

ДОДАТОК А

Графічний матеріал атестаційної роботи

Харківський національний університет радіоелектроніки



Атестаційна робота

«Методи оцінки захищеності комп'ютерної мережі при тестуванні на проникнення»

Виконав:
Студ. гр. КСМзм-19-1
Рязанін С.Г.

Керівник:
к.т.н, доцент
Голубничий Д.Ю.

Мета та завдання атестаційної роботи

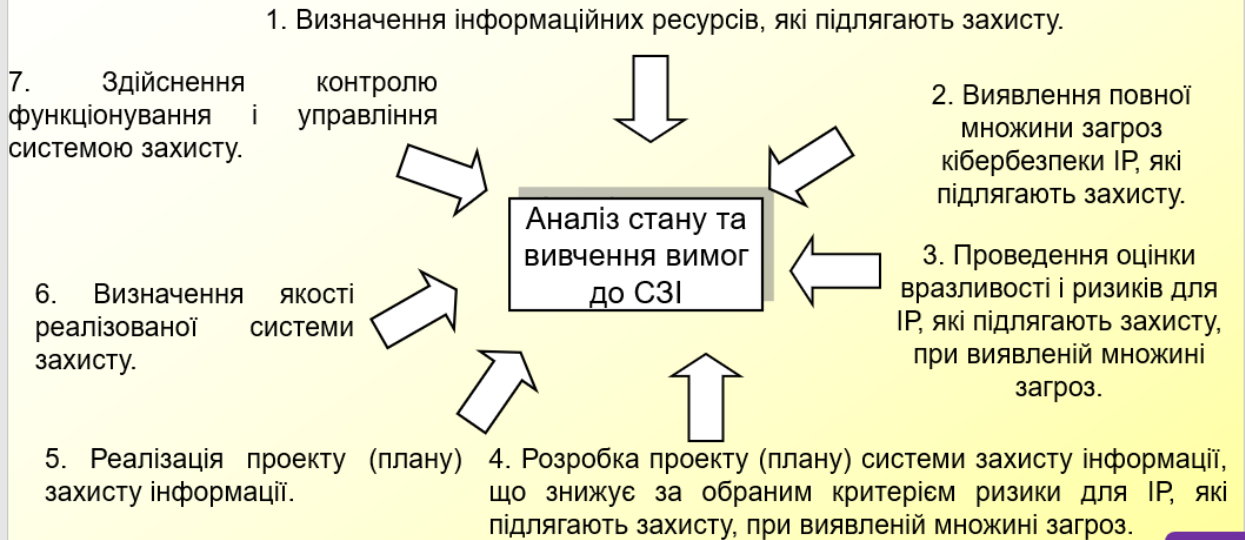
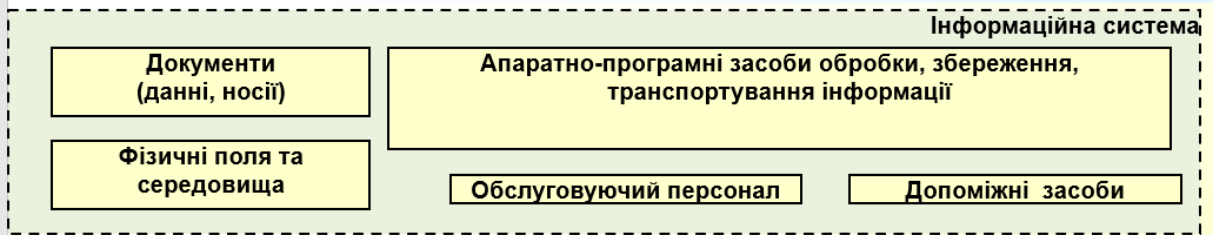
Мета атестаційної роботи :

Підвищення рівня захищеності комп'ютерної мережі за рахунок використання послуги тестування на проникнення, яка дозволяє здійснити санкціонований обхід існуючого комплексу засобів захисту власних інформаційних систем та виявити в них слабкі місця.

