2. Środowiska wirtualne

Środowisko wirtualne (ang. **Virtual Environments**, VE) to oprogramowanie symulujące działanie sprzętu komputerowego. W odróżnieniu od tradycyjnych systemów fizycznych umożliwia ono jednoczesne funkcjonowanie wielu niezależnych systemów operacyjnych lub aplikacji na jednej maszynie [1]. Działają one niezależnie od fizycznej struktury sprzętu. Tworzenie środowisk wirtualnych możliwe jest dzięki wykorzystaniu technologii wirtualizacji. Jest to technologia, wykorzystująca środowisko logiczne do przekroczenia fizycznych ograniczeń sprzętowych [2].

Podstawowym elementem środowisk wirtualnych jest maszyna wirtualna (ang. **Virtual Machine**, VM). Jest to aplikacja, wykonujące program tak, jakby była fizycznym urządzeniem, więc można byłoby powiedzieć, że jest to „komputer”, działający wewnątrz fizycznego komputera. Aplikacja VM (nazywana „gościem”) uruchamia swój własny system operacyjny na rzeczywistej maszynie (zwanej „gospodarzem”). Wirtualny system operacyjny może być dowolny, np. Windows lub MacOS, i nie jest ograniczony do jednego systemu operacyjnego na maszynie gospodarza [3]. Każda maszyna wirtualna działa niezależnie i nie ma wpływu na działanie innych VM-ów.

2.1. Charakterystyka wirtualizacji

Wirtualizacja to technologia umożliwiająca tworzenie wielu odizolowanych środowisk komputerowych – zwanych maszynami wirtualnymi (VM) – na jednym fizycznym urządzeniu. Dzięki warstwie pośredniczącej, zwanej hipernadzorcą (**hypervisor**), każda maszyna wirtualna może działać jak odrębny komputer z własnym systemem operacyjnym i aplikacjami, niezależnie od innych instancji. To podejście pozwala na efektywne wykorzystanie zasobów sprzętowych, zwiększenie skalowalności, uproszczenie zarządzania oraz ograniczenie kosztów operacyjnych [4].

Hipernadzorca (hypervisor) to oprogramowanie, które umożliwia tworzenie i zarządzanie maszynami wirtualnymi poprzez oddzielenie systemów operacyjnych gości od fizycznej infrastruktury sprzętowej. W zależności od sposobu działania, wyróżniamy dwa główne typy:

* typ 1: natywny (bare-metal) – działa bezpośrednio na sprzęcie, bez potrzeby instalowania systemu operacyjnego gospodarza. Przykładowo: Microsoft Hyper-V,
* typ 2: hostowany – funkcjonuje jako aplikacja zainstalowana w ramach istniejącego systemu operacyjnego. Przykładowo: VirtualBox, VMware Workstation.

Dodatkowo, hypervisory można klasyfikować ze względu na sposób wirtualizacji:

* Pełna wirtualizacja – system gościa działa bez konieczności modyfikacji, nieświadomy, że funkcjonuje w środowisku wirtualnym, jest w pełni niezależny.
* Wirtualizacja wspierana sprzętowo – wykorzystuje specjalne funkcje procesora, takie jak Intel VT-x czy AMD-V, w celu optymalizacji pracy maszyn wirtualnych.
* Parawirtualizacja – wymaga modyfikacji systemu gościa, który jest świadomy, że działa w środowisku wirtualnym i potrafi efektywnie współpracować z hipernadzorcą [5].

2.2. VMware jako platforma testowa

Vmware Workstation Pro (od firmy Broadcom) jest w pełni zwirtualizowanym środowiskiem sprzętowym dla systemu operacyjnego gościa. Program ten obsługuje wiele systemów operacyjnych gospodarza, w tym Windows, Linux oraz macOS, i został zaprojektowany z myślą o maksymalnym wykorzystaniu fizycznych zasobów komputera, co przekłada się na wysoką wydajność działania maszyn wirtualnych [4].

Oprogramowanie to stara się wykonywać instrukcje bezpośrednio na procesorze gospodarza, o ile jest to możliwe. W przypadkach, gdy bezpośrednie wykonanie kodu nie jest wspierane przez sprzęt, oprogramowanie korzysta z techniki dynamicznego tłumaczenia binarnego, która pozwala na przekształcanie instrukcji w czasie rzeczywistym. Tak przetworzony kod jest przechowywany w pamięci RAM, co umożliwia dalsze działanie maszyny wirtualnej z dużą szybkością – według producenta, z wydajnością sięgającą ponad 80% względem natywnego systemu [4].

