**KONSPEKT PRZEDMIOTU**

Semestr letni, rok akad. 2020/2021

|  |  |
| --- | --- |
| Nazwa przedmiotu | Bezpieczeństwo systemów informatycznych |
| Kierunek/-i studiów / rok studiów / semestr studiów | Informatyka/4/VIII |
| Tryb studiów | Stacjonarny |
| Forma zajęć | Laboratorium |
| Liczba godzin | 30 |
| Koordynator przedmiotu: | mgr inż. Łukasz Laszko |
| Jakie są ogólne cele dydaktyczne tego przedmiotu? | Przygotowanie studentów do praktycznego wdrożenia zabezpieczeń systemów informatycznych. |
| Jak są kryteria zaliczenia tego przedmiotu? | Za ćwiczenia laboratoryjne studenci mogą uzyskać 100 punktów. Punkty student zdobywa po realizacji wydanych zadań na zajęciach. Laboratoria uznaje się za zaliczone jeżeli student uzyska co najmniej 40 punkty, co stanowi 40% osiągniętych efektów uczenia się. Za ćwiczenia laboratoryjne wystawiana jest ocena uogólniona (zal/nzal). |
| Jakie są kryteria zaliczenia tego przedmiotu na ocenę celującą? | Uzyskanie z laboratoriów co najmniej 85% z 100 możliwych punktów i realizacja wszystkich dodatkowych zadań laboratoryjnych. Informacja o spełnieniu przez studenta powyższych warunków jest przekazywana wykładowcy odpowiedzialnemu za przedmiotu, który podejmuje decyzję o wystawieniu oceny celującej z przedmiotu po spełnieniu przez studenta wszystkich warunków uzyskania oceny celującej według kryteriów ustalonych dla całego przedmiotu. |
| Pozostałe informacje, dotyczące tego przedmiotu, ważne dla studenta | Student, który nie był obecny na co najmniej 10% zajęć w semestrze lub w czasie semestru nie zdobył co najmniej 10% z 100 możliwych punktów do zdobycia, nie może przystąpić do zaliczenia poprawkowego |

|  |  |
| --- | --- |
| **ZAJĘCIA 1**  **(3 godz.)**  **Testy penetracyjne (skanowanie)** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie znał podstawowe techniki skanowania stosowane w testach penetracyjnych. 2. Student będzie umiał przeprowadzić skanowanie systemu operacyjnego oraz sieci lokalnej. 3. Student będzie umiał zidentyfikować niektóre podatności swojego systemu operacyjnego oraz innego komputera w sieci lokalnej. |
| Treści zajęć | 1. Skanowanie stanu zabezpieczeń systemu operacyjnego (MBSA). 2. Skanowanie stanu zabezpieczeń systemu operacyjnego oraz sieci lokalnej (MegaPing). 3. Skanowanie stanu zabezpieczeń systemu operacyjnego, sieci lokalnej oraz innego komputera w sieci lokalnej (GFI LanGuard). |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - Patkowski A.E., Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych, 2007, [link](http://www.ita.wat.edu.pl/cgi-bin/downloadCounter.cgi?sid=40608c8d7ef3962407e99a850e546004d8dee95634d8b362c0fd8d436b75bfc3eaa368a7ac53c2fa1f625714976450fa1e107e42385b3d47b569e6825d0f1ee83a9ad1d56de2d5949424e5c82a483fd4e727667b812bd7ba5841c0fdce72f16903aa47d081e7b70fd33c1a12ee48588c5d810d6b8407cd9c265342e669ce7b1dfaf25b85ed97ead7c03274b20cb829b2b82cbf9adbcee3c8f0f4e5fb5d7368499bdb96d2a929f4a6de4383c37a8bca4e0ed535e1d2de38da983c0e45121b0966787ebdaabbb16d478992e2d18325a4f7a7d970426caad6bb19520fd31ff79100) |

