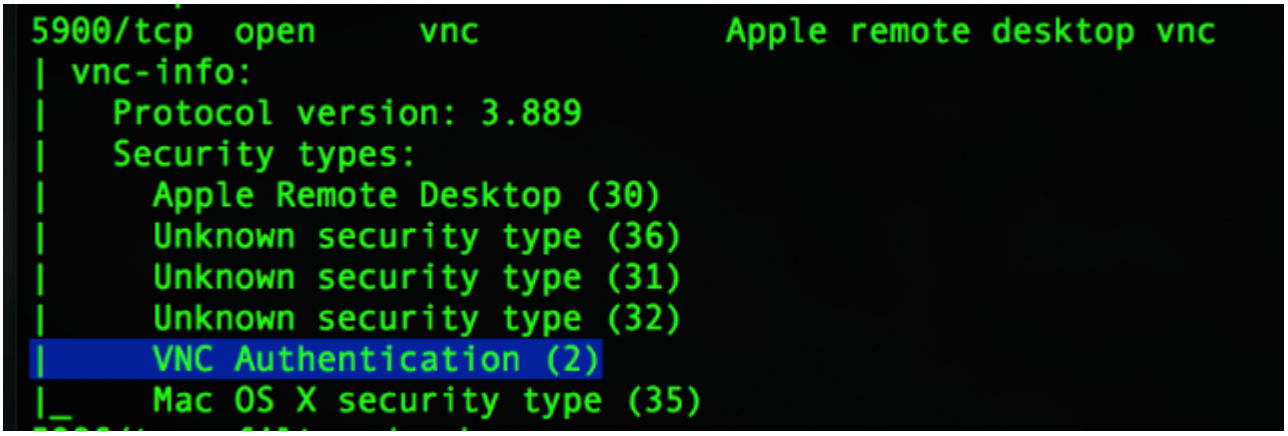
MacOS Red Teaming 206: ARD (Apple Remote Desktop Protocol)

By Action Dan

Archived: 2026-04-06 01:13:27 UTC

One of the things people always ask about when they are exploring MacOS pentesting is "what are the available lateral movement options?". Today we are going to explore one of the most popular methods of remote access for macOS, ARD or Apple Remote Desktop or Remote Management. There are several native ways to remotely access a macOS machine, specifically under the Sharing option in the System Preferences. The most interesting methods are Screen Sharing (tcp:5900), Remote Login (tcp:22), Remote Management (tcp:3283, tcp:5900), and Remote Apple Events (tcp:3031). Remote Login is essentially SSH access on port 22, which has been covered heavily from a security perspective many times before. I plan on covering Remote Apple Events on port 3031 in a later post, but this post will focus on Remote Management which is ARD and Screen Sharing which is just VNC.

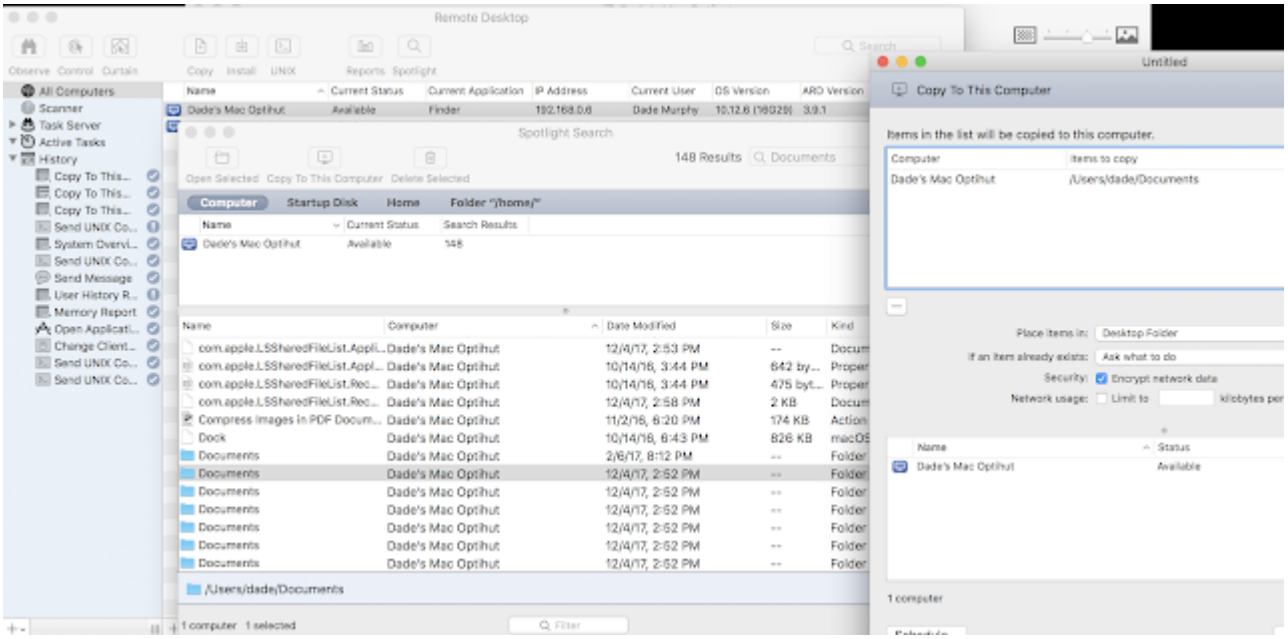
So today we are drilling down on ARD, which is essentially a bastardized VNC with some extra macOS specific features. Hosting an ARD server is native macOS functionality but the client costs $70 from the App Store. ARD is old software, and like a lot of Apple software it has evolved over the years into a mix of proprietary and open source software. It has largely merged with the VNC protocol to send the screen and control buffers, as well as for backwards compatibility with VNC clients. However, full ARD will also use protocols such as SSH for secure file transfer when you copy a file over. All VNC-like communications are encrypted with a minimum of 128bit AES. The Screen Sharing option is just a basic VNC server. There is also an advanced ARD or Remote Management option to set a control screen password which will make ARD backwards compatible for VNC clients. However there is a weakness to this authentication method that limits this password to an 8 character auth buffer, making it very easy to brute force with a tool like Hydra or GoRedShell (there are also no rate limits by default). You can identify vulnerable instances of Screen Sharing or Remote Management with nmap, using the script "vnc-info", and if the service supports "VNC Authentication (2)" then they are likely vulnerable to brute force. The service will truncate all passwords sent on the wire down to 8 characters, such that if you set the VNC auth to "password", both "passwords" and "password123" will authenticate.