VMware emuluje podstawowe elementy sprzętowe, takie jak karta graficzna (czego nie oferuje np., VirtualBox od firmy Oracle), karta sieciowa czy kontrolery dysków, a także umożliwia dostęp do urządzeń USB, portów szeregowych i równoległych za pomocą sterowników pośredniczących. Warto jednak zauważyć, że przenoszenie maszyn wirtualnych między różnymi komputerami, szczególnie z odmiennymi architekturami procesora lub liczbą rdzeni, może wymagać dodatkowej konfiguracji ze względu na różnice w zestawach instrukcji [4].

Dzięki powyższym rozwiązaniom, VMware Workstation Pro wyróżnia się wysoką wydajnością i wszechstronnością, co czyni go solidnym narzędziem do prowadzenia badań nad bezpieczeństwem w środowiskach wirtualnych.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 1 Widok podstawowy Vmware Workstation w wersji 17.6.3

Podstawowymi funkcjami dostarczanymi przez środowisko Vmware Workstation są m.in.:

- tworzenie maszyn wirtualnych z wybraną konfiguracją systemu operacyjnego, pamięci RAM, przestrzeni dyskowej,

- snapshoty, czyli zapisywanie stanu maszyny wirtualnej w wybranym przez użytkownika momencie, co daje możliwość przywrócenia zapisanego obrazu,

- klonowanie maszyn wirtualnych,

- uruchamianie maszyn wirtualnych jednocześnie przy jednoczesnym ich izolowaniu.

- zaawansowana konfiguracja sieciowa, pozwalająca na definiowanie topologii sieci wirtualnych (m.in. NAT, bridge, host-only)

- połączenia ze zdalnymi serwerami, np. z Vmware ESXi.

2.3 Konfiguracja środowiska testowego

Do przeprowadzenia testów wykorzystany został komputer stacjonarny. Wyposażony został w następujące podzespoły:

- procesor AMD Ryzen 5 3600,

- 64GB pamięci RAM typu DDR4, 3600MHz,

- dysk M.2 o pojemności 2TB,

- karta graficzna NVIDIA GeForce RTX 3060 Ti.

Zainstalowany system operacyjny gospodarza to Windows 11 Pro w wersji 24H2.

Wykorzystana wersja Vmware to Workstation Pro 17.6.3 (rys.1).

2.3.1 Tworzenie maszyny wirtualnej systemu Windows

Do postawienia nowej maszyny wirtualnej z systemem Windows 10 wykorzystano zaawansowane ustawienia, które pozwalają na określenie opcji takich jak chociażby:

- typ kontrolera SCSI,

- typ dysku wirtualnego,

- kompatybilność ze starszymi produktami VMware (fot. 2).

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 2. Wybór typu konfiguracji przy tworzeniu nowej maszyny wirtualnej w VMware Workstation Pro 17.

Została wybrana kompatybilność sprzętowa dla wersji Workstation 17.5 lub nowszych (fot.3).

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 3. Wybór kompatybilności sprzętowej dla nowej maszyny wirtualnej.

Instalacja odbyła się przy użyciu pliku iso z systemem Windows 10 22H2 w architekturze 64-bitowej (fot. 4).

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 4. Wybór pliku iso z systemem operacyjnym

Dla porządku, maszynie wirtualnej została nadana nazwa „Windows 10 x64 Security Tests” oraz przypisana została odpowiednia lokalizacja na dysku.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 5. Nazwa maszyny wirtualnej oraz nadanie ścieżki.

Istotną kwestią jest wybranie odpowiedniego typu instalowanego oprogramowania.

A screenshot of a computer

AI-generated content may be incorrect.

Fot.6. Wybór typu oprogramowania (UEFI lub BIOS)

Dla stawianego na maszynie wirtualnej systemu Windows 10 został wybrany typ oprogramowania UEFI (Unified Extensible Firmware Interface) , ze względu na lepsze dostosowanie do obecnych standardów bezpieczeństwa (niektóre narzędzia i techniki zabezpieczeń mogą działać tylko z UEFI, np. Microsoft Defender Credential Guard). BIOS jest technologią przestarzałą, a system Windows 10 jest domyślnie instalowany w technologii UEFI. Za użyciem UEFI przemawia także to, że:

- posiada modularną architekturę (co może być przydatne w kontekście testów bezpieczeństwa przy użyciu VMware, np. do wgrania sterowników DXE[[1]](#footnote-1))

- ma szybszy czas rozruchu niż BIOS,

- posiada abstrakcję sprzętową,

- oferuje zaawansowane opcje, obejmujące np. obsługę większych dysków twardych,

- dostarcza mechanizmy bezpieczeństwa. [7].

