Red Teaming Articles

[**Windows Persistence using Application Shimming**](https://www.hackingarticles.in/windows-persistence-using-application-shimming/)

[**Windows for Pentester: BITSAdmin**](https://www.hackingarticles.in/windows-for-pentester-bitsadmin/)

[**Windows for Pentester: Certutil**](https://www.hackingarticles.in/windows-for-pentester-certutil/)

[**Guide to Red Team Operations**](https://www.hackingarticles.in/guide-to-red-team-operations/)

[**Command and Control & Tunnelling via ICMP**](https://www.hackingarticles.in/command-and-control-tunnelling-via-icmp/)

[**Cloakify-Factory: A Data Exfiltration Tool Uses Text-Based Steganography**](https://www.hackingarticles.in/cloakify-factory-a-data-exfiltration-tool-uses-text-based-steganography/)

[**Data Exfiltration using PowerShell Empire**](https://www.hackingarticles.in/data-exfiltration-using-powershell-empire/)

[**Get Meterpreter Session Alert over slack**](https://www.hackingarticles.in/get-meterpreter-session-alert-over-slack/)

[**Covert Channel: The Hidden Network**](https://www.hackingarticles.in/covert-channel-the-hidden-network/)

[**Command & Control: Ares**](https://www.hackingarticles.in/command-control-ares/)

[**Command & Control: WebDav C2**](https://www.hackingarticles.in/command-control-webdav-c2/)

[**Command & Control: WebSocket C2**](https://www.hackingarticles.in/command-control-websocketc2/)

[**Command and Control with DropboxC2**](https://www.hackingarticles.in/command-and-control-with-dropboxc2/)

[**dnscat2: Command and Control over the DNS**](https://www.hackingarticles.in/dnscat2-command-and-control-over-the-dns/)

[**Command & Control: Silenttrinity Post-Exploitation Agent**](https://www.hackingarticles.in/command-control-silenttrinity-post-exploitation-agent/)

[**Command & Control Tool: Pupy**](https://www.hackingarticles.in/command-control-tool-pupy/)

[**Command and Control Guide to Merlin**](https://www.hackingarticles.in/command-and-control-guide-to-merlin/)

[**nps\_payload: An Application Whitelisting Bypass Tool**](https://www.hackingarticles.in/nps_payload-an-application-whitelisting-bypass-tool/)

[**GreatSct – An Application Whitelist Bypass Tool**](https://www.hackingarticles.in/greatsct-an-application-whitelist-bypass-tool/)

[**Command and Control with HTTP Shell using JSRat**](https://www.hackingarticles.in/command-and-control-with-http-shell-using-jsrat/)

[**Koadic – COM Command & Control Framework**](https://www.hackingarticles.in/koadic-com-command-control-framework/)

[**TrevorC2 – Command and Control**](https://www.hackingarticles.in/trevorc2-command-and-control/)

[**Generate Metasploit Payload with Ps1encode**](https://www.hackingarticles.in/generate-metasploit-payload-with-ps1encode/)

[**Bypass Application Whitelisting using Weak Path Rule**](https://www.hackingarticles.in/bypass-application-whitelisting-using-weak-path-rule/)

[**Bypass Application Whitelisting using cmstp**](https://www.hackingarticles.in/bypass-application-whitelisting-using-cmstp/)

[**Bypass Application Whitelisting using rundll32.exe (Multiple Methods)**](https://www.hackingarticles.in/bypass-application-whitelisting-using-rundll32-exe-multiple-methods/)

[**Bypass Application Whitelisting using regsrv32.exe (Multiple Methods)**](https://www.hackingarticles.in/bypass-application-whitelisting-using-regsrv32-exe-multiple-methods/)

[**Bypass Application Whitelisting using wmic.exe (Multiple Methods)**](https://www.hackingarticles.in/bypass-application-whitelisting-using-wmic-exe-multiple-methods/)

[**Bypass Application Whitelisting using msbuild.exe (Multiple Methods)**](https://www.hackingarticles.in/bypass-application-whitelisting-using-msbuild-exe-multiple-methods/)

[**Bypass Application Whitelisting using mshta.exe (Multiple Methods)**](https://www.hackingarticles.in/bypass-application-whitelisting-using-mshta-exe-multiple-methods/)

[**Bypass Application Whitelisting using msiexec.exe (Multiple Methods)**](https://www.hackingarticles.in/bypass-application-whitelisting-using-msiexec-exe-multiple-methods/)

[**Windows Applocker Policy – A Beginner’s Guide**](https://www.hackingarticles.in/windows-applocker-policy-a-beginners-guide/)

[**Penetration Testing on Group Policy Preferences**](https://www.hackingarticles.in/penetration-testing-on-group-policy-preferences/)

[**Comprehensive Guide on MSFPC**](https://www.hackingarticles.in/comprehensive-guide-on-msfpc/)

[**Multiple Ways to Exploiting Windows PC using PowerShell Empire**](https://www.hackingarticles.in/multiple-ways-to-exploiting-windows-pc-using-powershell-empire/)

[**Empire GUI: Graphical Interface to the Empire Post-Exploitation Framework**](https://www.hackingarticles.in/empire-gui-graphical-interface-to-the-empire-post-exploitation-framework/)

[**OSX Exploitation with Powershell Empire**](https://www.hackingarticles.in/osx-exploitation-with-powershell-empire/)

[**Windows Persistence with PowerShell Empire**](https://www.hackingarticles.in/windows-persistence-with-powershell-empire/)

[**Multiple Ways to Exploiting OSX using PowerShell Empire**](https://www.hackingarticles.in/multiple-ways-to-exploiting-osx-using-powershell-empire/)

[**Hiding IP During Pentest using PowerShell Empire (http\_hop)**](https://www.hackingarticles.in/hiding-ip-during-pentest-using-powershell-empire-http_hop/)

[**Hacking with Empire – PowerShell Post-Exploitation Agent**](https://www.hackingarticles.in/hacking-with-empire-powershell-post-exploitation-agent/)