Anna Bieńkowska, Mateusz Murawski

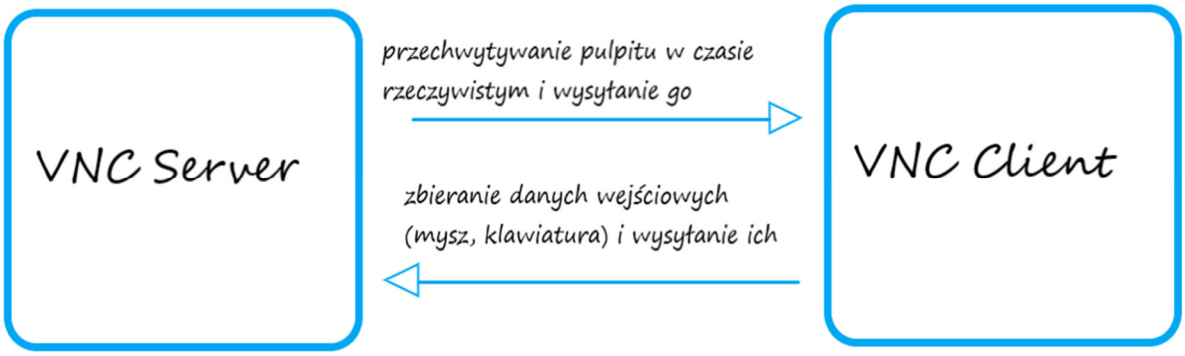
VNC

Informacje ogólne

VNC jest to graficzny system współdzielenia ekranu, zdalnego sterowania innym komputerem. Zazwyczaj jest używany do zdalnego wsparcia technicznego oraz do udostępniania plików pomiędzy pracą a domem.

System VNC wykorzystuje protokół Remote Frame Buffer (RFB). RFB jest prostym protokołem umożliwiającym zdalny dostęp do graficznego interfejsu użytkownika. Protokół ten ma zastosowanie we wszystkich systemach okienkowych i aplikacjach, w tym Windows, X11, macOS.

Działanie serwera VNC sprowadza się do wysyłania obrazu pulpitu za każdym razem, gdy pulpit komputera zdalnego jest aktualizowany. Ponieważ wielokrotne wysyłanie zmienionego obrazu przez sieć wymaga dużej ilości zasobów, więc protokół RFB aktualizuje jedynie te piksele obrazu, które uległy zmianie.



Oryginalna wersja VNC używana jest jedynie do celów referencyjnych i testów zgodności. Obecnie stosuje się różne implementacje systemu VNC, między innymi:

- RealVNC - oferuje zdalną dostępność każdego przełącznika KVM (Keyboard, Video, Mouse) przez TCP/IP i dowolną przeglądarkę VNC; posiada również wersję komercyjną.
- TightVNC - oferuje udoskonaloną kompresję danych i obsługę transferu plików.
- UltraVNC - uważana przez wielu za najbardziej zaawansowaną wersję. Oferuje ulepszoną kompresję, obsługę wideo, transfer plików, funkcję czatu. Ostatnio rozwijaną funkcją była płynna obsługa okien - zdalne sterowanie pojedynczym oknem programu, zamiast całym pulpitem.

Bezpieczeństwo

VNC jest systemem typu klient-serwer, dlatego też mamy dwie możliwości ataku na system:

1. Atakujący korzysta z tej samej sieci co VNC server i próbuje go przejąć, aby wykonywać kod z uprawnieniami serwera.
2. Użytkownik łączy się z serwerem atakującego, a ten wykorzystując luki w zabezpieczeniach klienta, wykonuje kod na komputerze użytkownika.

Aby uniemożliwić cyberprzestępcom wykorzystanie luk w zabezpieczeniach systemu VNC zaleca się:

1. Sprawdzić, które z urządzeń mogą się łączyć zdalnie i uniemożliwić zdalne łączenie się w przypadku, gdy nie jest ono potrzebne.
2. Sprawdzić aktualność wersji VNC.
3. Chronić się silnymi hasłami.
4. Łączyć się jedynie z zaufanymi i przetestowanymi serwerami VNC.

W przedsiębiorstwach często stosuje się dodatkowe, specjalistyczne rozwiązania zabezpieczające.

Poszczególne implementacje systemu VNC radzą sobie z lukami w zabezpieczeniach w różny sposób:

1. UltraVNC wspiera użycie ogólnodostępnej wtyczki szyfrującej całą sesję VNC łącznie z uwierzytelnianiem hasła i transferem danych.
2. RealVNC oferuje szyfrowanie AES, jednak w wersji komercyjnej.
3. TightVNC nie używa szyfrowania, jest więc najmniej bezpieczne, jednak jego użytkownicy mogą zabezpieczyć się poprzez tunelowanie.

