Приложение на инструменти за мониторинг и анализ на сигурността в Windows в обучението

Светослав Хаджитодев

Applying Windows Security Monitoring and Analysis Tools in Education

Svetoslav Hadzhitodev

Abstract:
Blended learning enables practical classes to be conducted in specialized laboratories and virtual environments, in which students work with vulnerability testing tools. This approach allows students and cadets from the N. Y. Vaptsarov Naval Academy to gain practical experience in a real environment, while simultaneously developing skills in risk analysis, assessment and management. Their integration into laboratory exercises within the framework of blended learning significantly increases the effectiveness of the preparation of future cybersecurity specialists. Software products and functions such as Event Viewer, Sysmon, Microsoft Defender, Autoruns, Process Explorer and TCPView for security analysis of Windows operating systems are applied in the learning process.
Keywords: киберсигурност, Windows, мониторинг, логове, анализ, обучение

For contacts: Assist. Prof. Svetoslav Hadzhitodev, N. Y. Vaptsarov Naval Academy, s.hadzhitodev@naval-acad.bg

ВЪВЕДЕНИЕ

С нарастващата сложност на киберзаплахите се увеличава необходимостта от добре подготвени специалисти по информационна сигурност. Ефективното обучение изисква не само теоретични знания, но и практически умения за работа с реални инструменти.

Операционната система Windows е една от най-разпространените платформи, което я прави основна цел на кибератаки. Според данните от Statcounter Global Stats за април 2026 г., тя има пазарен дял от 63,6% от всички Desktop операционни системи по света. [13] Познаването на инструментите за мониторинг и анализ, които предоставя тя, е ключово за откриване на инциденти, реакция и превенция. Обучението на бъдещи киберспециалисти трябва да включва работа с реални инструменти, които се използват в индустрията.

ИЗЛОЖЕНИЕ

1. Вградени инструменти в Windows

Операционната система Windows разполага с вградени механизми, които са фундаментални за разбирането на системната сигурност. Обучаемите трябва да овладеят тези инструменти, преди да преминат към по-сложни методи за анализ.

Microsoft Defender е вграденият антивирусен софтуер в Windows и предоставя защита в реално време срещу вируси, зловреден софтуер и шпионски програми. В учебна среда обучаемите анализират как Defender използва евристика и поведенчески анализ за блокиране на заплахи, както и как администраторите могат да управляват политиките за сигурност, да изолират заразени машини и да извършват разследвания чрез Windows Security. Вградените му настройки позволяват управление на правилата на защитната стена, защита на информацията от ransomware чрез позволяване на достъп само на надеждни

приложения до защитени от потребителя директории, с помощта на функцията *Controlled folder access*, блокиране на злонамерени или ненадеждни приложения чрез *Smart App Control*, предотвратяване на атаки от вмъкване на зловреден код в процеси с висока защита чрез *Memory Integrity* и защита срещу фишинг и зловредни сайтове и файлове чрез *SmartScreen*. [2, 3, 4, 7]

Event Viewer е системен инструмент за преглед на логове в Windows, който позволява преглед, анализ и управление на системни, защитни и приложни събития. [5] Комбинирайки прозрачност и подробна отчетност, Event Viewer остава критичен елемент за поддръжката и сигурността на Windows системите. Използва се при разследване на инциденти, откриване на неуспешни опити за влизане и анализ на системни грешки. Обучаемите могат да развият умения за интерпретиране на логове и откриване на подозрителни събития.

System Monitor (Sysmon) е усъвършенствана системна услуга и драйвер, който наблюдава и записва дейностите в системата в дневника за събития в Windows. Той разширява възможностите на Event Viewer, като записва данни за създаването на процеси (включително и техните hash стойности), мрежови връзки и промени във времето на създаване на файлове. [12] Sysmon е част от пакета Sysinternals и е наскоро вграден в Windows 11, но е изключен по подразбиране. [1] За бъдещите киберспециалисти, е незаменим инструмент за проследяване на индикатори за компрометиране и разбиране на поведението на зловредния код.

