GitHub - Adaptix-Framework/AdaptixC2: AdaptixC2 is a highly modular advanced redteam toolkit

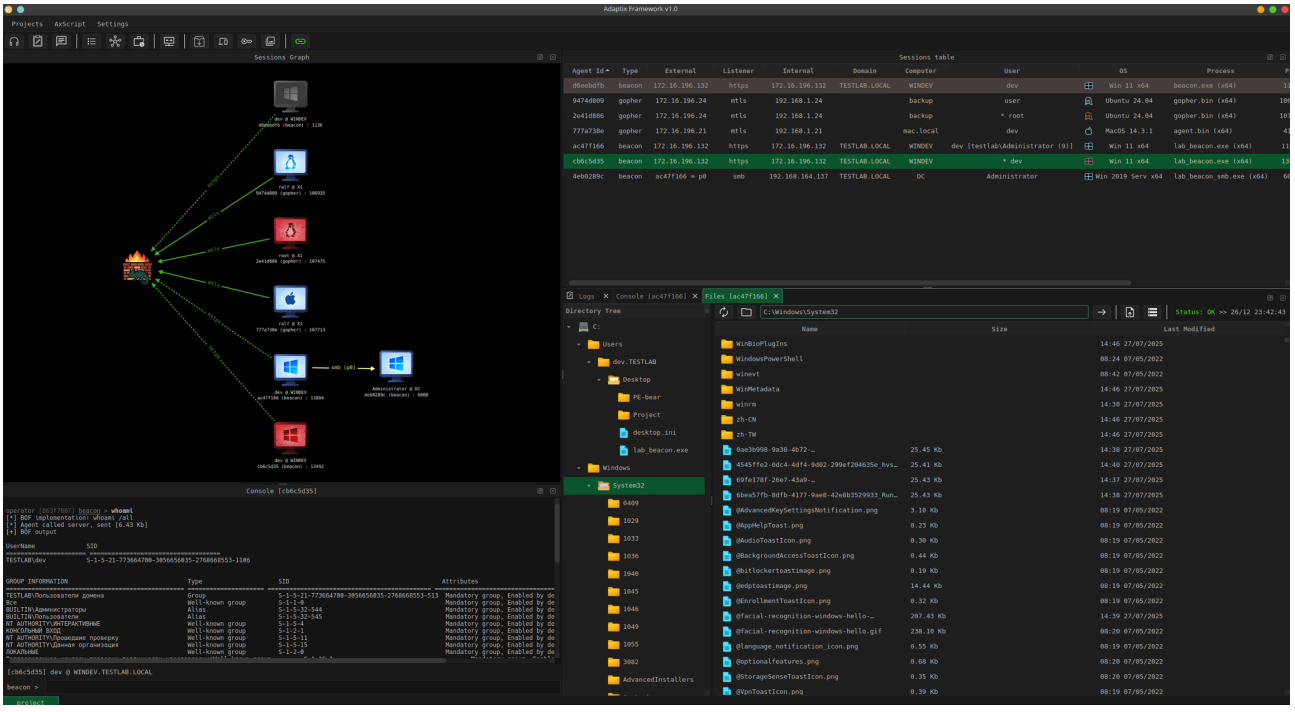
By RalfHacker

Archived: 2026-04-05 18:24:21 UTC

AdaptixC2 v1.2

FEB, 28: What has changed in version v1.2?

Adaptix is an extensible post-exploitation and adversarial emulation framework made for authorized penetration testing. The Adaptix server is written in Golang and to allow operator flexibility. The GUI Client is written in C++ QT, allowing it to be used on Linux, Windows, and MacOS operating systems. Full documentation is available here.



Legal Warning

This tool is designed for AUTHORIZED security testing and red team operations ONLY. Unauthorized use is strictly prohibited and may violate local and international laws. Use at your own risk.

Getting Started

Please checkout the wiki.