Dzięki tunelowaniu poprzez połączenie SSH lub VPN (dostępne dla większości platform) można uzyskać kolejną warstwę zabezpieczeń dla systemu VNC.

Najpopularniejsze protokoły służące do zdalnej pracy w trybie graficznym

1. RFB
    a. Dostępny dla większości systemów operacyjnych, w tym Windows, Linux, Solaris.
    b. Pracuje na poziomie bufora ramki, w którym znajdują się informacje o pojedynczym pikselu w ramce obrazu.

c. Nakłada niewiele wymagań na klienta - było to główne założenie w projektowaniu RFB.
d. Stan klienta po rozłączeniu z serwerem i ponownym połączeniu pozostaje bez zmian.
e. Interfejs aplikacji użytkownika jest mobilny - do połączenia z tym samym serwerem klient może użyć innego endpointa. Na nowym endpoincie klient ujrzy dokładnie ten sam interfejs, co na oryginalnym endpoincie, w niezmienionym stanie.

2. RDP
   a. Wykorzystywany jest głównie w aplikacjach windowsowych, ale również przez systemy operacyjne takie jak Linux, FreeBSD, Solaris i OS X.
   b. Używa szyfru RSA Security RC4 do wydajnego szyfrowania małych ilości danych.
   c. Stosuje mechanizmy kompresji danych, trwałego buforowania bitmap i fragmentów w pamięci RAM, co poprawia wydajność zwłaszcza w przypadku aplikacji, które wykorzystują duże mapy bitowe
   d. Użytkownik może rozłączyć się z sesją pulpitu zdalnego bez wylogowywania się (tak dzieje się np. przy awarii sieci). Po ponownym zalogowaniu się do systemu z dowolnego urządzenia, użytkownik łączy się z rozłączoną sesją w tym samym stanie.
3. NX
   a. Dostępny dla wielu systemów operacyjnych, w tym Windows, iOS, Linux.
   b. Od wersji 4.0 została wprowadzona optymalna kompresja danych, buforowanie oraz nowe techniki kodowania wideo.
   c. Umożliwia uwierzytelnianie za pomocą hasła, klucza prywatnego lub uwierzytelniania z użyciem protokołu Kerberos.
   d. Kontroluje przepływ informacji, dynamicznie dostosowuje kompresję i przepustowość zgodnie z szybkością i pojemnością sieci.
   e. Dane NX mogą być przesyłane w strumieniach TCP i UDP, co jest dynamicznie ustalane przez klienta i serwera na podstawie typu danych i warunków sieciowych.
4. X11
   a. Głównie używany do tworzenia graficznych interfejsów użytkownika w systemie Linux, ale jest też obsługiwany przez prawie wszystkie inne nowoczesne systemy operacyjne.
   b. Może używać *SSH with X forwarding* aby uruchamiać aplikacje graficzne w bezpieczny sposób.
   c. W podstawowym protokole X Window System przez sieć wysyłane są (asynchronicznie) cztery rodzaje pakietów:

i. żądania - prośby o wykonanie jakiejś operacji i odesłanie przechowywanych danych, wysyłane przez klienta do serwera
ii. odpowiedzi - informacje zwrotne odnośnie żądań wysyłane od serwera do klienta
iii. zdarzenia - powiadomienia wysyłane klientom przez serwer
iv. błędy - powiadomienia wysyłane klientom przez serwer związane z błędami powstałymi podczas przetwarzania żądań

Wady i zalety VNC

Wady

1. Brak funkcji zabezpieczeń w większości dostępnych programów.
2. Problemy z wydajnością, które narastają w miarę korzystania z aplikacji interaktywnych, czy programów czasu rzeczywistego.
3. Lepsze zabezpieczenia oferowane są często w komercyjnych wersjach VNC.

Zalety

1. Darmowy, dzięki użyciu licencji GPL darmowego i otwartego oprogramowania.
2. Jest niezależny od platformy oraz kompatybilny z każdym systemem operacyjnym.
3. Część wersji systemu VNC oferuje udoskonaloną kompresję danych i lepszy transfer plików, a także obsługę wideo.
4. Poszczególne wersje stosują mechanizmy szyfrowania pomagające zabezpieczyć system.

Część praktyczna – Real VNC

Pakiet VNC Connect jest jednym z produktów dostarczanych przez Real VNC. Składa się on z dwóch programów: VNC Server oraz VNC Viewer, które stanowią odpowiednio usługę serwera i klienta VNC.

