Интегриране на инструменти за анализ на уязвимости в операционни системи в смесена образователна среда

Светослав Хаджитодев, Валентина Петрова

Integrating operating system vulnerability analysis tools in a blended learning environment

Svetoslav Hadzhitodev, Valentina Petrova

Abstract:
The development of cybersecurity requires the application of modern educational methods and practically oriented training tools. This report examines the application of blended learning in the preparation of students and cadets in cybersecurity at the N. Y. Vaptsarov Naval Academy, combining traditional classroom classes, practical laboratory exercises and the use of online environments, allowing for effective acquisition of knowledge and skills for detecting, analyzing and eliminating vulnerabilities in operating systems. Solutions such as Kali Linux, Nmap, Tenable Nessus, Greenbone Vulnerability Manager, Metasploit and the Hack the Box web platform are applied in the learning process.

Keywords: киберсигурност, операционни системи, уязвимости, киберсигурност, анализ, обучение

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

ВЪВЕДЕНИЕ

В епохата на дигитализацията и увеличаващите се асиметрични заплахи, киберсигурността се утвърждава като критичен елемент от националната и глобалната сигурност. Това налага използването на образователни програми в съвременни технологични среди. Подготовката на бъдещите специалисти по киберсигурност във Висшето военноморско училище „Н. Й. Вапцаров“ (ВВМУ) изисква надграждане на теоретичните модели чрез интегриране на смесеното обучение. Този подход позволява гъвкаво съчетаване на класическото академично преподаване с практически тренировки в специализирани виртуални среди и платформи.

Настоящият доклад прави преглед на основните софтуерни инструменти за анализ на уязвимости в операционни системи и penetration testing, интегрирани в учебния процес, и анализира техния принос за изграждане на практически умения в обучаемите.

ИЗЛОЖЕНИЕ

1. Инструменти за анализ на уязвимости

Ефективното практическо обучение налага използването на индустриални стандарти и софтуерни решения с отворен код, които курсантите и студентите ще срещнат в реалната си професионална практика.

Kali Linux е специализирана дистрибуция, разработена от Offensive Security и е базирана на операционната система Debian Linux. Тя е стандартна платформа за провеждане на одити по информационна сигурност и penetration testing.

Съдържа над 600 предварително инсталирани и конфигурирани инструмента за различни фази на етичното хакерство – от събиране на информация и мрежово сканиране до експлоатация и анализ на зловреден код. [6] Служи като основна работна среда (атакуваща машина) в лабораторните занятия. Чрез нея обучаемите се запознават с архитектурата на Linux, управлението на процеси и мрежовите конфигурации, докато едновременно с това оперират с вградения арсенал за сигурност.

Nmap е мощен инструмент с отворен код за мрежово откриване и одит на сигурността. Той изпраща IP пакети за определяне на наличните хостове в мрежата, предоставяните от тях услуги (имена на приложения и версии), работещите операционни системи и използваните защитни стени. Използва се за първоначално проучване на целевата инфраструктура. [3] Обучаемите се научават да разчитат мрежовите топологии и да идентифицират потенциални вектори за атака чрез откриване на отворени портове и уязвими услуги.

Автоматизираните скенери за уязвимости са критичен компонент от защитата на всяка информационна система.

- Tenable Nessus е един от най-широко разпространените комерсиални скенери, предлагащ образователни версии. Разполага с огромна, постоянно обновяваща се база данни от сигнатури на уязвимости (CVEs).
- Greenbone Vulnerability Manager (GVM) е алтернативна платформа с отворен код, произлязла от проекта OpenVAS, която предоставя цялостна рамка за управление на уязвимости. [2]

Обучаемите ги използват за автоматизирано сканиране на лабораторни виртуални машини, с цел генериране и анализиране на доклади, филтриране на фалшиво положителните резултати (false positives), приоритизиране на уязвимостите според тяхната система за оценка на уязвимостите (CVSS) и планиране на процеса по смекчаване на риска.

Разработен от Rapid7, Metasploit Framework е най-популярната платформа за разработване, тестване и изпълнение на експлойти. Той предоставя модулна архитектура, включваща хиляди експлойти, полезни товари и модули за последваща експлоатация. [4, 5] Демонстрира нагледно на обучаемите как откритите от Nmap, Nessus или GVM уязвимости могат да бъдат реално компрометирани. Използва се в контролирана среда за придобиване на права за достъп (shell/root достъп), което помага за разбиране на механизмите на атаките и, съответно, на методите за защита от тях.

В подготовката на курсанти и студенти се включва анализатор на мрежови протоколи Wireshark. Приложението му в обучението позволява на обучаемите да наблюдават мрежовия трафик на ниво пакети, да анализират мрежови атаки в реално време (напр. Man-in-the-Middle) и да извършват криминалистичен анализ на мрежата (Network Forensics).

Използването на тези инструменти е организирано в рамките на модел за смесено обучение. Този подход балансира присъствените лабораторни занятия, където се акцентира върху екипната работа и сложните конфигурации, с асинхронна подготовка в специализирани дигитални платформи. По този начин се гарантира непрекъснатост на учебния процес и възможност за персонализиране на темпото на усвояване на материала.