Науково-технічна задача, що вирішується у атестаційній роботі :

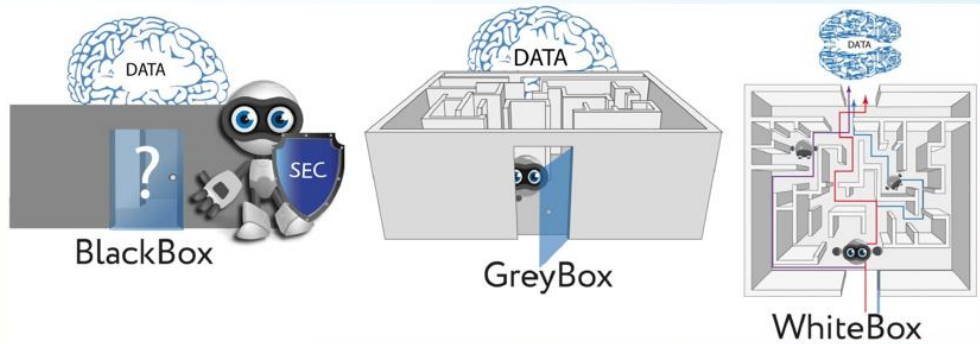
- Проведення аналізу захищеності комп'ютерної мережі як об'єкта кібербезпеки.
- Проведення аналізу вразливостей інформаційних систем та оцінка їх критичності для комп'ютерних мереж.
- Побудова методу оцінки захищеності комп'ютерної мережі за рахунок використання експлойтів при тестуванні на проникнення