2. Допълнителни инструменти от Sysinternals

Пакетът Sysinternals, създаден от Mark Russinovich, предоставя мощни инструменти за диагностика, отстраняване на неизправности и анализ на сигурността в Windows и Linux системи. [6] Тяхното усвояване позволява на обучаемите да извършват дълбочинен анализ на подозрителна активност. Инструментите са налични за изтегляне от сайтовете на Microsoft и Sysinternals.

Process Explorer е разширен вариант на Task Manager в Windows и предоставя детайлна йерархична структура на активните процеси. Той позволява на анализаторите да видят кои библиотеки (DLL файлове) са заредени от даден процес, какви мрежови връзки поддържа и какви ресурси използва. [10] Интеграцията му с VirusTotal дава възможност за бърза проверка на процесите с помощта на над 70 антивирусни програми, което го прави отличен инструмент за откриване на съмнителни и зловредни процеси. [14]

Process Monitor (Procmon) е усъвършенстван инструмент за наблюдение, който показва активността на файловата система, системния регистър и процесите/нишките в реално време. [11] Включването му в учебната програма е критично, тъй като позволява на обучаемите да наблюдават точно какви промени прави даден зловреден софтуер в системата в момента на неговото изпълнение (динамичен анализ). Също позволява филтриране на определени ключове, процеси и стойности.

Зловредният софтуер често търси начини да си осигури устойчивост (persistence) в системата, за да се стартира автоматично след рестартиране. Autoruns показва абсолютно всички програми, услуги, драйвери и планирани задачи, които са конфигурирани да се стартират автоматично. Предоставя също възможност за изключване или изтриване на процес от конфигурацията при стартиране на системата. [9] Обучаемите използват този инструмент, за да

идентифицират скрити механизми за устойчивост, използвани от нападателите, като модификации в системния регистър.

TCPView предоставя динамична картина в реално време на всички активни TCP и UDP връзки в системата, включително локални и отдалечени адреси, състояния на връзката и процеса, който ги е инициирал. [8] В обучението TCPView се използва за засичане на нерегламентирана комуникация със Command & Control (C2) сървъри и за анализ на мрежовото поведение на съмнителни приложения.

3. Приложение и ползи в обучението на бъдещи киберспециалисти

Смесеното обучение съчетава традиционни присъствени занятия, онлайн платформи, виртуални лаборатории и самостоятелна подготовка, което позволява по-гъвкаво и ефективно усвояване на знанията и уменията в областта на киберсигурността. Чрез комбиниране на теоретични лекции с практически упражнения, обучаемите могат да затвърждават знанията си в реална или симулирана среда.

Използването на виртуални среди и дистанционни лаборатории дава възможност курсистите да упражняват техники за анализ и защита независимо от физическото местоположение и учебното време. Това позволява многократно изпълнение на упражненията, проследяване на напредъка и адаптиране на учебния процес към индивидуалното темпо на всеки курсант или студент. Онлайн платформите като Moodle подпомагат споделянето на ресурси, демонстрации и записани упражнения, което улеснява подготовката и самостоятелното обучение.

Интегрирането на тези инструменти в смесеното обучение, особено в институции с висок стандарт на подготовка като ВВМУ „Н. Й. Вапцаров“, носи множество академични и практически ползи като запознаване на обучаемите с инструменти за мониторинг в Windows, изграждане на реалистични сценарии, развиване на аналитично мислене, реакция при инциденти и разбиране на жизнения цикъл на атаките.

Във виртуални лаборатории бъдещите киберспециалисти могат безопасно да изследват зловреден софтуер. Използвайки Sysmon и Process Explorer, те наблюдават жизнения цикъл на атаката – от първоначалното заразяване през изграждането на устойчивост (видимо чрез Autoruns) до мрежовата комуникация (видима чрез TCPView). Обучаемите преминават от пасивно четене на теория към активно търсене на аномалии. Те се научават да различават легитимни системни процеси (като svchost.exe или lsass.exe) от зловредни такива, които се опитват да се маскират чрез сходни имена или инжектиране на код. Умението да се събират доказателства чрез Event Viewer и Procmon изгражда основата на дигиталната криминалистика. Курсистите се обучават как да изолират компрометирана машина, да съберат необходимите логове и да съставят времева линия на инцидента. Работата с изброените инструменти им позволява да картографират своите открития към модели като *Cyber Kill Chain* и *MITRE ATT&CK*. Например, засичането на необичайно създаване на процес чрез Sysmon се свързва с тактиката за изпълнение (Execution), а откриването на нов запис в Autoruns – с тактиката за устойчивост (Persistence).

