



MIDA Multitool

Information Security Inc.

Contents

- About MIDA
- Testing Environment
- Installing MIDA
- Using MIDA
- References

About MIDA

- MIDA is a Bash script purposed for system enumeration, vulnerability identification and privilege escalation
- Aims to be a comprehensive assistant for operations and utilities related to system enumeration, vulnerability identification, exploitation and privilege escalation

MIDA - Multitool

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG REPORT URL="http://bugs.kali.org/"
```

Installing MIDA

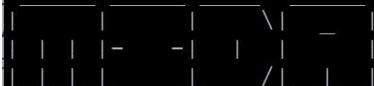
- Download GitHub repository

```
root@kali2017:~# git clone https://github.com/NullArray/MIDA-Multitool.git
Cloning into 'MIDA-Multitool'...
remote: Counting objects: 77, done.
remote: Total 77 (delta 0), reused 0 (delta 0), pack-reused 77
Unpacking objects: 100% (77/77), done.
```

Using MIDA

- Running mida.sh

```
root@kali2017:~# cd MIDA-Multitool/
root@kali2017:~/MIDA-Multitool# chmod +x mida.sh
root@kali2017:~/MIDA-Multitool# ./mida.sh
```



```
MIDA - Multitool

1) Usage           3) Common Utilities      5) Cleartext Credentials
2) System Enumeration 4) External Utilities 6) Quit

Please enter your choice: 
```

Using MIDA

- Mida.sh System enumeration

```
MIDA - Multitool

1) Usage          3) Common Utilities      5) Cleartext Credentials
2) System Enumeration 4) External Utilities 6) Quit
Please enter your choice: 2

|_ _ _ _|_|_|_|_\_|_|
|_|_|_|-|-|_|_|_|_
|_|_|_|_|_|_|_|_|_|

MIDA - Multitool

This module enumerates system information and appends it to a textfile.

These items will be enumerated:

1. User IDs login history & /etc/passwd.
2. OS details and mounted disks, kernel.
3. Network status and information.
4. Process info & cron jobs.
5. System logs.

Continue? Y/n : 3

Please provide a path to which the output will be saved. I.e /tmp/output.txt
Path to outfile : /tmp/Results
```

Using MIDA

- mida.sh System enumeration

```
Network status & info

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.10.12 netmask 255.255.255.0 broadcast 192.168.10.255
        inet6 fe80::20c:29ff:fc73:aaze prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:73:aaf:2e txqueuelen 1000  (Ethernet)
            RX packets 133931 bytes 1487956468 (141.9 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 76950 bytes 21316061 (20.3 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4098<BROADCAST,MULTICAST> mtu 1500
      ether 00:0c:29:73:aa:38 txqueuelen 1000  (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4098<BROADCAST,MULTICAST> mtu 1500
      ether 00:0c:29:73:aa:42 txqueuelen 1000  (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000  (Local Loopback)
          RX packets 31 bytes 2778 (2.7 KIB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 31 bytes 2778 (2.7 KIB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Address           HWtype   HWaddress           Flags Mask       Iface
192.168.10.21    ether    00:0c:29:a5:1c:b2  C          cth0
192.168.10.15    ether    48:51:b7:15:98:cf  C          eth0
_gateway         ether    1c:b1:7f:e1:4b:d4  C          eth0
```

Using MIDA

- mida.sh Common Utilities

```
1) Usage           3) Common Utilities      5) Cleartext Credentials
2) System Enumeration 4) External Utilities   6) Quit
Please enter your choice: 3
| [ ] | [ ] | [ ] \ | [ ] |
| [ ] | - | [ ] | [ ] | - | [ ]
| [ ] | [ ] | [ ] | / | [ ] |

MIDA - Multitool

Listing common, available utilities

/usr/bin/curl
/usr/bin/wget
/usr/bin/telnet
/bin/netcat
/usr/sbin/tcpdump
/usr/bin/nmap
/bin/mknod
/usr/bin/ssh
/usr/bin/python
/usr/bin/ruby
/usr/bin/perl
/usr/bin/gcc

Done. Would you like to list all utilities?

Continue? Y/n : █
```

References

- Kitploit

<http://www.kitploit.com/2017/10/mida-multitool-bash-script-purposed-for.html>

- Kali Linux

<https://www.kali.org/downloads/>

- GitHub

<https://github.com/NullArray/MIDA-Multitool>