Аналіз стану та вивчення вимог до СЗІ для ІС



3

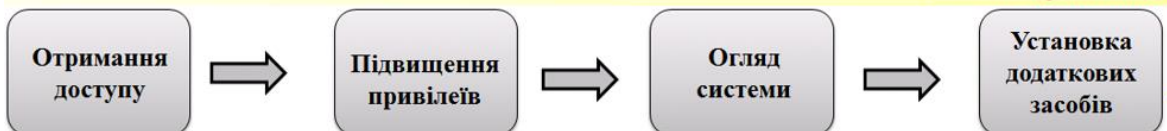
Методи тестування на проникнення



Життєвий цикл тестування



Етапи тестування на проникнення



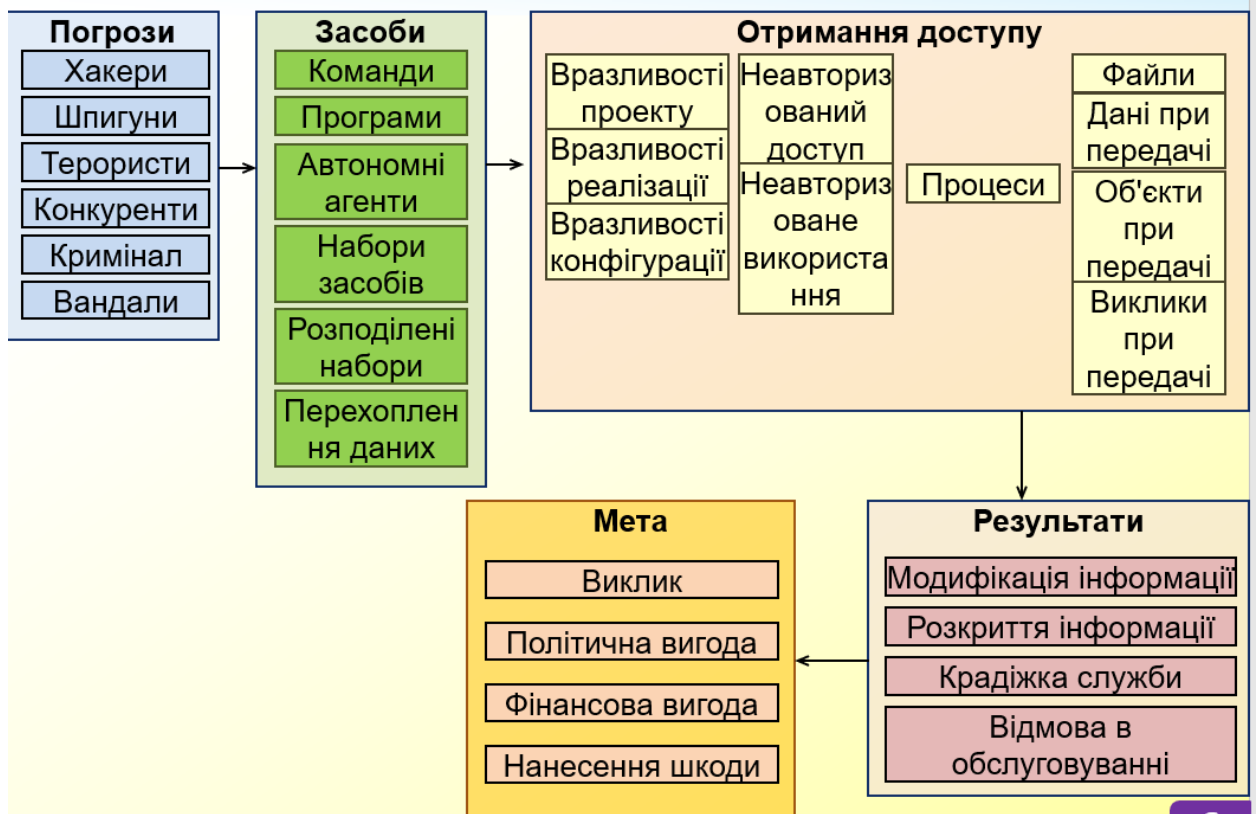
4

Класифікація можливих видів мережевих атак

Опис	Мнемонічна схема
Destruction. Атака на доступність руйнування. Руйнування інформації та/або мережевих ресурсів.	
Interruption. Атака на доступність. Переривання обслуговування, мережа недоступна або непридатна до використання	
Removal. Атака на доступність. Крадіжка, видалення або втрата інформації і/або інших ресурсів.	
Corruption. Атака на цілісність. Несанкціонована модифікація цінної інформації.	
Disclosure. Атака на конфіденційність. Несанкціонований доступ до конфіденційної інформації	

