

Zdalna pomoc i zarządzanie

Czas: 2 × 45 min

praca w parach (role: pomagający i użytkownik, potem zamiana)

Cel: Skonfigurowanie bezpiecznego zdalnego dostępu do komputerów: Pulpit zdalny z NLA, pomoc zdalna przez internet oraz SSH z uwierzytelnianiem kluczem i przesyłanie plików.

Po zajęciach potrafisz:

- włącza i konfiguruje Pulpit zdalny z uwierzytelnianiem na poziomie sieci oraz ogranicza krąg użytkowników
- udziela pomocy zdalnej programem RustDesk lub Pomoc szybka
- generuje parę kluczy SSH, instaluje klucz publiczny na serwerze i wyłącza logowanie hasłem
- przesyła pliki programem WinSCP z użyciem klucza
- wyjaśnia zagrożenia związane z wystawieniem RDP do internetu

Sprzęt i materiały

- dwa komputery stacjonarne z VirtualBox: maszyna wirtualna Windows 11 Pro i Ubuntu Server (karty sieciowe w trybie mostkowanym)

Oprogramowanie

- **Podłączanie pulpitu zdalnego (`mstsc`)** — wbudowany w Windows; serwer RDP tylko w wersjach Pro, Education, Enterprise
- **RustDesk** — darmowy, open source; pobieranie z GitHub: <https://github.com/rustdesk/rustdesk/releases>
rustdesk.com
- **Pomoc szybka (Quick Assist)** — opcjonalnie — pomagający musi zalogować się kontem Microsoft
apps.microsoft.com
- **OpenSSH (klient w Windows, serwer w Ubuntu)** — `ssh`, `ssh-keygen` są wbudowane w Windows 11
ubuntu.com/server/docs
- **WinSCP** — przesyłanie plików SFTP
winscp.net/eng/download.php

Przygotowanie przed zajęciami

- Sprawdź, że obie maszyny wirtualne uruchamiają się i mają adresy IP z sieci pracowni (`ipconfig`, `ip a`). Wykonaj migawki.
- Pobierz RustDesk (wersja dla Windows, x64) i WinSCP na pendrive.

Bezpieczeństwo

- Zdalny dostęp konfiguruj tylko w maszynach wirtualnych — nie włączaj Pulpitu zdalnego ani RustDesk na stałe w szkolnym systemie.
- Nigdy nie podawaj nikomu identyfikatora i hasła RustDesk ani kodu Pomocy szybkiej poza ćwiczeniem — tak działają oszuści podający się za serwis.
- Klucz prywatny SSH (`id_ed25519`) zostaje tylko u Ciebie — nie kopiuj go na serwer ani do sprawozdania.
- Przy zmianie konfiguracji SSH nie zamykaj działającej sesji, dopóki nie sprawdzisz w drugim oknie, że logowanie kluczem działa.
- Po zajęciach wyłącz Pulpit zdalny i usuń RustDesk z VM albo przywróć migawki.

Przebieg zadania

1 Pulpit zdalny (RDP)

Na maszynie wirtualnej Windows 11 Pro partnera.

1. Partner: Ustawienia → System → Pulpit zdalny → włącz. Rozwiń ustawienia i sprawdź, że włączone jest wymaganie uwierzytelniania na poziomie sieci (NLA).
2. Partner: dodaj konto standardowe `uczen` do grupy uprawnionych: w PowerShell (administrator) `Add-LocalGroupMember -SID S-1-5-32-555 -Member uczen` (SID grupy Użytkownicy pulpitu zdalnego).
3. Ty: sprawdź dostępność portu `Test-NetConnection <IP> -Port 3389`, uruchom `mstsc`, połącz się jako `uczen`. Zrób zrzut i zanotuj, co widzi w tym czasie partner.
4. Wpisz celowo złe hasło jeden raz. Partner odszukuje w Podglądzie zdarzeń → Dzienniki systemu Windows → Zabezpieczenia zdarzenia 4624 i 4625 i zapisuje adres źródłowy.