Features

- Server/Client Architecture for Multiplayer Support
- Cross-platform GUI client
- Fully encrypted communications
- Listener and Agents as Plugin (Extender)
- AxScript Engine
- Task and Jobs storage
- Credentials Manager
- Targets Manager
- Remote Terminal / Shell
- Files and Process browsers
- Socks4 / Socks5 / Socks5 Auth support
- Local and Reverse port forwarding support
- BOF & Async BOF support
- Linking Agents and Sessions Graph
- Agents Health Checker
- Agents KillDate and WorkingTime control
- Windows/Linux/MacOs agents support

Current Extenders

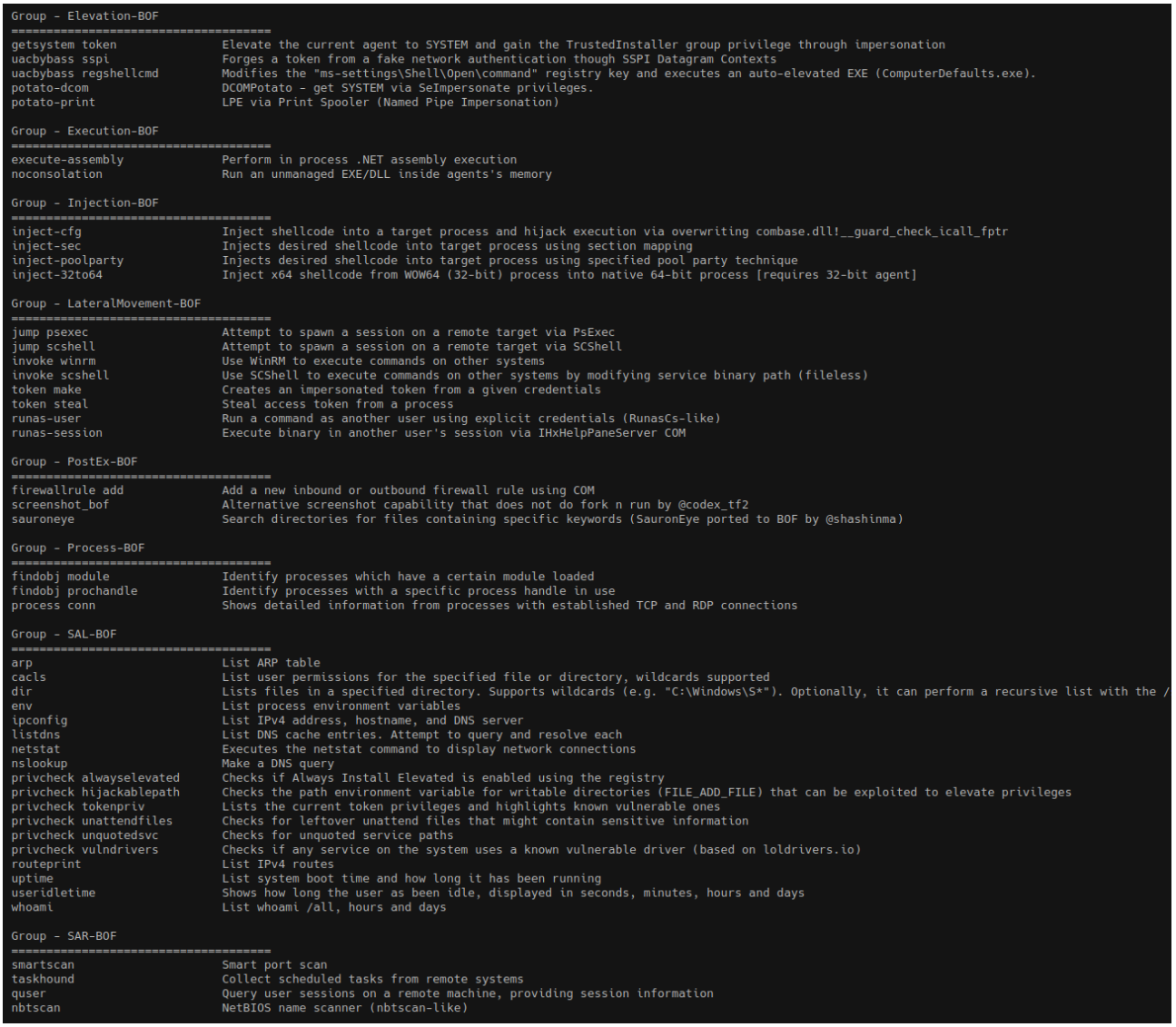
- HTTP/S Beacon Listener
- DNS/DoH Beacon Listener
- SMB Beacon Listener
- TCP Beacon Listener
- Beacon Agent
- TCP/mTLS Gopher Listener
- Gopher Agent