Instalacja i uruchomienie VNC Connect

Proces instalacji serwera VNC

0. Jeżeli korzystasz z systemu operacyjnego bez graficznego interfejsu użytkownika, musisz go zainstalować[1]

```
yum group list
yum groupinstall "Fedora Workstation" --skip-broken
```

Uruchomienie usługi poprzez komendę:

```
systemctl start graphical.target
```

Nie trzeba insalowac calej grupy. Wysta

1. Instalacja VNC Server
   1.1. Pobierz plik instalacyjny VNC Server ze witryny internetowej Real VNC. W tym celu musisz założyć konto i wykupić interesujący Cię pakiet lub skorzystać z 30-dniowego okresu próbnego. W celach demonstracyjnych zalecany jest okres próbny wersji Enterprise, który umożliwia dostęp do uruchamiania nowej sesji dla każdego logującego się użytkownika.
   1.2. Zainstaluj pobrany VNC ze wszystkim wymaganymi pakietami:

```
sudo yum install ./VNC-Server-6.7.2-Linux-x86.rpm
```

Uwaga techniczna: podobna funkcj

2. Konfiguracja VNC Server
   2.1. Pobierz i wypakuj plik vncsetup.sh dostępny na witrynie Real VNC
   2.2. Uruchom interface graficzny i uruchom konfigurator VNC

```
systemctl start graphical.target
chmod +x vncsetup.sh
./vncsetup.sh
```

   2.3. W menu wybierz opcję
   „1. License VNC Server and enable cloud connectivity”, a następnie

[1] https://ulyaoth.com/tips-tricks/how-to-install-a-graphical-desktop-on-fedora-server/

„2. Sign in to your RealVNC account to activate subscription”

2.4. Podążaj za poleceniami konfiguratora VNC|

2.5. Teraz możesz uruchomić VNC server

Proces instalacji klienta VNC Viewer

1. Pobierz plik instalacyjny VNC Server ze witryny internetowej Real VNC. Również w tym celu musisz posiadać konto Real VNC.
2. Uruchom instalator i podążaj za wskazanymi instrukcjami

   ```
   sudo yum install ./VNC-Server-6.7.2-Linux-x86.rpm
   ```

3. Uruchom program w interfejsie graficznym lub poprzez komendę

   ```
   sudo yum install ./VNC-Server-6.7.2-Linux-x86.rpm
   ```

4. Zaloguj się i wybierz dostępny serwer.

Istnieje wiele roznych aplikacji klie

Uruchomienie usług

Po zainstalowaniu usługi Server i Viewer na dwóch osobnych maszynach otrzymujemy dostęp do zestawu trybów[2]. W szczególności:

1. Tryb wirtualny – tworzy wirtualny pulpit, środowisko i niezależną sesję użytkownika na maszynie hosta do czasu rozłączenia lub wylogowania z sesji (ekran ponownego logowania nie pojawi się). W celu uruchomienia serwera należy użyć komendy:

   ```
   vncserver-virtual
   ```
   lub
   ```
   vncserver-virtuald
   ```

   Druga komenda uruchamia daemona, który tworzy sesję użytkownika na każde żądanie uprawnionego użytkownika VNC Viewer. Aby uruchamiać usługę przy uruchomieniu systemu należy zastosować polecenie:

   ```
   systemctl enable vncserver-virtuald.service #systemd
   update-rc.d vncserver-virtuald defaults #initd
   ```

2. Tryb użytkownika – umożliwia zdalny dostęp do sesji obecnie zalogowanego użytkownika. Klient ma podgląd i kontrolę nad obecnie wyświetlaną sesją użytkownika serwera do czasu rozłączenia lub wylogowania. W celu uruchomienia serwera należy użyć komendy:

[2] https://help.realvnc.com/hc/en-us/articles/360002251417

```
vncserver-x11
```

3. Tryb serwisowy – umożliwia zdalny dostęp do sesji obecnie zalogowanego użytkownika. Klient ma podgląd i kontrolę nad obecnie wyświetlaną sesją użytkownika serwera. Tryb ten w odróżnieniu od trybu użytkownika utrzymuje połączenie, gdy użytkownik serwera zostanie wylogowany. W celu uruchomienia serwera należy użyć komendy:

   ```
   vncserver-x11-serviced
   ```

   Aby uruchamiać usługę przy uruchomieniu systemu należy zastosować polecenie:

   ```
   systemctl enable vncserver-x11-serviced.service #systemd
   update-rc.d vncserver-x11-serviced defaults #initd
   ```

Aby klient VNC Viewer mógł połączyć się z serwerem konieczne jest dołączenie go do zespołu w ustawieniach użytkownika manage.realvnc.com. Następnie po zalogowaniu wystarczy kliknąć dwukrotnie na wybrany serwer dostępny na głównej karcie uruchomionego klienta.