When you use the ARD client to connect to mac machine, there are methods to lock down the permissions based on groups, however many admins will take the simpler route of using a shared local account across multiple machines. In fact, the ARD admin wizard prompts the administrator to create such a user on their first connect, which was a historical weakness in Windows as it allowed for lateral movement once that user's password was compromised. There are some LAPS like solutions for macOS, but nothing official. You can use the *kickstart* command to launch and configure ARD in server mode from the command line. This can be useful for persistence or if you need to escalate from an SSH session, to say accept some TCC prompts. The following is a good kickstart commands to launch ARD for all users:

```
sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -activate -configure -allowAccessFor -allUsers -privs -all -clientopts -setmenuextra -menuextra yes
```

If you do get credentials to a machine with the ARD service running, it is an extremely rich service with many features that lend itself to pentesting. For example you can switch between observation mode, shared control, and full control, going from spying on a user to taking over their desktop at the click of a button. You can even lock a user out of their desktop while you make edits, although this is less advised. If you do get access to an ARD session, that session will remain open until the session is terminated, even if the user's password is changed during the session. You can also send unix commands directly over ARD and you can specify the root user to execute things as root if your an administrative user. You can even use this unix command method to schedule remote tasks to run at a specific time, however this occurs as a network connection at the specified time (vs being stored and executing on the target server). Finally, remote Spotlight is one of my favorite features. It's really neat because you can run a low impact, indexed search quickly and remotely. This is gold for searching for sensitive files because it's quick, lets you run searches concurrently across multiple machines, and won't spike the CPU. However this won't get directories which aren't indexed by Spotlight, such as *~/.ssh/* by default:



These events obviously leave logs. Spotlight searches will show up in logs, specifically the "Mac Analytic Data", however the contents of the search will not appear here. VNC logon and screen sharing events also appear here. Another good way to view these logs is using the new macOS "log" command, like so:

```
log show --last 3d --predicate 'processImagePath CONTAINS "screensharingd" AND eventMessage CONTAINS "Authentication"'
```

Finally you can also use an ARD feature called Advanced System Reporting show things like recently touched files and memory usage. Here is an example of catching the VNC brute forcing and regular ARD authentication in the logs:

```
Dades-Mac-Optihut:~ dade$ log show --last 3d --predicate 'processImagePath CONTAINS "screensharingd" AND eventMessage CONTAINS "Authentication"'
Skipping info and debug messages, pass --info and/or --debug to include.
Filtering the log data using "processImagePath CONTAINS "screensharingd" AND eventMessage CONTAINS "Authentication""
Timestamp                       Thread     Type        Activity             PID
2019-07-18 19:58:44.589349-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.590196-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.590651-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.591047-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.591439-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.591819-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.592127-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.592451-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.592745-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.593024-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.593302-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: SUCCEEDED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.970894-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.974027-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.974682-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.975312-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:44.975898-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.192521-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.193262-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.193786-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.194110-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.194415-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.194727-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.195043-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.225597-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-18 19:58:45.225919-0700 0x9a3cb    Default     0x0                  2453   screensharingd: Authentication: FAILED :: User Name: N/A :: Viewer Address: 192.168.0.19 :: Type: VNC DES
2019-07-19 22:08:30.606980-0700 0xbb03e    Default     0x0                  2649   screensharingd: Authentication: SUCCEEDED :: User Name: dade :: Viewer Address: 192.168.0.19 :: Type: SRP
---------------------------------------------------------------------------------------------------------------------------
Log      - Default:         26, Info:              0, Debug:            0, Error:          0, Fault:          0
Activity - Create:           0, Transition:        0, Actions:          0
Dades-Mac-Optihut:~ dade$
```

Source: http://lockboxx.blogspot.com/2019/07/macos-red-teaming-206-ard-apple-remote.html