Extension-Kit

Official Extension-Kit on GitHub

```
Group - AD-BOF
==================================
adwssearch                    Executes ADWS query
badtakeover                   BOF for performing account takeover using the BadSuccessor technique
dcsync single                 Perform a DCSync operation on a single user
dcsync all                    Perform DCSync operations for all users in the domain
ldapsearch                    Executes LDAP query
ldapq computers               Get list of computers from ldap
readlaps                      Read LAPS password for a computer
webdav enable                 Enable the WebDAV client service without elevated permissions
webdav status                 Determine if the WebDAV is running on a remote system

Group - ADCS-BOF
==================================
certi auth                    Authenticate with certificate (PKINIT + UnPAC-the-hash)
certi enum                    Enumerate CAs and templates in the AD
certi request                 Request an enrollment certificate
certi request_on_behalf       Request certificate on behalf of another user (ESC3)
certi shadow                  Shadow Credentials attack - write KeyCredentialLink and get certificate

Group - Kerbeus-BOF
==================================
kerbeus asreproasting         Perform AS-REP roasting
kerbeus asktgt                Retrieve a TGT
kerbeus asktgs                Retrieve a TGS
kerbeus changepw              Reset a user's password from a supplied TGT
kerbeus dump                  Dump tickets
kerbeus hash                  Calculate rc4_hmac, aes128_cts_hmac_sha1, aes256_cts_hmac_sha1 hashes
kerbeus kerberoasting         Perform Kerberoasting
kerbeus klist                 List tickets
kerbeus ptt                   Submit a TGT
kerbeus describe              Parse and describe a ticket
kerbeus purge                 Purge tickets
kerbeus renew                 Renew a TGT
kerbeus s4u                   Perform S4U constrained delegation abuse
kerbeus cross_s4u             Perform S4U constrained delegation abuse across domains
kerbeus tgtdeleg              Retrieve a usable TGT for the current user without elevation by abusing the Kerberos GSS-API
kerbeus triage                List tickets in table format

Group - SQL-BOF
==================================
mssql 1434udp                 Obtain SQL Server connection information from 1434/UDP
mssql adsi                    Obtain ADSI creds from ADSI linked server
mssql agentcmd                Execute a system command using agent jobs
mssql agentstatus             Enumerate SQL Agent status and jobs
mssql checkrpc                Enumerate RPC status of linked servers
mssql clr                     Load and execute a .NET assembly in a stored procedure
mssql columns                 Enumerate columns within a table
mssql databases               Enumerate SQL databases
mssql disableclr              Disable CLR integration
mssql disableole              Disable OLE Automation Procedures
mssql disablerpc              Disable RPC and RPC out on a linked server
mssql disablexp               Disable xp_cmdshell
mssql enableclr               Enable CLR integration
mssql enableole               Enable OLE Automation Procedures
mssql enablerpc               Enable RPC and RPC out on a linked server
mssql enablexp                Enable xp_cmdshell
mssql impersonate             Enumerate users that can be impersonated
mssql info                    Gather information about the SQL Server
mssql links                   Enumerate linked servers
mssql olecmd                  Execute a system command using OLE automation procedures
mssql query                   Execute a custom SQL query
mssql rows                    Get the count of rows in a table
mssql search                  Search a table for a column name
mssql smb                     Coerce NetNTLM auth via xp_dirtree
mssql tables                  Enumerate tables within a database
mssql users                   Enumerate users with database access
mssql whoami                  Gather logged in user, mapped user and roles from SQL server
mssql xpcmd                   Execute a system command via xp_cmdshell
```

```
Group - LDAP-BOF
==================================
ldap get-acl                  Get ACL/security descriptor for an object
ldap get-attribute            Get specific attribute values (comma-separated list supported)
ldap get-computers            List all computers in the domain
ldap get-groups               List all groups in the domain
ldap get-groupmembers         List all members of a group
ldap get-delegation           Get delegation configuration for an object
ldap get-domaininfo           Get domain information from rootDSE
