Модуль: Реагування на інциденти безпеки інформації



Практична вправа:

«Виявлення провісників та індикаторів інциденту інформаційної безпеки»



Навчальна мета заняття: навчитись виявляти провісники та індикатори інцидентів інформаційної безпеки.



Місце проведення: комп'ютерний клас.



Устаткування:

Час проведення: 1 год.

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі Інтернет, веббраузер Google Chrome.

Порядок проведення заняття

Задача 1.

- 1. Налаштувати ведення та забезпечення доступу до журналу подій Windows Defender Firewall.
- 2. Встановити Nmap Security Scanner та здійснити сканування системи, яке розглядається як підготовка до атаки.
- 3. Виявити провісники атаки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Windows Defender Firewall with Advanced Security (пошуковим виразом може бути «Засоби адміністрування») (рис. 1).

Найкраца відповідність Найкраща відповідність Умілдомз Defender Firewall with Advanced Security Програма для настільного комп'юте Image: Security Image: Security Програма для настільного комп'юте Vindows Defender Firewall with Advanced Security Image: Security Програма для пошуку Пропозиції для пошуку Image: Security Image: Security Image: Security Ponosuli для пошуку Image: Security Image: Security Image: Security Pinonsuli для пошуку Image: Security Image: Security Image: Security Bescraitru (1) Image: Security Image: Security	Усі Програми	Документи	Настройки	Веб	Додатково 🗸	Відгук	
№ Windows Defender Firewall with Advanced Security Програма для настільного комп'ютеля. → № Windows Defender Firewall with Advanced Windows Defender Firewall with Advanced Security • Firefox > № • Гриватний перегляд Firefox > № • Приватний перегляд Firefox > № • Пропозиції для пошуку № fi - Переглянути результати пошуку в № > □ • Білеритаі Настройки (1+) □ Відкрити розташування файлу Веб-сайти (1) № № №	Найкраща відпові,	цність					
Програми Windows Defender Firewall with Advanced • Firefox > © Приватний перегляд Firefox > Phonoswuïi для пошуку Програма для настільного комп'ютера Phonoswuïi для пошуку Г Phonoswuïi для пошуку Г Phonoswuïi для пошуку Г Phonoswuïi для пошуку в Інтернеті > Be6-сайти (1) Г	Windows I Advanced Програма д	Defender Firewal Security ля настільного ког	with →				
 Firefox Firefox Приватний перегляд Firefox Пропрама для настільного комп'ютера Пропрама для настільного комп'ютера Відкрити Відкрити Су у режимі адміністратора Відкрити розташування файлу Веб-сайти (1) Веб-сайти (1) 	Програми				Windows Defender Firewall with A	dvanced	
Приватний перегляд Firefox Програма для настільного комп'ютера Пропозиції для пошуку Відкрити Г Відкрити Г Відкрити Г Відкрити Відкрити С У рехимі адміністратора Відкрити розташування файлу Веб-сайти (1) -13 Закріпити в меню Тірск*	ۏ Firefox		>		Security		
Пропозиції для пошуку	🧐 Приватний г	ерегляд Fi refox	>		Програма для настільного комп'юте	.pa	
 № fi - Переглянути результати пошуку в У С У режимі адміністратора Настройки (1+) Відкрити розташування файлу Веб-сайти (1) на закріпити в меню "Пуск" 	Пропозиції для по	шуку			and the		
Настройки (1+) 🔃 Відкрити розташування файлу Веб-сайти (1) – +Закріпити в меню "Пуск"	Я fi - Переглянут Інтернеті	и результати пош	ку в >		 ыдкрити У режимі адміністратора 		
Веб-сайти (1) -Н Закріпити в меню "Пуск"	Настройки (1+)				🚺 Відкрити розташування файлу		
No. 1	Веб-сайти (1)				-🛱 Закріпити в меню "Пуск"		
т⊶ Закріпити на панелі завдань					🛱 Закріпити на панелі завдань		
0 4	0 4						

Рис. 1. Відкриття Windows Defender Firewall with Advanced Security

У Windows Defender Firewall with Advanced Security (рис. 2):

- відкрити налаштування Windows Defender Firewall Properties;
- пересвідчитись, що Firewall активований (Firewall state: on);
- для кожної вкладки Domaine Profile, Private Profile, Public Profile через опцію Logging – Customize включити записування у журнал подій про блокування мережевих пакетів (Log dropped packets: Yes) та успішне встановлення мережевого з'єднання (Log successful connections: Yes).