|  |  |
| --- | --- |
| **ZAJĘCIA 2**  **(3 godz.)**  **Testy penetracyjne (enumeracja)** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie znał podstawowe techniki enumeracji stosowane w testach penetracyjnych. 2. Student będzie umiał przeprowadzić enumerację systemu operacyjnego. 3. Student będzie umiał pozyskać informację o zasobach innego komputera w sieci lokalnej. |
| Treści zajęć | 1. Enumeracja zasobów komputera (userinfo, enum). 2. Enumeracja sieci lokalnej (nbtscan, net view). 3. Identyfikacja systemów operacyjnych (nmap). |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - Suski Z., Wybrane przypadki enumeracji systemu Windows Server 2012, Przegląd Teleinformatyczny, nr 1-2, 2014, [link](http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-a4267cb1-9057-4599-abef-e166b54baf29/c/2_PT1-2-s17-suski.pdf)  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - Patkowski A.E., Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych, 2007, [link](http://www.ita.wat.edu.pl/cgi-bin/downloadCounter.cgi?sid=40608c8d7ef3962407e99a850e546004d8dee95634d8b362c0fd8d436b75bfc3eaa368a7ac53c2fa1f625714976450fa1e107e42385b3d47b569e6825d0f1ee83a9ad1d56de2d5949424e5c82a483fd4e727667b812bd7ba5841c0fdce72f16903aa47d081e7b70fd33c1a12ee48588c5d810d6b8407cd9c265342e669ce7b1dfaf25b85ed97ead7c03274b20cb829b2b82cbf9adbcee3c8f0f4e5fb5d7368499bdb96d2a929f4a6de4383c37a8bca4e0ed535e1d2de38da983c0e45121b0966787ebdaabbb16d478992e2d18325a4f7a7d970426caad6bb19520fd31ff79100) |

|  |  |
| --- | --- |
| **ZAJĘCIA 3**  **(3 godz.)**  **Ataki sieciowe i metody przeciwdziałania** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie umiał przeprowadzić prosty atak DoS oraz ocenić jego wpływ na wydajność systemu. 2. Student będzie rozumiał specyfikę ataku DoS po przeprowadzonej analizie przebiegu ataku w snifferze sieciowym. 3. Student będzie potrafił wykonać rekonfigurację systemu operacyjnego w celu przeciwdziałania lub ograniczenia skutków przykładowego ataku DoS. |
| Treści zajęć | 1. Ataki DoS (SYNFlood, UDPFlood). 2. Analiza wydajności atakowanego komputera (Perfmon). 3. Analiza przebiegu ataku DoS (WireShark). 4. Przeciwdziałanie atakom DoS. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - [SYN Flood Attack,](http://www.ita.wat.edu.pl/cgi-bin/downloadCounter.cgi?sid=40608c8d7ef3962407e99a850e546004d8dee95634d8b362c0fd8d436b75bfc3eaa368a7ac53c2fa1f625714976450fa1e107e42385b3d47b569e6825d0f1ee83a9ad1d56de2d5949424e5c82a483fd4e727667b812bd7ba5841c0fdce72f16903aa47d081e7b70fd33c1a12ee48588c5d810d6b8407cd9c265342e669ce7b1dfaf25b85ed97ead7c03274b20cb829b2b82cbf9adbcee3c8f0f4e5fb5d7368499bdb96d2a929f4a6de4383c37a8bca4e0ed535e1d2de38da983c0e45121b0966787ebdaabbb16d478992e2d18325a4f7a7d970426caad6bb19520fd31ff79100)  https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/  - Network DoS Attacks,  https://www.juniper.net/documentation/en\_US/junos/topics/topic-map/security-network-dos-attack.html  - How to Use Wireshark: A Complete Tutorial,  https://www.lifewire.com/wireshark-tutorial-4143298 |