ЗАКЛЮЧЕНИЕ

Инструментите за мониторинг и анализ на сигурността в Windows като Microsoft Defender, Event Viewer, Sysmon, Process Explorer, Process Monitor, Autoruns и TCPView са фундаментални за практическата подготовка на всеки съвременен експерт по информационна сигурност. Прилагането на модела на смесено обучение, съчетаващ присъствени занятия, електронни ресурси и виртуални лаборатории, трансформира теоретичните концепции в приложими технически умения и създава условия за активно, гъвкаво и практико-ориентирано обучение.

Чрез използването на дистанционни платформи и виртуализирани среди, обучаемите могат да изпълняват практически упражнения, да анализират реалистични сценарии и да усъвършенстват своите умения в безопасна контролирана среда. Това повишава ефективността на обучението и позволява изграждането на опит, необходим за работа в динамичната среда на съвременната киберсигурност.

Този подход, активно прилаган в институции като ВВМУ „Н. Й. Вапцаров“, гарантира, че бъдещите киберспециалисти завършват не просто с академични знания, а с реална готовност да се справят със сложни кибератаки, да извършват качествен анализ на риска и да управляват ефективно сигурността на критични информационни инфраструктури.

ЛИТЕРАТУРА

[1] MICROSOFT LEARN, Enable and configure Sysmon in Windows. [online]. Available from: https://learn.microsoft.com/en-us/windows/security/operating-system-security/sysmon/how-to-enable-sysmon.

[2] MICROSOFT LEARN, Microsoft Defender SmartScreen overview. [online]. Available from: https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/.

[3] MICROSOFT LEARN, Protect important folders from ransomware from encrypting your files with controlled folder access - Microsoft Defender for Endpoint. [online]. Available from: https://learn.microsoft.com/en-us/defender-endpoint/controlled-folders.

[4] MICROSOFT LEARN, Smart App Control. [online]. Available from: https://learn.microsoft.com/en-us/windows/apps/develop/smart-app-control/overview.

[5] MICROSOFT LEARN, 2019., Event Viewer. [online]. 29 January 2019. Available from: https://learn.microsoft.com/en-us/shows/inside/event-viewer.

[6] MICROSOFT LEARN, 2026., Sysinternals. [online]. 7 May 2026. Available from: https://learn.microsoft.com/en-us/sysinternals/.

[7] MICROSOFT SUPPORT, Device Security in the Windows Security App. [online]. Available from: https://support.microsoft.com/en-us/windows/device-security-in-the-windows-security-app-afa11526-de57-b1c5-599f-3a4c6a61c5e2.

[8] RUSSINOVICH, M., 2023. TCPView for Windows - Sysinternals | Microsoft Learn. [online]. 11 April 2023. Available from: https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview.

[9] RUSSINOVICH, M., 2026. Autoruns - Sysinternals | Microsoft Learn. [online]. 7 May 2026. Available from: https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns.

[10] RUSSINOVICH, M., 2026. Process Explorer - Sysinternals | Microsoft Learn. [online]. 7 May 2026. Available from: https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer.

[11] RUSSINOVICH, M., 2026. Process Monitor - Sysinternals | Microsoft Learn. [online]. 7 May 2026. Available from: https://learn.microsoft.com/en-us/sysinternals/downloads/procmon.

[12] RUSSINOVICH, M., GARNIER, T., 2026. Sysmon - Sysinternals | Microsoft Learn. [online]. 26 March 2026. Available from: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon.

[13] STATCOUNTER, 2026. Desktop Windows Version Market Share Worldwide. [online]. 1 May 2026. Available from: https://gs.statcounter.com/os-market-share/desktop/worldwide/.

[14] VIRUSTOTAL, 2025., VirusTotal Documentation - How it works. [online]. December 2025. Available from: https://docs.virustotal.com/docs/how-it-works.