ldap get-maq                  Get machine account quota (ms-DS-MachineAccountQuota)
ldap get-object               Get all attributes of an object
ldap get-rbcd                 Get RBCD configuration for an object
ldap get-spn                  Get SPNs for an object
ldap get-uac                  Get UAC flags for an object
ldap get-users                List all users in the domain
ldap get-usergroups           List all groups a user is a member of
ldap get-writable             Find objects you have write access to
ldap move-object              Move an object to a different OU
ldap add-ace                  Add an ACE to an object's DACL
ldap add-attribute            Add a value to an attribute
ldap add-computer             Add a computer to the domain
ldap add-delegation           Add a delegation SPN to an object
ldap add-group                Add a group to the domain
ldap add-groupmember          Add a member to a group
ldap add-ou                   Add an organizational unit
ldap add-rbcd                 Add an RBCD delegation
ldap add-sidhistory           Add a SID to an object's sidHistory attribute
ldap add-spn                  Add an SPN to a object
ldap add-user                 Add a user to the domain
ldap add-uac                  Add UAC flags to an object
ldap add-genericall           Add a GenericAll ACE to an object's DACL
ldap add-genericwrite         Add a GenericWrite ACE to an object's DACL
ldap add-dcsync               Add DCSync ACEs to an object's DACL
ldap add-asreproastable       Make a user AS-REP roastable (set DONT_REQ_PREAUTH)
ldap add-unconstrained        Enable unconstrained delegation on an object
ldap add-constrained          Set/replace delegation SPNs
ldap set-attribute            Set/replace an attribute value
ldap set-delegation           Set/replace delegation SPNs
ldap set-owner                Set the owner of an object (requires WriteOwner)
ldap set-spn                  Set/replace all SPNs on an object
ldap set-password             Set/reset a user's password
ldap set-uac                  Set UAC flags (replaces all)
ldap remove-ace               Remove an ACE from an object's DACL
ldap remove-attribute         Remove an attribute or attribute value
ldap remove-delegation        Remove a delegation SPN
ldap remove-dcsync            Remove DCSync ACEs from an object's DACL
ldap remove-genericall        Remove a GenericAll ACE from an object's DACL
ldap remove-genericwrite      Remove a GenericWrite ACE from an object's DACL
ldap remove-groupmember       Remove a member from a group
ldap remove-object            Remove an object from the domain
ldap remove-rbcd              Remove an RBCD delegation
ldap remove-spn               Remove an SPN from an object
ldap remove-uac               Remove UAC flags from an object

Group - AD RelayInformer
==================================
relay-informer http           Inform on HTTP(S) service binding enforcement and HTTPS channel binding enforcement
relay-informer ldap           Inform on LDAP signing enforcement and LDAPS channel binding enforcement
relay-informer mssql          Inform on MSSQL service binding and channel binding enforcement
relay-informer smb            Inform on SMB2 signing enforcement

Group - Creds-BOF
==================================
askcreds                      Prompt for credentials
autologon                     Checks the registry for autologon information
credman                       Checks the current user's Windows Credential Manager for saved web passwords
get-netntlm                   Retrieve NetNTLM hash for the current user
hashdump                      Dump SAM hashes
cookie-monster                Locate and copy the cookie file used for Edge/Chrome/Firefox
nanodump                      Use syscalls to dump LSASS
nanodump_ppl_dump             Bypass PPL and dump LSASS
nanodump_ppl_medic            Bypass PPL and dump LSASS
nanodump_ssp                  Load a Security Support Provider (SSP) into LSASS
underlaycopy                  Copy file using low-level NTFS access (MFT or Metadata mode)
lsadump_secrets               Dump LSA secrets from SECURITY hive (requires SYSTEM)
lsadump_sam                   Dump SAM hashes (requires admin)
lsadump_cache                 Dump cached domain credentials (DCC2/MSCacheV2, requires SYSTEM)
```



```
Group - Elevation-BOF
=====================================
getsystem token               Elevate the current agent to SYSTEM and gain the TrustedInstaller group privilege through impersonation
uacbybass sspi                Forges a token from a fake network authentication though SSPI Datagram Contexts