|  |  |
| --- | --- |
| **ZAJĘCIA 4**  **(3 godz.)**  **Zabezpieczenia kryptograficzne (GPG, podpis cyfrowy i szyfrowanie, bezpieczna poczta elektroniczna)** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie znał podstawowe zasady stosowania podpisu cyfrowego oraz szyfrowania w oparciu o certyfikaty GPG. 2. Student będzie umiał wykorzystać certyfikaty GPG do zabezpieczenia swojej poczty elektronicznej oraz swoich dokumentów. 3. Student będzie umiał zbudować małą sieć WoT (Web of Trust). |
| Treści zajęć | 1. Generowanie certyfikatów GPG. 2. Stosowanie zabezpieczeń kryptograficznych. 3. Budowa sieci WoT. 4. Zabezpieczanie i weryfikacja integralności dokumentów. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - Dokumentacja GnuPG, https://gnupg.org/documentation/index.html |

|  |  |
| --- | --- |
| **ZAJĘCIA 5**  **(3 godz.)**  **Urząd certyfikacji i certyfikacja (certyfikaty x509, zabezpieczanie usług sieciowych)** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie umiał zainstalować i skonfigurować urząd certyfikacji w systemie Windows Server. 2. Student będzie umiał generować certyfikaty x509 w oparciu o przygotowane żądania. 3. Student będzie umiał zabezpieczać usługi sieciowe z wykorzystaniem certyfikatów x509. |
| Treści zajęć | 1. Instalacja roli ADCS. 2. Konfiguracja urzędu certyfikacji. 3. Generowanie certyfikatu x509 dla użytkownika oraz dla usługi sieciowej. 4. Zabezpieczanie usługi sieciowej z wykorzystaniem certyfikatu x509. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - SSL : Part 1 : Building a Microsoft Certificate Authority for your lab,  https://virtuallythere.blog/2018/04/24/making-things-a-bit-more-secure-part-1/  - SSL : Part 2 : Signing a CSR with your Microsoft Certificate Authority,  https://virtuallythere.blog/2018/04/27/making-things-a-bit-more-secure-part-2/ |

|  |  |
| --- | --- |
| **ZAJĘCIA 6**  **(3 godz.)**  **Zapory sieciowe** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie umiał skonfigurować systemową zaporę sieciową stosując reguły proste oraz zaawansowane. 2. Student będzie umiał posługiwać się konsolą tekstową PowerShell w zakresie konfiguracji systemowej zapory sieciowej. 3. Student będzie umiał zablokować oraz analizować dostęp do wybranej witryny internetowej z wykorzystaniem systemowej zapory sieciowej. |
| Treści zajęć | 1. Filtr aplikacji oraz filtr zaawansowany. 2. Konfiguracja zapory sieciowej z poziomu konsoli tekstowej PowerShell. 3. Blokowanie i weryfikacja wybranego ruchu wyjściowego z komputera. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - Configuring Windows Firewall Rules with PowerShell,  http://woshub.com/manage-windows-firewall-powershell/ |

|  |  |
| --- | --- |
| **ZAJĘCIA 7**  **(3 godz.)**  **Systemy wykrywania włamań** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie umiał zainstalować i skonfigurować system wykrywania włamań (IDS) Snort for Windows. 2. Student będzie umiał skorzystać z wbudowanych reguł systemu IDS. 3. Student będzie umiał napisać własną regułę systemu IDS. |
| Treści zajęć | 1. Instalacja i konfiguracja systemu Snort for Windows. 2. Testowanie i adaptacja reguł wbudowanych. 3. Wykrywanie sieciowych incydentów bezpieczeństwa. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - Defending your network with Snort for Windows, https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/  - Dokumentacja systemu Snort,  https://www.snort.org/documents |

|  |  |
| --- | --- |
| **ZAJĘCIA 8**  **(3 godz.)**  **Sieci prywatne (PPTP, IPSec)** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie umiał wdrożyć wirtualną sieć prywatną (VPN) w ramach swojej sieci lokalnej. 2. Student będzie umiał zweryfikować działanie oraz poufność komunikacji sieci VPN z wykorzystaniem sniffera sieciowego. |
| Treści zajęć | 1. Wdrożenie wirtualnych sieci prywatywnych wykorzystujących protokół PPTP oraz IPSec. 2. Weryfikacja poufności komunikacji z wykorzystaniem sniffera sieciowego WireShark. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  Rozszerzające / uzupełniające:  - How to set up a PPTP VPN on Windows Server 2016,  https://www.snel.com/support/how-to-set-up-a-vpn-with-windows-server/  - Secure Windows Traffic with IPsec,  https://it.cornell.edu/managed-servers/secure-windows-traffic-ipsec  - How to Use Wireshark: A Complete Tutorial,  https://www.lifewire.com/wireshark-tutorial-4143298 |