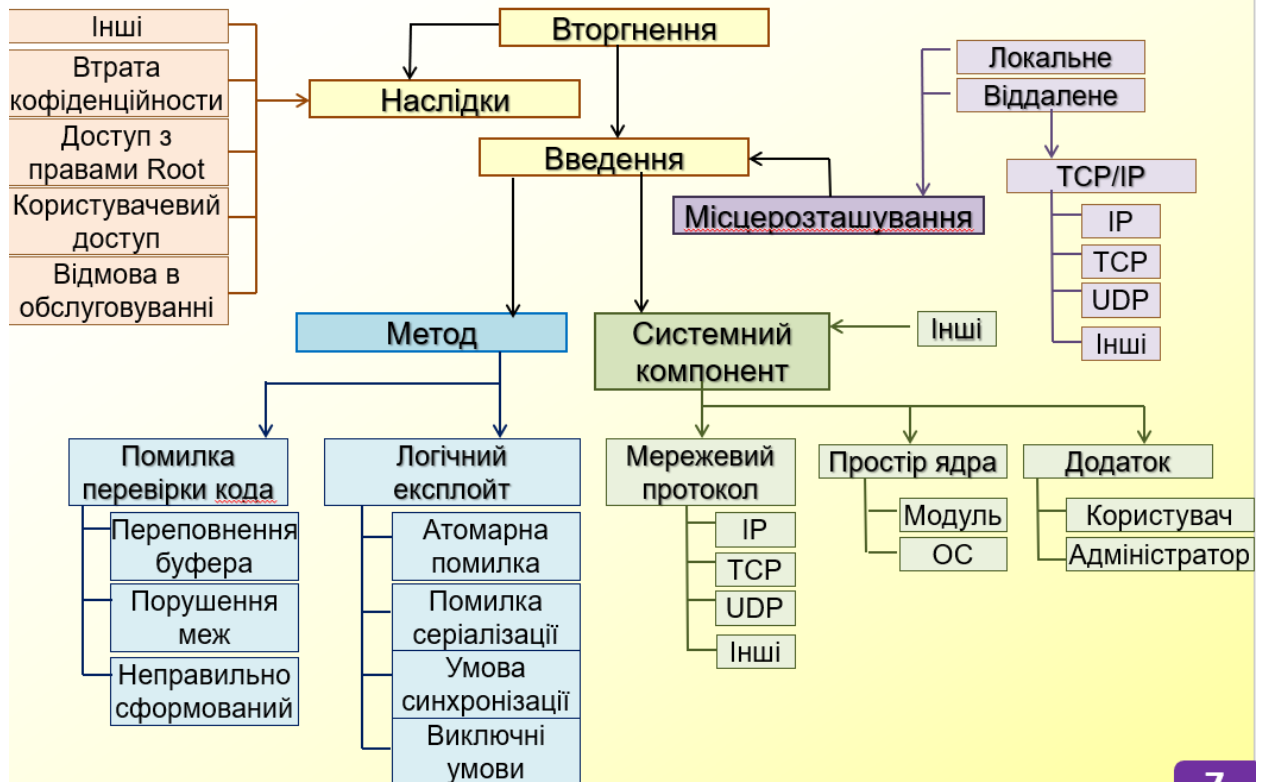
5

Таксономія атак Ховарда



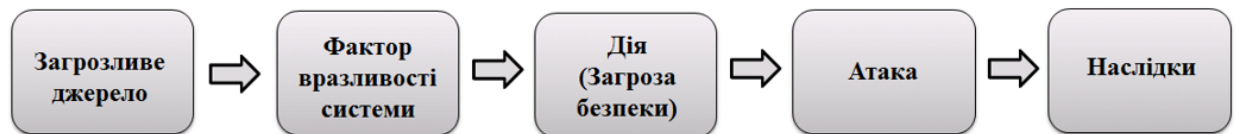
6

Повна онтологія атак



7

Логічний ланцюг трансформації інформації



Метрика	Можливі значення	
Вектор доступу (AV)	AV: L	Локальний
	AV: A	Сусідня мережа
	AV: N	Віддалений
Автентифікація (AC)	AC: H	Висока
	AC: M	Середня
	AC: L	Низька
Вплив на конфіденційність (CI)	CI: N	Ні
	CI: P	Істотне
	CI: C	Критичний
Вплив на цілісність (II)	II: N	Ні
	II: P	Істотне
	II: C	Критичний
Вплив на доступність (AI)	AI: N	Ні
	AI: P	Істотне
	AI: C	Критичний

8

Складові експлойта



Параметри експлойта

Обробник мережевих з'єднань

Shell код / корисне навантаження

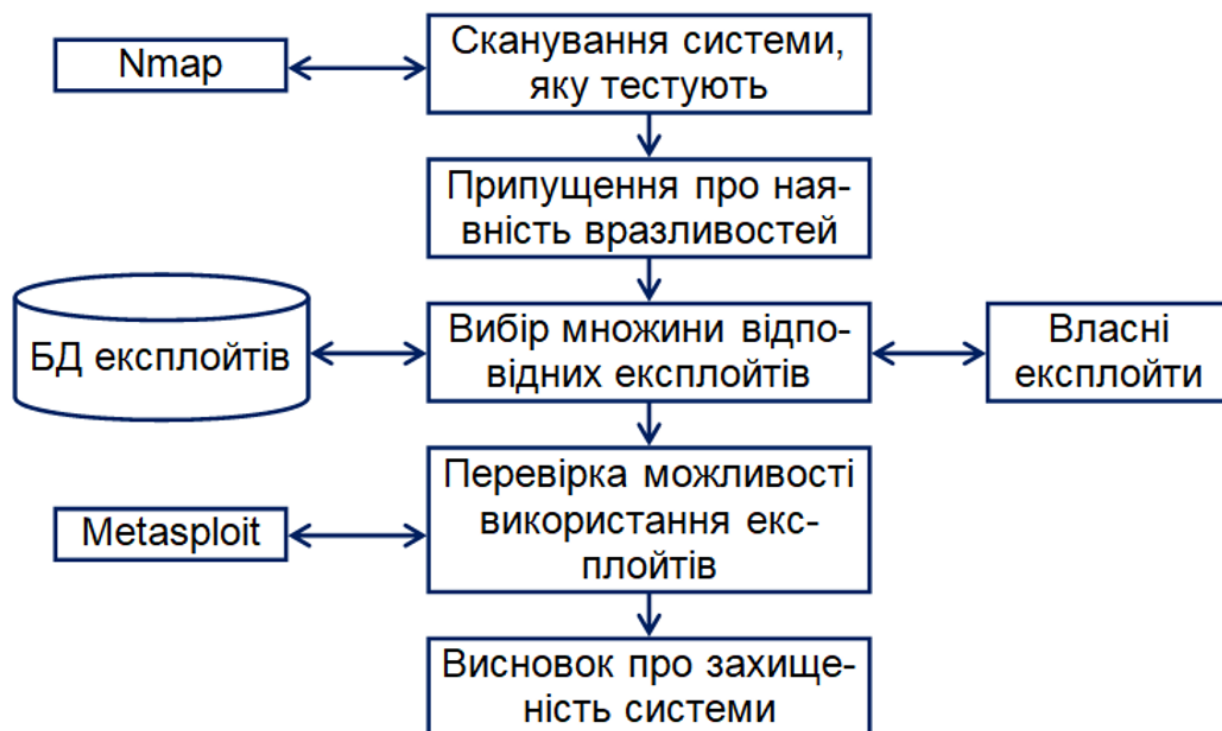
Побудовник запиту

Стандартний оброблювач

Експлойт (Exploit) – це програма, послідовність команд або частина програмного коду, що використовують вразливості в програмному забезпеченні для проведення атаки на інформаційну систему