uacbybass regshellcmd         Modifies the "ms-settings\Shell\Open\command" registry key and executes an auto-elevated EXE (ComputerDefaults.exe).
potato-dcom                   DCOMPotato - get SYSTEM via SeImpersonate privileges.
potato-print                  LPE via Print Spooler (Named Pipe Impersonation)

Group - Execution-BOF
=====================================
execute-assembly              Perform in process .NET assembly execution
noconsolation                 Run an unmanaged EXE/DLL inside agents's memory

Group - Injection-BOF
=====================================
inject-cfg                    Inject shellcode into a target process and hijack execution via overwriting combase.dll!__guard_check_icall_fptr
inject-sec                    Injects desired shellcode into target process using section mapping
inject-poolparty              Injects desired shellcode into target process using specified pool party technique
inject-32to64                 Inject x64 shellcode from WOW64 (32-bit) process into native 64-bit process [requires 32-bit agent]

Group - LateralMovement-BOF
=====================================
jump psexec                   Attempt to spawn a session on a remote target via PsExec
jump scshell                  Attempt to spawn a session on a remote target via SCShell
invoke winrm                  Use WinRM to execute commands on other systems
invoke scshell                Use SCShell to execute commands on other systems by modifying service binary path (fileless)
token make                    Creates an impersonated token from a given credentials
token steal                   Steal access token from a process
runas-user                    Run a command as another user using explicit credentials (RunasCs-like)
runas-session                 Execute binary in another user's session via IHxHelpPaneServer COM

Group - PostEx-BOF
=====================================
firewallrule add              Add a new inbound or outbound firewall rule using COM
screenshot_bof                Alternative screenshot capability that does not do fork n run by @codex_tf2
sauroneye                     Search directories for files containing specific keywords (SauronEye ported to BOF by @shashinma)

Group - Process-BOF
=====================================
findobj module                Identify processes which have a certain module loaded
findobj prochandle            Identify processes with a specific process handle in use
process conn                  Shows detailed information from processes with established TCP and RDP connections

Group - SAL-BOF
=====================================
arp                           List ARP table
cacls                         List user permissions for the specified file or directory, wildcards supported
dir                           Lists files in a specified directory. Supports wildcards (e.g. "C:\Windows\S*"). Optionally, it can perform a recursive list with the /
env                           List process environment variables
ipconfig                      List IPv4 address, hostname, and DNS server
listdns                       List DNS cache entries. Attempt to query and resolve each
netstat                       Executes the netstat command to display network connections
nslookup                      Make a DNS query
privcheck alwayselevated      Checks if Always Install Elevated is enabled using the registry
privcheck hijackablepath      Checks the path environment variable for writable directories (FILE_ADD_FILE) that can be exploited to elevate privileges
privcheck tokenpriv           Lists the current token privileges and highlights known vulnerable ones
privcheck unattendfiles       Checks for leftover unattend files that might contain sensitive information
privcheck unquotedsvc         Checks for unquoted service paths
privcheck vulndrivers         Checks if any service on the system uses a known vulnerable driver (based on loldrivers.io)
routeprint                    List IPv4 routes
uptime                        List system boot time and how long it has been running
useridletime                  Shows how long the user as been idle, displayed in seconds, minutes, hours and days
whoami                        List whoami /all, hours and days

Group - SAR-BOF
=====================================
smartscan                     Smart port scan
taskhound                     Collect scheduled tasks from remote systems
quser                         Query user sessions on a remote machine, providing session information
nbtscan                       NetBIOS name scanner (nbtscan-like)
```

CONTRIBUTING

Please push changes to the **dev** branch. Otherwise, changes will be made manually in the dev branch.

Source: https://github.com/Adaptix-Framework/AdaptixC2