Konfiguracja VNC Connect

Dla każdej z usług opisanych powyżej VNC aplikuje kolejne pliki konfiguracyjne[3]:

1. VNC Server w trybie serwisowym

   ```
   /etc/vnc/config.d/common.custom
   /etc/vnc/config.d/vncserver-x11
   /root/.vnc/config.d/common
   /root/.vnc/config.d/vncserver-x11
   /etc/vnc/policy.d/common
   /etc/vnc/policy.d/vncserver-x11
   ```

2. VNC Server w trybie użytkownika

   ```
   /etc/vnc/config.d/common.custom
   /etc/vnc/config.d/vncserver-x11
   ~/.vnc/config.d/common
   ~/.vnc/config.d/vncserver-x11
   <parametry linii poleceń>
   /etc/vnc/policy.d/common
   /etc/vnc/policy.d/vncserver-x11
   ```

3. VNC Server w trybie wirtualnym

   ```
   /etc/vnc/config.d/common.custom
   /etc/vnc/config.d/Xvnc
   ~/.vnc/config.d/common
   ~/.vnc/config.d/Xvnc
   ```

[3] https://help.realvnc.com/hc/en-us/articles/360002253878-Configuring-VNC-Connect-Using-Parameters

```
<parametry linii poleceń>
/etc/vnc/policy.d/common
/etc/vnc/policy.d/Xvnc
```

4. VNC Server w trybie wirtualnym, uruchamianym poprzez daemon

```
/etc/vnc/config.d/common.custom
/etc/vnc/config.d/vncserver-virtuald
/root/.vnc/config.d/common
/root/.vnc/config.d/vncserver-virtuald
<parametry linii poleceń>
/etc/vnc/policy.d/common
/etc/vnc/policy.d/vncserver-virtuald
```

5. VNC Viewer

```
/etc/vnc/config.d/common.custom
/etc/vnc/config.d/vncviewer
~/.vnc/config.d/common
~/.vnc/config.d/vncviewer
<parametry linii poleceń>
/etc/vnc/policy.d/common
/etc/vnc/policy.d/vncviewer
```

Struktura pliku konfiguracyjnego

Każdy z powyższych plików posiada następującą budowę:

- każdy parametr powinien znajdować się w osobnym wierszu
- początkowe i końcowe białe znaki oraz komentarze (poprzedzone „#”) są pomijane
- mogą zawierać zmienne środowiskowe

Przykładowy fragment pliku konfiguracyjnego:

```
#To jest komentarz
Desktop=Build machine
Encryption=AlwaysOn
Authentication=SystemAuth
RsaPrivateKeyFile=$HOME/secure/vnc
Permissions=admin:f,vncusers:d,guests:v
```

Z pełną listą dostępnych opcji można zapoznać się w dokumentacji real VNC[4].

[4] https://help.realvnc.com/hc/en-us/articles/360002254318

Logi VNC Connect

Logi standardowe

Domyślnie VNC Viewer i VNC Server rejestrują podstawowe informacje o aktywności połączenia. Rejestrowanie jest automatycznie włączane w `syslog` oraz zapisywane do pliku zlokalizowanego w domyślnym folderze wyjściowym VNC. Lokalizację i nazwę pliku używanego do zapisu można zmienić za pomocą odpowiednich parametrów[5].

Domyślne miejsce docelowe danych wyjściowych z serwera VNC (określone przez parametr Log):

- tryb wirtualny
  `~/.vnc/<computer>:<display-number>.log`
- tryb użytkownika
  ~/.vnc/vncserver-x11.log
- tryb serwisowy
  /var/log/vncserver-x11.log

Logi debugowania

Aby program VNC Viewer i VNC Server rejestrował szczegółowe logi należy odpowiednio ustawić parametr `Log` w pliku konfiguracyjnym lub jako parametr uruchomienia.

Podaj uporządkowaną listę działań oddzielonych przecinkami, każda z postaci:

```
<log>: <target>: <level>
```

- `<log>` określa typ czynności do zarejestrowania, dostępne wartości:

  ```
  connection
  printing
  file transfer activity
  ```
  `*`, aby rejestrować wszystko.