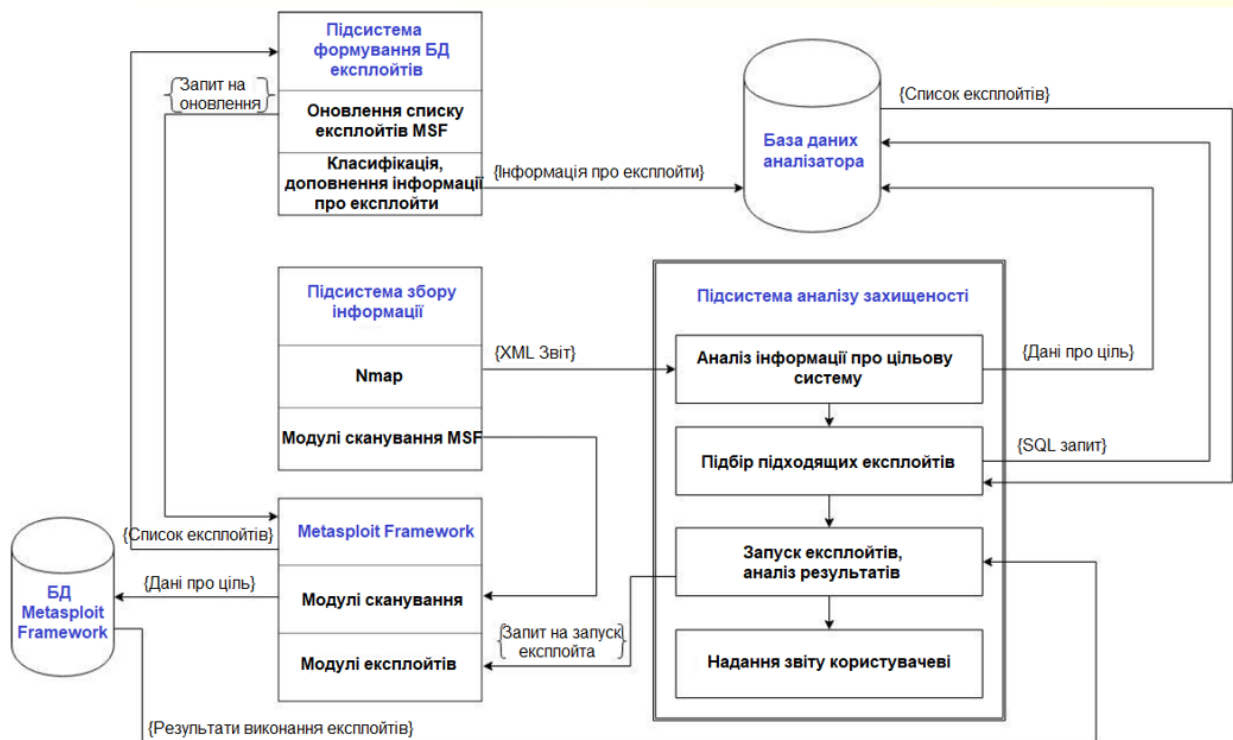
9

Схема автоматизованого тестування на проникнення



10

Архітектура розробленої системи тестування на проникнення



11

Приклад збору відомостей утилітою Nmap

The screenshot shows the Metasploit Framework interface with the following components:

- Target Properties:** IP: 192.168.01.131, MAC: 08:0c:29:3b:12:b1, DNS Name: metasploitable, OS name: Linux, OS flavor: , Service Pack: , OS lang: , OS arch: , OS purpose: server, Services count: 20.
- Nmap options:** Profile: intence scan (selected), Intence scan + UDP, Intence scan, all TCP ports, Intence scan, no ping, Quick scan, Quick scan plus, Regular scan, Slow comprehensive scan, /root/.msf4/mimic/scans/nc.
- Find Exploits:** Exploits found: 0.
- Run exploits:** Failed: 0, Exploited: 0, Error: 0.
- Exploit DB:** Exploits count: , Successful exploits: .
- Terminal Output:**

```

# nmap -R -T4 scanme.nmap.org d0ze
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2020-01-20 15:53 PST
Interesting ports on scanme.nmap.org (202.217.152.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
119/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.3
OS details: Linux 2.6.0 - 2.6.11
Uptime: 26.177 days (since Wed Feb 20 11:39:16 2020)

Interesting ports on d0ze.internal (192.168.12.31):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U FTPd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 301-1
135/tcp   open  wstask   Microsoft wstask (task server - c:\winnt\logstea32)
139/tcp   open  netbios-ssn
145/tcp   open  microsoft-ds
1025/tcp  open  wsrpc   Microsoft Windows RPC
5900/tcp  open  vnc-http
VNC Address: 00:00:00:00:00:00 (Lite on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP/7
OS details: Microsoft Windows 7 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
FlagName/Path/nmap-4.01c/Screenshots/01202004

```

12

Результати аналізу різних ОС на хостах комп'ютерної мережі

Операційні системи	Кількість виявлених запущених служб і відкритих портів	Кількість відібраних експлойтів для цільової системи	Кількість успішних експлойтів	Час виконання	
				Загальний, хв. сек.	Нормований, сек/експ. л.
Windows 10	11/11	45/1450	1/1	3 хв 02 сек	3,75
Windows 7	10/10	39/1450	3/3	2 хв 30 сек	3,84
Windows Vista	9/9	33/1450	2/3	3 хв 06 сек	5,6
Windows XP SP3	9/9	231/1450	1/1	20 хв 02 сек	5,19
Windows Server 2008 R2	10/10	37/1450	2/2	2 хв 46 сек	3,98
Windows Server 2003	4/4	95/1450	3/4	5 хв 30 сек	3,45
Mac OS X High Sierra	4/4	37/1450	1/1	5 хв 30 сек	3,75
Mac OS X Sierra	5/5	65/1450	1/1	4 хв 27 сек	4,23
Linux Mint 17	2/2	84/1450	0/0	4 хв 34 сек	3,25
CentOS 7	1/1	8/1450	1/1	0 хв 41 сек	3,17
Metasploitable 2	30/30	283/1450	7/7	25 хв 45 сек	5,43

13

Методи тестування на проникнення



Метод Open Source Security Testing Methodology



Метод Information Systems Security Assessment Framework

Метод NIST Special Publications 800-115



14

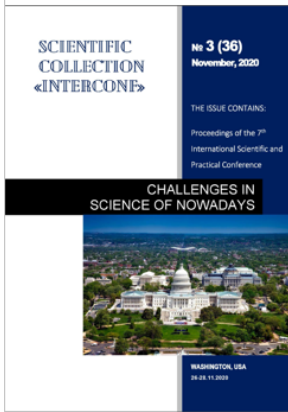
Структурно-логічна схема та алгоритм проведення pentest