Opcja Secure Boot nie została zaznaczona, ponieważ w pierwszej fazie testów system będzie sprawdzany przy możliwie najmniejszych zabezpieczeniach (opcja ta chroni np. przed bootkitami czy rootkitami, czyli złośliwym kodem wykonywanym już przy starcie systemu).

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 7. Konfiguracja liczby procesorów i rdzeni.

Procesor zainstalowany w jednostce centralnej używanej do testów to AMD Ryzen 5 3600, co za tym idzie, posiada on 6 rdzeni fizycznych i obsługuje 12 wątków. Optymalnym wyborem będzie przypisanie jednego procesora logicznego oraz czterech rdzeni, co daje w sumie cztery wirtualne rdzenie. Przy takiej konfiguracji zapewniona zostanie wystarczająca wydajność, a także zostaną zachowane potrzebne zasoby dla hosta i innych zadań, wykonywanych równolegle przez komputer. Przydzielenie zbyt dużej liczby rdzeni maszynie wirtualnej mogłoby spowodować utratę stabilności systemu.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 8. Konfiguracja przydzielonej ilości pamięci operacyjnej.

Wykorzystywany do testów komputer dysponuje 64GB pamięci RAM, zatem dla maszyny wirtualnej optymalną wartością będzie przypisanie 8GB pamięci (dokładnie 8192MB). Pozwoli to na płynne działanie pod potencjalnym większym obciążenie, gdzie rekomendowane 2GB mogłyby okazać się niewystarczające.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 8. Konfiguracja sieci dla maszyny wirtualnej.

Dla przeprowadzanych w pracy testów bezpieczeństwa najlepszym typem połączenia z siecią jest połączenie mostkowane, ponieważ pozwoli to na przeprowadzenie ataków takich jak np. Man-in-the-Middle, sniffing czy ARP spoofing. Maszyna wirtualna w tym wypadku jest dostępna z poziomu sieci lokalnej. Umożliwia to sprawdzenie jak maszyna wirtualna wchodzi w interakcje z innymi urządzeniami. Wybór NAT mógłby być problematyczny, ze względu brak bezpośredniego dostępu z sieci, przez co maszyna wirtualna nie byłaby dostępna az poziomu innych urządzeń w sieci.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 9. Konfiguracja dla urządzeń wejścia/wyjścia.

Wybrano rekomendowany typ LSI Logic SAS, który jest domyślnym kontrolerem I/O zapewnia wysoką kompatybilność z systemami operacyjnymi. Wadą tego rozwiązania względem Paravirtualized SCSI jest mniejsza wydajność, jednak przy wyborze wymienionej opcji należałoby ręcznie instalować wymagane sterowniki.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 10. Konfiguracja typu dysku.

Dla zapewnienia odpowiedniej wydajności został wybrany rekomendowany typ dysku NVMe, który wykorzystuje wydajne (w porównaniu do SCSI czy SATA) interfejsy SSD.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 11. Konfiguracja dysku – utworzenie izolowanego dysku wirtualnego.

Do utworzenia nowej maszyny wirtualnej w przypadku testów bezpieczeństwa najlepszym wyborem, jeśli chodzi o dysk, jest utworzenie nowego dysku wirtualnego. Oznacza to, że środowisko będzie izolowane, a jest to istotna kwestia w przypadku przeprowadzanych badań. Wybór istniejącego dysku wirtualnego nie jest możliwy, ponieważ nie został wcześniej utworzony żaden dysk, który spełniałby wymagania ustalone do testów bezpieczeństwa, natomiast użycie dostępu do dysku fizycznego mogłoby okazać się ryzykowne (potencjalnie uszkodzenie danych na dysku fizycznym), a także niepotrzebne, ponieważ stworzyłoby to niepotrzebne komplikacje.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 12. Określenie wielkości dysku wirtualnego.

Optymalną wielkością dla wirtualnego dysku będzie 80GB, co jest wartością maksymalną, którą może on osiągnąć – miejsce nie jest z góry alokowane, co jest oszczędnością miejsca dla dysku fizycznego. Przechowywanie dysku wirtualnego w postaci jednego pliku pozwoli zwiększyć wydajność, względem dzielenia go na osobne pliki (mogłoby to ułatwić przenoszenie go na inne komputery, co nie jest przewidywane).

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 13. Nazwa pliku dla dysku wirtualnego.

„Windows 10 x64 Security Tests” jest domyślną nazwą zaproponowaną przez kreator nowej maszyny wirtualnej. Rozszerzenie pliku vmdk jest domyślnym formatem, w którym VMware zapisuje pliki przechowujące dyski wirtualne.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 14. Parametry nowej maszyny wirtualnej.