  Aby zobaczyć listę dostępnych działań dla konkretnych usług uruchom polecenie:
  `<app> -help all`

- `<target>` określa docelowe miejsce docelowe. W systemie Linux `syslog` (skonfigurowany przy użyciu `SyslogFacility`), `stderr` lub plik.
- `<level>` określa wagę:
  0 obejmuje tylko poważne błędy

[5] https://help.realvnc.com/hc/en-us/articles/360002254238-All-About-Logging, więcej o odpowiednich parametrach patrz przypis 4.

10 obejmuje podstawowe informacje audytu
30 zawiera informacje ogólne
100 obejmuje wszystkie możliwe informacje, w tym potencjalnie naciśnięcia klawiszy.

Jeśli używasz SysLog, `<level>` tłumaczy w następujący sposób:
0 to Syslog 3 (błąd)
od 1 do 5 to 4 (ostrzeżenie)
6 do 10 to 5 (uwaga)
11 do 30 to 6 (informacje)
więcej niż 30 to 7 (debugowanie).

Przykład:
`*:file:10,Connections:file:100`

Pierwsza pozycja `(*:file:10)` określa, że cała aktywność jest rejestrowana w pliku na poziomie 10.
Drugi wpis (`Connections:file:100`) nadpisuje to dla aktywności związanej z połączeniem, zapisując ją (do tego samego pliku) na poziomie 100.

Bezpieczeństwo VNC Connect[6]

VNC Connect jest domyślnie wyposażony w systemy bezpieczeństwa. Wszystkie połączenia są szyfrowane end-to-end, a komputery zdalne są domyślnie chronione hasłem (subskrypcja Home) lub poświadczeniami logowania systemu (subskrypcja Professional i Enterprise). Wszystkie przeglądy i linki do oficjalnych dokumentów, testów penetracyjnych i nie tylko są zamieszczane na
Dodatkowo jest możliwość uruchomienia dodatkowych funkcji w celu zwiększenia bezpieczeństwa:

1. Dostępne schematy uwierzytelniania:
   - Hasło konta VNC
   - Autentyfikacja systemu (hasło użytkownika)
   - Single sign-on – dostęp do usług tylko z sieci wewnętrznej
   - Magazyn kart inteligentnych/certyfikatów
   - Autentyfikacja RADIUS[7]
2. Uwierzytelnianie wieloskładnikowe
3. Ustawienie 256-bitowego AES poprzez ustawienie parametru szyfrowania (dla wybranego z powyższych schematów) na `AlwaysMaximum`

[6] https://help.realvnc.com/hc/en-us/articles/360002253278-Setting-up-VNC-Connect-for-Maximum-Security-
[7] https://help.realvnc.com/hc/en-us/articles/360002253538-Setting-up-RADIUS-Authentication-

4. Ustawienia łączności bezpośredniej, poprzez ustawienie parametru `AllowIpListenRfb` serwera VNC na `FALSE`.
5. Odpowiednie ograniczenia uprawnień sesji, aby poszczególni użytkownicy mieli dostęp tylko do wyznaczonych zasobów.
6. Zmniejszenie liczby dozwolonych nieudanych prób uwierzytelnienia, obniżając parametr serwera `BlacklistThreshold`.
7. Rozłączanie bezczynnych sesji poprzez ustawienie parametru Serwera `IdleTimeout`.
8. Zablokuj lub wyloguj zdalny pulpit, gdy ostatni użytkownik rozłączy się, ustawiając parametr serwera `DisconnectAction`.
9. Zminimalizowanie ilości przechowywanych w chmurze danych[8]

[8] https://help.realvnc.com/hc/en-us/articles/360002312178

Bibliografia

1. https://en.wikipedia.org/wiki/Virtual_Network_Computing
2. http://ipinfo.info/html/vnc_remote_control.php
3. https://www.comparitech.com/vpn/what-is-a-vnc-and-how-does-it-differ-from-a-vpn/
4. https://help.realvnc.com/hc/en-us/articles/360002320638-How-does-VNC-technology-work-?fbclid=IwAR137K5SMA9ExF2kviElXeSAH6DBUBKD30BWLe1P_ty7s7S74-SvIEMUr1I
5. https://tools.ietf.org/html/rfc6143
6. https://ics-cert.kaspersky.com/reports/2019/11/22/vnc-vulnerability-research/
7. https://www.kaspersky.com/blog/vnc-vulnerabilities/31462/
8. https://pl.wikipedia.org/wiki/Remote_Desktop_Protocol
9. https://docs.microsoft.com/en-us/windows/win32/termserv/remote-desktop-protocol
10. https://en.wikipedia.org/wiki/NX_technology
11. https://en.wikipedia.org/wiki/X_Window_System_core_protocol
12. https://help.realvnc.com/hc/en-us/categories/360000301637-Documentation