Рис. 2. Налаштування журналу подій Windows Defender Firewall

У каталозі C:\Windows\System32\LogFiles\Firewall знайти файл pfirewall.log (рис. 3).

Файл Основне Спільний доступ Вигляд 🗸	
	\sim (?)
← → • ↑ 🖡 C:\Windows\System32\LogFiles\Firewall V Ū Ποшук: Firewall	vall 🗸 🗸 Vall 🖉
▲ Ім'я Дата змінення Тип Розмір	Дата змінення Тип Розмір
р Deskton страници с	18.05.2023 1:30 Текстовий докум 36 КБ
■ Desktop / ■ pfirewall.log.old 18.05.2023 1:27 Файл OLD 0 КБ	18.05.2023 1:27 Файл OLD 0 КБ
Documents *	

Рис. 3. Локація журналу подій pfirewall.log

Через властивості файлу pfirewall.log перейти по вкладкам Безпека – Додатково – Дозволи – Продовжити (рис. 4), а потім – Увімкнути успадкування (рис. 5).



Рис. 4. Налаштування параметрів доступу до файлу pfirewall.log

м'я:	C:\\	Windows\System32\LogFiles\	Firewall\pfirewall.log			
Власник:	Adr	ministrators (MSEDGEWIN10\A	Administrators) Зміни	ти		
Дозволи	Аудит	Чинний доступ				
"Редагувати Записи дозв	(якщо вона дост олів:	упна).	locara	Успаниовано від		.7
69 Л ана	принципал		Доступ	Успадковано від		
Дозв	SVSTEM		Повний доступ	Немає		
Дозв	Administrators (MSEDGEWIN10\Administra	Повний доступ	Немає		
Дозв	Network Configu	uration Operators (MSEDGE	Повний доступ	Немає		
Додати	Видали	ти Перегляд			 	

Рис. 5. Увімкнення успадкування прав доступу для файлу pfirewall.log

Переконатися, що файл журналу pfirewall.log доступний для читання, відкривши його текстовим редактором (рис. 6).

pfirewall.log - Блокнот X Файл Редагування Формат Вигляд Довідка #Version: 1.5 #Software: Microsoft Windows Firewall #Time Format: Local #Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path 2023-05-18 01:27:37 ALLOW UDP 10.0.2.9 192.168.0.1 59169 53 0 - - - - - SEND 2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 78.154.186.177 51230 80 0 - 0 0 0 - - - SEND 2023-05-18 01:27:37 ALLOW UDP 10.0.2.9 192.168.0.1 61346 53 0 -SEND 2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 23.64.225.161 51231 443 0 - 0 0 0 - SEND 2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 8.253.190.121 51232 80 0 - 0 0 0 -SEND 2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 8.253.95.121 51233 80 0 - 0 0 0 -SEND 2023-05-18 01:27:38 ALLOW UDP 10.0.2.9 192.168.0.1 54942 53 0 -SEND 2023-05-18 01:27:38 ALLOW TCP 10.0.2.9 78.154.186.153 51234 80 0 - 0 0 0 - - SEND 2023-05-18 01:27:38 ALLOW TCP 10.0.2.9 209.197.3.8 51235 80 0 - 0 0 0 -SEND 2023-05-18 01:27:38 ALLOW TCP 10.0.2.9 209.197.3.8 51236 80 0 - 0 0 0 SEND 2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 52.168.117.170 51237 443 0 - 0 0 0 2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 209.197.3.8 51238 80 0 - 0 0 0 - -- - SEND SEND 2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 209.197.3.8 51239 80 0 - 0 0 0 SEND 2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 13.107.4.50 51240 80 0 - 0 0 0 SEND 2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 41.63.96.0 51241 80 0 - 0 0 0 -SEND 2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 41.63.96.128 51242 80 0 - 0 0 0 - SEND 2023-05-18 01:27:40 ALLOW TCP 10.0.2.9 52.168.117.170 51243 443 0 - 0 0 0 - SEND 2023-05-18 01:27:40 ALLOW TCP 10.0.2.9 209.197.3.8 51244 80 0 - 0 0 0 - - - SEND

Рис. 6. Зміст журналу аудиту Microsoft Windows Firewall

У журналі аудиту Microsoft Windows Firewall (рис. 6) зазначені: дата і час, дозвіл на встановлення з'єднання (ALLOW), протокол з'єднання (UDP, TCP), IP адреси з'єднання (src-ip, dst-ip), порти з'єднання (src-port, dst-port), інше. Завантажити та встановити Nmap Security Scanner в OC Windows (https:// nmap.org/download#windows) (рис. 7).