Po przejściu wszystkich poprzednich kroków kreator pokazuje podsumowanie, w którym widoczny jest opis parametrów nowej maszyny. Po naciśnięciu przycisku „Finish” maszyna zostaje utworzona, natomiast po jej pierwszym uruchomieniu następuje standardowa instalacja systemu Windows 10 (w tym wypadku została wybrana wersja Windows 10 Pro (Fot.14.)).

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 14. Wybór wersji systemu Windows 10.

Po instalacji VMware sugeruje także instalację VMware Tools, co obejmuje potrzebne sterowniki urządzeń wejścia/wyjścia oraz poprawia wydajność maszyny wirtualnej. Narzędzia te zostały zainstalowane.

2.3.1 Tworzenie maszyny wirtualnej systemu Linux

Instalacja systemu Linux (Ubuntu 24.04.2 LTS) jako maszyny wirtualnej odbywa się analogicznie do instalacji systemu Windows 10. Należy pobrać plik ISO z oficjalnej strony [8] dystrybutora.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 15. Personalizacja systemu Linux.

Dla porządku ustawiono nazwę SecurityTest dla systemu Linux oraz nazwę użytkownika vmtestuser.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 15. Personalizacja systemu Linux.

Została również wybrana nazwa maszyny wirtualnej analogiczna do tej z Windows 10.

A screenshot of a computer

AI-generated content may be incorrect.

Fot. 16. Wybór typu dysku dla Linuxa wVMWare.

Wyjątkowo, dla Linuxa wybrano typ dysku SCSI, czyli inaczej niż NVMe dla systemu Windows. Wynika to z zaleceń istalatora, co wynika z tego, że Windows 10 domyślnie wspiera typ NVMe, natomiast Ubuntu zapewnia lepszą kompatybilność oraz stabilność przy kontrolerze SCSI. Ze względu na to, że testy skupiają się na aspektach bezpieczeństwa, a nie wydajności, różnice te nie mają znaczenia w kontekście wyników przeprowadzanych badań.

Reszta parametrów została dobrana identycznie, jak dla maszyny wirtualnej z systemem Windows 10.

Po instalacji systemu, zainstalowano także VMWare Tools, czyli narzędzia i sterowniki potrzebne do poprawnej i wydajnej pracy maszyny wirtualnej.

VMware sugeruje także instalację VMware Tools, co obejmuje potrzebne sterowniki urządzeń wejścia/wyjścia oraz poprawia wydajność maszyny wirtualnej. Narzędzia te zostały zainstalowane.

2.4 Kali Linux – narzędzie do przeprowadzania testów

Na osobnym komputerze podłączonym do tej samej sieci zainstalowany został system Kali Linux w wersji 2025.1c. Jest to dystrybucja typu open-source oparta na systemie Debian, stworzona przez Offensive Security w celach przeprowadzania testów penetracyjnych oraz audytów bezpieczeństwa. Posiada on wbudowane narzędzia dedykowane testom bezpieczeństwa, a także dostosowane jądro systemu do wstrzykiwania różnego rodzaju pakietów [8].

System ten został wybrany do testów, ze względu na swoją popularność, stabilność oraz szeroką społeczność skupioną wokół oprogramowania. Jest to adekwatne narzędzie do przeprowadzenia testów bezpieczeństwa w środowiskach wirtualnych.

4. Testowanie bezpieczeństwa – faza pierwsza

4.1 Ataki sieciowe

a) Sniffing

|  |  |  |
| --- | --- | --- |
| Test ID | System atakowany | Środowisko |
| A1 | Windows 10 | VMware |
| A2 | Windows 10 | Bare-metal |
| A3 | Ubuntu 22.04 | VMware |
| A4 | Ubunu 22.04 | Bare-metal |

Tabela x.

Celem testów A1-A4 było sprawdzenie czy możliwe jest pasywne podsłuchiwanie ruchu sieciowego (sniffing) z systemu Kali Linux zainstalowanego na fizycznym komputerze, przy użyciu narzędzia Wireshark. Wszystkie urządzenia były połączone do tej samej sieci lokalnej (Wi-Fi). We wszystkich wypadkach włączone były domyślne zabezpieczenia systemowe (Firewall dla Windows oraz ufw dla Ubuntu).

A screenshot of a computer

AI-generated content may be incorrect.  
Fot. x.

