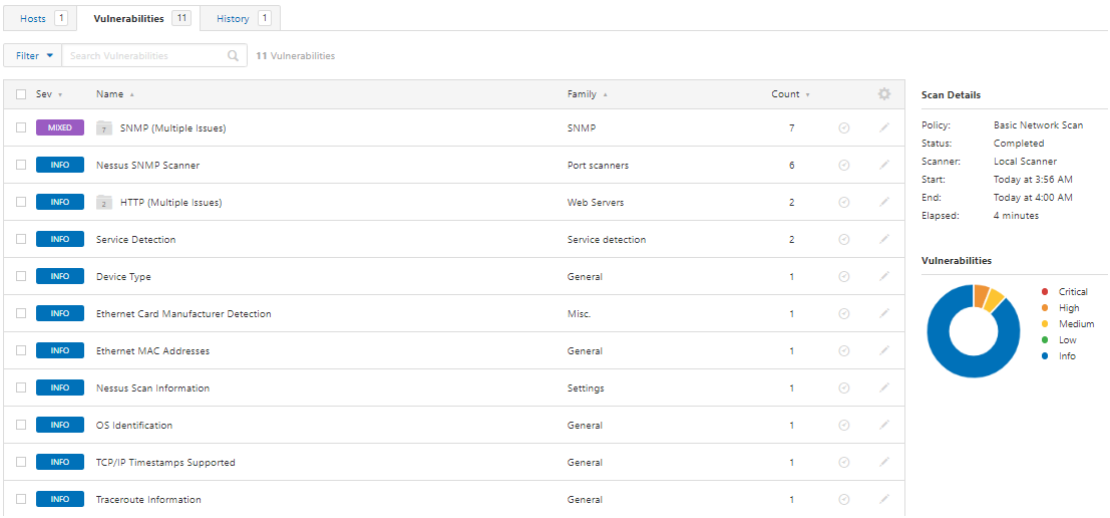
- компанияның қауіпсіздігін жақсарту және қауіпсіздік тәуекелдерін жою бойынша ұсыныстар беру.

Nessus Vulnerability Scanner толықтай орнатылғаннан соң ашылған сұқбаттық терезеде 192.168.1.0/24 IP адресінің барлық ішкі желісін сканерлейміз.



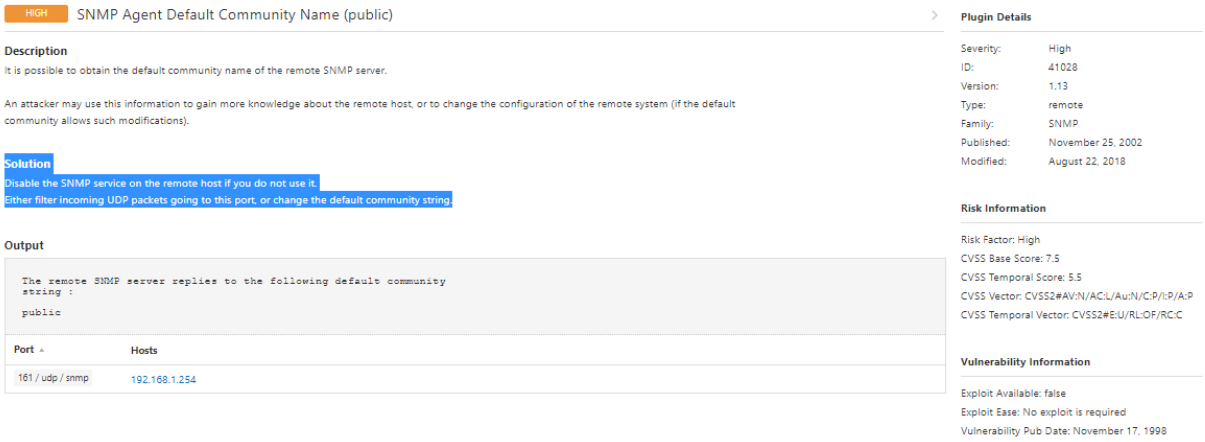
2 – сурет. Ішкі желіні сканерлеу [11]

Сканерлеу нәтижелері бойынша біз IP адрестер тізімін және осы адрестерге байланысты осалдықтарды аламыз. Осалдықтар түрлі түстермен берілген (3-сурет).



3-сурет. Сканерлеу нәтижесінде анықталған осалдықтар

Қажетті осалдықты белгілей отырып толық ақпарат алуға болады және осы есепті қалаған форматта сақтай аламыз. Мысалы, SNMP Agent Default Community Name (public) осалдығына берілген талдау және осалдықты жою жолдары 4 - суретте көрсетілген.



4-сурет. Анықталған осалдыққа талдау

Тапсырма №1: Төмендегі сарапшылардың рейтингін басқаратын осалдық сканерлерін салыстырыңыздар:

- **Symantec Security Check;**
- **XSpider;**
- **QualysGuard;**
- **Rapid 7 NeXpose;**
- **X-Scan.**