За разлика от предходните софтуерни инструменти, Hack the Box е онлайн платформа за обучение чрез симулация и геймификация, която предоставя достъп до десетки уязвими виртуални машини, предизвикателства от тип „Capture The Flag“ (CTF) и симулирани корпоративни мрежи. [1] Тя е подходяща за самостоятелна подготовка и дистанционна част от смесеното обучение. Обучаемите тестват своите умения в легална, безопасна, но същевременно изключително реалистична среда, състезавайки се при решаване на различни казуси.

В контекста на смесеното обучение, Hack the Box действа като „мост“ между лекционния материал и реалното му приложение. Докато в аудиторията се разясняват теоретичните основи на уязвимостите, в дистанционната фаза обучаемите прилагат наученото самостоятелно. Платформата позволява на преподавателите да проследяват напредъка на всеки курсант и студент чрез детайлни метрики, което прави оценяването обективно и базирано на реално постигнати резултати в симулирана среда.

2. Приложение и ползи в обучението на бъдещи киберспециалисти

Интеграцията на гореописаните инструменти във ВВМУ „Н. Й. Вапцаров“ трансформира традиционния образователен модел в динамична, ориентирана към практиката среда. Ползите от този подход са следните: свързване на теорията с практиката, придобиване на опит с реални инструменти, развиване на аналитично мислене, гъвкавост чрез смесено обучение и адекватност към пазара на труда.

Абстрактни понятия като *Reverse Shell*, *Buffer Overflow*, *OS Command Injection* или *Privilege Escalation* стават реални, когато студентът използва Metasploit Framework, за да ги изследва, като наблюдава ефекта им на системно ниво. Обучаемите се запознават с инструменти, които киберспециалистите използват често в практиката. Разбират начина на работа и предназначението на всеки един инструмент и особеностите при използването им.

Процесът на откриване на уязвимости (чрез Nmap и Nessus/GVM) и тяхното анализиране изисква от обучаемите да мислят като потенциални нападатели (*Red Teams*), за да изградят подходящи защитни механизми (*Blue Teams*). Платформи като Moodle и Hack the Box, комбинирани с локални виртуални лаборатории, базирани на Kali Linux, позволяват на курсистите да продължат своето обучение извън аудиториите, в удобно за тях време. Това стимулира самостоятелността и самоусъвършенстването. CTF състезанията и практическите изпити във виртуални полигони (Cyber Ranges) симулират напрежението, характерно за реални инциденти в киберсигурността. Това развива психиката на бъдещите офицери и киберспециалисти.

Обучението с актуални индустриални стандарти драстично съкращава времето за адаптация на завършващите специалисти в корпоративна или военна среда. Те придобиват фундамент, който им позволява лесно да се сертифицират с престижни международни сертификати като *CEH (Certified Ethical Hacker)*, *CompTIA PenTest+* и *OSCP (Offensive Security Certified Professional)*.

Смесеното обучение позволява задачи като инсталация на софтуер, първоначално четене и базови конфигурации да се изнесат в дистанционна форма чрез Moodle. Това освобождава ценно време в присъствените часове за дискусии

върху критични казуси, сложни сценарии на атака и индивидуални консултации с преподавателя. Този модел развива навици за непрекъснато учене, което е критично за динамично развиващата се сфера на киберсигурността.

ЗАКЛЮЧЕНИЕ

Подготовката на висококвалифицирани кадри в сферата на киберсигурността е невъзможна без осигуряване на пряк достъп до инструментите и методологиите, използвани в реални условия. Смесеното обучение във ВВМУ „Н. Й. Вапцаров“, съчетаващо академична теория с интензивното използване на системи като Kali Linux, Nmap, скенери за уязвимости (Nessus, GVM), платформи за изпълнение на експлойти (Metasploit) и тренировъчни платформи (Hack the Box), доказва своята висока ефективност и могат да бъдат полезни и за други обучителни институции в тази сфера. Този комплексен подход гарантира изграждането на киберспециалисти с изразени практически умения, способни своевременно да откриват, анализират и неутрализират уязвимости в критични операционни системи и мрежови инфраструктури.

ЛИТЕРАТУРА

[1] HACK THE BOX, Develop Your Workforce. [online]. Available from: https://www.hackthebox.com/develop-cybersecurity-workforce.

[2] HADZHITODEV, S., PETROVA, V., 2026. Analyzing Vulnerabilities In Desktop Operating Systems. In: *2025 International Conference Automatics and Informatics (ICAI).* Varna, Bulgaria, ISBN: 979-8-3315-8611-9, pp. 89–93. [online]. 14 January 2026 Available from: https://doi.org/10.1109/ICAI67591.2025.11324497.

[3] NMAP, Nmap: the Network Mapper - Free Security Scanner. [online]. Available from: https://nmap.org/.

[4] RAPID7, Metasploit | Penetration Testing Software. [online]. Available from: https://www.metasploit.com/.

[5] RAPID7, Metasploit Framework | Metasploit Documentation. [online]. Available from: https://docs.rapid7.com/metasploit/msf-overview/.

[6] THE KNOWLEDGE ACADEMY, 2026. Kali Linux Features: A Comprehensive Overview. [online]. 21 February 2026. Available from: https://www.theknowledgeacademy.com/blog/kali-linux-features/.