Wireshark w wersji 4.4.4 został połączony przez wlan0. Następnie rozpoczęto przechwytywanie pakietów. Ustawiony został filtr http. Test polegał na odwiedzeniu strony http (http://testphp.vulnweb.com/login.php)[[2]](#footnote-2) na maszynie ofiary oraz zasymulowaniu ruchu poprzez wprowadzenie i wysłanie przykładowych danych logowania. Upewniono się także, czy włączony jest tryb promiscous.[[3]](#footnote-3)

A screenshot of a computer

AI-generated content may be incorrect.  
Fot. x.

Wireshark nie wykrył ruchu w żadnym z przeprowadzanych testów (A1-A4). Sprawdzony został także wpływ Windows Firewall oraz ufw dla Ubuntu. Wyniki były identyczny przy wyłączonych zabezpieczeniach sieciowych.

Połączenie na maszynach wirtualnych było ustawione mostkowo, co zostało opisane w 2.3.1.

A screenshot of a computer

AI-generated content may be incorrect.  
Fot. x.

Dla porównania i zobrazowania ataku, a także sprawdzenia metodologii, przeprowadzony został dodatkowy test, gdzie połączenie http odbyło się na komputerze atakującym. Wireshark odnotował ruch sieciowy.

A screenshot of a computer

AI-generated content may be incorrect.  
Fot. x.

Przy pomocy narzędzia Follow http Steam, udało się odczytać dane wykorzystane do logowania (fot.x).

Z przeprowadzonych badań wynika, że w przypadku testów sniffingu maszyny wirtualne nie wykazują różnicy w kontekście bezpieczeństwa w porównaniu do maszyn fizycznych. Ustawienie urządzeń w tej samej sieci (typu bridged) nie wystarczyło do przechwycenia ruchu http z maszyny ofiary.

W środowiskach wykorzystujących przełączniki sieciowe (np. domowe routery Wi-Fi, przełączniki warstwy 2) standardowy sniffing z użyciem narzędzi takich jak Wireshark nie pozwala na podsłuchiwanie ruchu pomiędzy innymi urządzeniami w sieci. Wynika to z faktu, że przełączniki przekazują pakiety tylko do właściwego odbiorcy, co uniemożliwia pasywne przechwytywanie pakietów przez inne hosty [9].

W związku z tym, w nowoczesnych sieciach lokalnych, gdzie przełączniki izolują ruch, skuteczne podsłuchiwanie ruchu może wymagać wykonania ataku typu Man-in-the-Middle (MITM), np. przy użyciu ARP spoofingu.

Bibliografia

[1] Virtualization Throughout the Software Lifecycle, Sarah N. Crutchfield

[2] Virtualization and Security Aspects: An Overview, Rui Filipe Pereira, Rui Miguel Silva & João Pedro Orvalho

[3] Virtualization and Forensics A Digital Forensic Investigator’s Guide to Virtual Environments

[4] VMware vSphere Essentials: A Practical Approach to vSphere Deployment and Management Luciano Patrão

[5] Optimal guest file system for type-2 hypervisorbased virtualization in Virtual box

[6] <https://uefi.org/specs/PI/1.8/V2_Overview.html>

[7] UEFI Memory Forensics: A Framework for UEFI Threat Analysis Kalanit Suzan Segal∗

[8] <https://www.kali.org/docs/introduction/what-is-kali-linux/>

[9] Patel, N. P., Patel, R. G., & Patel, D. R. (2009). Packet Sniffing: Network Wiretapping. W: 2009 IEEE International Advance Computing Conference (IACC 2009) (s. 2691-2696). Patiala, Indie: IEEE.

- podrozdział dlaczego win I linux i dlaczego w takich wersjach

- ‘wykorzystanie istniejących narzędzi, wyodrębnienie obszarów bezpieczeństwa, przeprowadzenie testów, podsumowanie i wnioski’

- Uzasadnienie czemu te a nie inne narzędzia

- Mocne wyodrębnienie obszarów bezpieczeństwa

- Kompleksowa ocena bezpieczeństwa systemów wirtualnych

- Które systemy na jaki typ ataków

Ubuntu: vmtestuser, password

Kali: kaliuser, password

1. Są to sterowniki, odpowiadające za inicjalizację chipsetu, procesora czy innych komponentów, a także za dostarczenie warstwy abstrakcji dla np. usług systemowych [6] [↑](#footnote-ref-1)
2. Podana strona umożliwia przeprowadzanie testów bezpieczeństwa, poprzez przechwytywanie danych logowania przesływanych przez http. [↑](#footnote-ref-2)
3. Promiscius to tryb pracy interfejsu sieciowego, w którym przechwytywane są wszystkie pakiety przechodzące przez sieć. [↑](#footnote-ref-3)