2 Pomoc zdalna przez internet

Symulacja: „użytkownik” prosi o pomoc w zmianie ustawienia.

1. Użytkownik uruchamia RustDesk (bez instalacji) i podaje pomagającemu identyfikator i jednorazowe hasło.
2. Pomagający łączy się, zmienia u użytkownika wskazane przez nauczyciela ustawienie (np. ikonę pulpitu albo rozdzielczość) i przesyła mu plik przez okno przesyłania plików.
3. Użytkownik kończy sesję i zamyka program. Zanotujcie, jakie uprawnienia (klawiatura, schowek, pliki) można odebrać pomagającemu.
4. Opcjonalnie: powtórzcie test Pomocą szybką i porównajcie oba narzędzia w tabeli.

3 SSH z kluczem

Na Ubuntu Server partnera (z zadania 10), z Windows (komputer lub VM).

- Połącz się hasłem: `ssh <użytkownik>@<IP> serwera` i zaakceptuj odcisk klucza serwera. Zapisz go.
- Na Windows wygeneruj klucze: `ssh-keygen -t ed25519 -C "imie-nazwisko"` (ustaw hasło do klucza).
- Skopiuj klucz publiczny na serwer w PowerShell: `type $env:USERPROFILE\.ssh\id_ed25519.pub | ssh <użytkownik>@<IP> "mkdir -p ~/.ssh && chmod 700 ~/.ssh && cat >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"`.
- Sprawdź logowanie kluczem (system pyta o hasło do klucza, nie do konta).
- Na serwerze utwórz `sudo nano /etc/ssh/sshd_config.d/10-tylko-klucze.conf` z liniami `PasswordAuthentication no` i `KbdInteractiveAuthentication no`. Sprawdź `sudo sshd -t` i `sudo sshd -T | grep -i passwordauthentication`, potem `sudo systemctl restart ssh`.
- W nowym oknie spróbuj zalogować się bez klucza: `ssh -o PubkeyAuthentication=no <użytkownik>@<IP>` — oczekiwany wynik: `Permission denied (publickey)`.

4 Przesyłanie plików WinSCP

- W WinSCP utwórz sesję SFTP do serwera. W Zaawansowane → SSH → Uwierzytelnianie wskaż plik klucza prywatnego (WinSCP zaproponuje konwersję do formatu .ppk — zgódź się).
- Prześlij na serwer plik tekstowy, a z serwera pobierz `/etc/os-release`. Zrób zrzut okna WinSCP.
- Wyłącz Pulpit zdalny w VM Windows i zamknij RustDesk.

W sprawozdaniu umieść

- ☐ zrzuty: połączenie RDP, zdarzenia 4624/4625, sesja RustDesk, odmowa logowania hasłem SSH, okno WinSCP
- ☐ tabela porównania narzędzi zdalnego dostępu
- ☐ zawartość pliku `10-tylko-klucze.conf` i wynik `sshd -T`
- ☐ krótka notatka: zasady bezpiecznej pomocy zdalnej dla użytkownika (3–5 punktów)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

- Dlaczego nie należy udostępniać portu 3389 (RDP) bezpośrednio do internetu i jak bezpiecznie dać pracownikowi dostęp z domu?
- Co daje uwierzytelnianie na poziomie sieci (NLA)?
- Dlaczego logowanie kluczem SSH jest bezpieczniejsze od hasła i co się stanie, gdy ktoś ukradnie klucz prywatny bez hasła?
- Czym różni się RDP (osobna sesja) od pomocy zdalnej typu RustDesk/Pomoc szybka (wspólny ekran) i kiedy wybrać każde z nich?

Kryteria oceny

Kryterium	Punkty
RDP z NLA, uprawnienia i analiza dziennika zdarzeń	5
Sesja pomocy zdalnej i porównanie narzędzi	3
SSH z kluczem i wyłączone logowanie hasłem (sprawdzone na stanowisku)	6
Przesyłanie plików WinSCP	2
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).