Рис. 7. Сторінка завантаження Nmap Security Scanner для ОС Windows

Відкрити сканер через ярлик «Nmap – Zenmap GUI», у полі Target вписати loopback IP адрес своєї системи: 127.0.0.1 та у режимі Quick scan plus запустити сканування (рис. 8). Сканування є підготовчим етапом перед атакою на систему, при якому здійснюється послідовний перебір портів підключення до цільової системи.

Zenmap Scan Tools Profile Help	X
scan <u>roois</u> <u>Frome</u> <u>rep</u>	
Target: 127.0.0.1	V Profile: Quick scan plus V Scan Cancel
Command: nmap -sV -T4 -O -Fvers	ion-light 127.0.0.1
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans
OS ◀ Host ▲	nmap -sV -T4 -O -Fversion-light 127.0.0.1 🗸 🖉 Details
Iocalhost (127.0.0.1)	<pre>Starting Nmap 7.93 (https://nmap.org) at 2023-05-18 04:26 NSOCK ERROR [0.8310s] ssl_init_helper(): OpenSSL legacy provider failed to load. Nmap scan report for localhost (127.0.0.1) Host is up (0.00021s latency). Not shown: 98 closed tcp ports (reset) PORT STATE SERVICE VERSION 135/tcp open msrpc Microsoft Windows RPC 445/tcp open microsoft-ds? Device type: general purpose Running (JUST GUESSING): Microsoft Windows 10 7 Longhorn 8.1 2008 Vista (98%) OS CPE: cpe:/o:microsoft:windows_10 cpe:/ o:microsoft:windows_7::spl cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8.1:rl cpe:/ o:microsoft:windows_vista::spl cpe:/ o:microsoft:windows_8 Aggressive OS guesses: Microsoft Windows 10 1809 -</pre>
Filter Hosts	1909 (98%), Microsoft Windows 10 1709 - 1803 (95%), 👻

Рис. 8. Запуск сканування своєї системи

Відкрити файл журналу аудиту pfirewall.log та знайти записи, які свідчать про сканування портів системи і є провісниками майбутньої атаки на систему (рис. 9). Основною ознакою сканування є наявність великою кількості одночасних підключень з одного IP адреса до різних портів системи.

pfirewall.lo	g - Блокнот						
Файл Редагуе	вання Форм	ат Вигля	яд Д	овідка			
2023-05-18	04:26:17	ALLOW	UDP	10.0.2.9	192.168.0.1	55398	3530SEND
2023-05-18	04:26:17	ALLOW	TCP	127.0.0.1	127.0.0.1	61546	3389 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	23 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	1025 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	8888 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	443 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	139 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	80 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	1720 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	25 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	110 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	TCP	127.0.0.1	127.0.0.1	61546	143 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	111 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	1723 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	3306 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	21 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	587 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	995 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	135 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	8080 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	113 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	TCP	127.0.0.1	127.0.0.1	61546	445 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	TCP	127.0.0.1	127.0.0.1	61546	53 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	22 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	5900 0 - 0 0 0 SEND
2023-05-18	04:26:17	ALLOW	тср	127.0.0.1	127.0.0.1	61546	993 0 - 0 0 0 SEND

Рис. 9. Записи журналу аудиту pfirewall.log, які свідчать про сканування портів системи

Заповнити шаблон звіту про подію інформаційної безпеки (табл. 1).