|  |  |
| --- | --- |
| **ZAJĘCIA 9**  **(3 godz.)**  **Bezpieczeństwo haseł (funkcje haszujące, metody łamania)** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie znał formę składowania haseł w systemie Windows. 2. Student będzie umiał pozyskać hasz hasła konta użytkownika systemu Windows. 3. Student będzie umiał skorzystać z wybranych programów do łamania haseł w systemie Kali Linux. 4. Student będzie umiał nadpisać hasło użytkownika systemu Windows. |
| Treści zajęć | 1. Pozyskiwanie haseł i ich haszy. 2. Metody łamania haseł w programach: John the Ripper oraz HashCat w systemie Kali Linux. 3. Nadpisywanie haseł użytkowników programem chntpw z poziomu systemu Kali Linux. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - McClure S., Hacking Exposed (7): Network Security Secrets and Solutions, 2012  - Stallings W., Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, 2012  Rozszerzające / uzupełniające:  - John The Ripper - Łamanie haseł i hashy,  https://www.youtube.com/watch?v=DglTmtwPqZE  - how to HACK a password // password cracking with Kali Linux and HashCat,  https://www.youtube.com/watch?v=z4\_oqTZJqCo  - How to Dump NTLM Hashes & Crack Windows Passwords,  https://null-byte.wonderhowto.com/how-to/hacking-windows-10-dump-ntlm-hashes-crack-windows-passwords-0198268/  - Cracking Windows Hashes,  https://robertscocca.medium.com/cracking-windows-hashes-fb0af3108c0a  - chntpw – Windows Password, Account Forensics & Change User Password,  https://kalilinuxtutorials.com/chntpw/ |

|  |  |
| --- | --- |
| **ZAJĘCIA 10**  **(3 godz.)**  **Audyt systemu operacyjnego** | |
| Po tych zajęciach student (będzie znał/ wiedział/ umiał/ potrafił / rozumiał) | Efekty uczenia się:   1. Student będzie umiał zrealizować niektóre zadania audytora systemu Windows. 2. Student będzie umiał przeanalizować aktywność użytkownika systemu Windows w wybranych zakresach, na podstawie systemowej inspekcji zdarzeń. |
| Treści zajęć | 1. Ocena zgodności audytowanego systemu z dostarczonym wzorcem. 2. Inspekcja zdarzeń (audit policy) w systemie Windows. 3. Weryfikacja aktywności użytkownika systemu Windows w wybranych zakresach. |
| Źródło/a do nauki treści z tych zajęć | Minimalne / obowiązkowe:  - Liderman K, Patkowski A.E. „Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego”, Biuletyn Instytutu Automatyki i Robotyki, 19/2003, [link](http://www.ita.wat.edu.pl/cgi-bin/downloadCounter.cgi?sid=)  - The Windows Security Log Revealed, Chapter 2: Audit Policies and Event Viewer, 2009,  https://www.ultimatewindowssecurity.com/securitylog/book/page.aspx?spid=chapter2  Rozszerzające / uzupełniające:  - Liderman K, Patkowski A.E. „Metodyka LP-A – dziesięć lat później”, Przegląd Teleinformatyczny, nr 2, 2013, [link](http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-5327f351-469b-4732-b968-a356d00fc537/c/Liderman.pdf)  - Artykuły dotyczące zgodności (compliance) i wzorców konfiguracyjnych (baselines) publikowane w blogu:  https://techcommunity.microsoft.com/t5/microsoft-security-and/ct-p/MicrosoftSecurityandCompliance  - Windows Security Log Quick Reference Chart,  https://www.ultimatewindowssecurity.com/securitylog/quickref/Default.aspx |