Підходи до проведення pentest



Апробація результатів



GENERAL ENGINEERING AND MECHANICS	PRODUCTS	1318
1318	1318	1318
1319	1319	1319
1320	1320	1320
1321	1321	1321
1322	1322	1322
1323	1323	1323
1324	1324	1324
1325	1325	1325
1326	1326	1326
1327	1327	1327
1328	1328	1328
1329	1329	1329
1330	1330	1330
1331	1331	1331
1332	1332	1332
1333	1333	1333
1334	1334	1334
1335	1335	1335
1336	1336	1336
1337	1337	1337
1338	1338	1338
1339	1339	1339
1340	1340	1340
1341	1341	1341
1342	1342	1342
1343	1343	1343
1344	1344	1344
1345	1345	1345
1346	1346	1346
1347	1347	1347
1348	1348	1348
1349	1349	1349
1350	1350	1350
1351	1351	1351
1352	1352	1352
1353	1353	1353
1354	1354	1354
1355	1355	1355
1356	1356	1356
1357	1357	1357
1358	1358	1358
1359	1359	1359
1360	1360	1360
1361	1361	1361
1362	1362	1362
1363	1363	1363
1364	1364	1364
1365	1365	1365
1366	1366	1366
1367	1367	1367
1368	1368	1368
1369	1369	1369
1370	1370	1370
1371	1371	1371
1372	1372	1372
1373	1373	1373
1374	1374	1374
1375	1375	1375
1376	1376	1376
1377	1377	1377
1378	1378	1378
1379	1379	1379
1380	1380	1380
1381	1381	1381
1382	1382	1382
1383	1383	1383
1384	1384	1384
1385	1385	1385
1386	1386	1386
1387	1387	1387
1388	1388	1388
1389	1389	1389
1390	1390	1390
1391	1391	1391
1392	1392	1392
1393	1393	1393
1394	1394	1394
1395	1395	1395
1396	1396	1396
1397	1397	1397
1398	1398	1398
1399	1399	1399
1400	1400	1400
1401	1401	1401
1402	1402	1402
1403	1403	1403
1404	1404	1404
1405	1405	1405
1406	1406	1406
1407	1407	1407
1408	1408	1408
1409	1409	1409
1410	1410	1410
1411	1411	1411
1412	1412	1412
1413	1413	1413
1414	1414	1414
1415	1415	1415
1416	1416	1416
1417	1417	1417
1418	1418	1418
1419	1419	1419
1420	1420	1420
1421	1421	1421
1422	1422	1422
1423	1423	1423
1424	1424	1424
1425	1425	1425
1426	1426	1426
1427	1427	1427
1428	1428	1428
1429	1429	1429
1430	1430	1430
1431	1431	1431
1432	1432	1432
1433	1433	1433
1434	1434	1434
1435	1435	1435
1436	1436	1436
1437	1437	1437
1438	1438	1438
1439	1439	1439
1440	1440	1440
1441	1441	1441
1442	1442	1442
1443	1443	1443
1444	1444	1444
1445	1445	1445
1446	1446	1446
1447	1447	1447
1448	1448	1448
1449	1449	1449
1450	1450	1450
1451	1451	1451
1452	1452	1452
1453	1453	1453
1454	1454	1454
1455	1455	1455
1456	1456	1456
1457	1457	1457
1458	1458	1458
1459	1459	1459
1460	1460	1460
1461	1461	1461
1462	1462	1462
1463	1463	1463
1464	1464	1464
1465	1465	1465
1466	1466	1466
1467	1467	1467
1468	1468	1468
1469	1469	1469
1470	1470	1470
1471	1471	1471
1472	1472	1472
1473	1473	1473
1474	1474	1474
1475	1475	1475
1476	1476	1476
1477	1477	1477
1478	1478	1478
1479	1479	1479
1480	1480	1480
1481	1481	1481
1482	1482	1482
1483	1483	1483
1484	1484	1484
1485	1485	1485
1486	1486	1486
1487	1487	1487
1488	1488	1488
1489	1489	1489
1490	1490	1490
1491	1491	1491
1492	1492	1492
1493	1493	1493
1494	1494	1494
1495	1495	1495
1496	1496	1496
1497	1497	1497
1498	1498	1498
1499	1499	1499
1500	1500	1500



Голубничий Д.Ю. Технології аудиту кібербезпеки інформаційних систем / Д.Ю.Голубничий, О.В. Коломійцев, В.Ф.Третяк, С.Г.Рязанін // Scientific Collection «InterConf», (36): with the Proceedings of the 7th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26 - 28, 2020) in Washington, USA: EnDeavour Publishers, 2020. – Pp. 333 – 342.
<https://ojs.ukrlogos.in.ua/index.php/interconf/issue/view/26-28.11.2020/396>.

Висновки

В результаті даної роботи були:

- 1. Проаналізовані підходи до проведення аудиту кібербезпеки** за рахунок технології тестування проникнення. Таким чином, на основі приведених результатів досліджень можливо сформулювати основні завдання, рекомендації та базові пропозиції щодо підходів до забезпечення кібербезпеки, яка циркулює в комп'ютерних мережах.
- 2. Проведено аналіз вразливостей інформаційних систем** та оцінка її критичності для комп'ютерних мереж. Аналіз дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.
- 3. Проведено аналіз існуючих методів тестування засобів захисту інформації, обрані допоміжні інструменти, з використанням яких була розроблена архітектура системи моделювання атак і реалізований прототип програмного засобу.**

Розроблену систему можна вдосконалити в декількох напрямках:

- ✓ можливість аудиту цілої комп'ютерної мережі, а не тільки окремого одного хоста;
- ✓ комбінування декількох мережевих сканерів;
- ✓ автоматизація процесів після успішної експлуатації системи.