Таблиця 1. Шаблон звіту про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОГ	РМАЦІЙНОЇ БЕЗПЕКИ						
1. Дата події	 Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне) 						
2. Номер події (надається фахівцем ISIRT)							
4. РЕКВІЗИТИ ОСС	БИ, ЯКА ЗВІТУЄ						
4.1. Ім'я та прізвище	4.2. Адреса						
4.3. Організація	4.4. Відділ						
4.5. Телефон	4.6. E-mail						
5. ОПИС ПОДІЇ ІНФОР	МАЦІЙНОЇ БЕЗПЕКИ						
 5.1. Опис події: Що сталося Яким чином сталося Чому так сталося Які компоненти/активи піддались впливу Оцінка впливу на діяльність організації Будь-які виявлені вразливості 							
6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ							
6.1. Дата та час події							
6.2. Дата та час виявлення події							
6.3. Дата та час повідомлення про подію							
6.4. Чи відповідь на цю подію усунула небезпеку?	ТАК 🗆 НІ 🗆 (позначте відповідне)						
6.5. Якщо так. вкажіть, скільки часу тривала подія (у днях/годинах/ хвилинах)							

Задача 2.

1. Налаштувати аудит входу користувача в систему.

2. Ввести кілька разів неправильний пароль при вході до OC Windows.

3. Виявити індикатори інциденту інформаційної безпеки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Налаштування групової політики (Edit group policy) (рис. 10).

Усі Програми Документи Настр	ойки Ве	еб Додатково ∨ Відгук
Найкраща відповідність		
Edit group policy Панель керування	\rightarrow	
Програми		1 <u>\$</u>
🧿 Google Chrome	>	Edit group policy
G roove Music	>	панель керування
💽 Solitaire & Casual G ames	>	E Biorouzu
Пропозиції для пошуку		С БІДКРИТИ
д - Переглянути результати пошуку в Інтернеті	>	
Документи (3+)		
Папки (2+)		
₽ g		

Рис. 10. Відкриття Налаштування групової політики (Edit group policy)

У розділі Конфігурація комп'ютера – Налаштування Windows – Security Settings – Advanced Audit Policy Configuration – «System Audit Policies – Local Group Policy Object» – Account Logon кликнути на параметр Audit Credential Validation та налаштувати аудит вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему (рис. 11).



Рис. 11. Налаштування аудиту вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему

Після кількох спроб введення неправильного паролю (рис. 12) через рядок пошуку відкрити Переглядач подій (Event Viewer) - Windows Log - Security та знайти невдалі спроби вводу паролю (рис. 13).



Рис. 12. Результат введення неправильного паролю

🛃 Event Viewer									
Файл Дія Вигляд Довідка									
🗢 🔿 🙍 🖬 👔									
Event Viewer (Local)	Security Number of	f events: 24 843							
 Gustom Views 									
🛛 🝸 Administrative Events	Keywords	Date and Time		Source					
🍸 Summary page events	Audit Success	19.05.2023 15:24:55		Microsoft Windows security auditing.					
🗸 📫 Windows Logs	Audit Failure	19.05.2023 15:24:49		Microsoft Windows security auditing.					
Application	🔒 Audit Failure	19.05.2023 15:24:47		Microsoft Windows security auditing.					
Security	🔒 Audit Failure	19.05.2023 15:24:45		Microsoft Windows security auditing.					
Setup	🔒 Audit Failure	19.05.2023 15:24:41		Microsoft Windows security auditing.					
System	Audit Success	19.05.2023 15:23:54		Microsoft Windows security auditing.					
Forwarded Events	Audit Success	19.05.2023 15:23:10		Microsoft Windows security auditing.					
 Applications and Services Loc 	Audit Success	19.05.2023 15:22:56		Microsoft Windows security auditing.					
Subscriptions	Audit Success	19.05.2023 15:22:56		Microsoft Windows security auditing.					
	<								
	Event 4776, Microsoft Windows security auditing.								
	Canaral D. I. I								
	General Details								
	The commuter atte								
	The computer atte	empted to validate the credent	tials for an accou	nt.					
	Authentication Pa	ckage: MICROSOFT_AUTHE	NTICATION_PAG	CKAGE_V1_0					
	Logon Account:	IEUser							
	Source Workstatio	n: MSEDGEWIN10							
	Error Code.	0XC 000000A							
	I								
	Log Name:	Security							
	Source:	Microsoft Windows security a	Logged:	19.05.2023 15:24:49					
	Event ID:	4776	Task Category:	Credential Validation					
	Level:	Information	Keywords:	Audit Failure					
	User	NI/A	Computer	MSEDGEWIN10					
	OnCoder		compater.	WSLDGLWINIO					
	OpCode:	into							
	More Information:	Event Log Online Help							

Рис. 13. Записи журналу подій про невдалі спроби входу у систему

Заповнити шаблон звіту про подію інформаційної безпеки (табл. 1).