Enhancing Network Security with FortiGate Firewalls

GROUP - 8
Presented by: Aryanth Reddy
Likith Salike
Ashish Reddy

Project Overview

- Aim: Design a scalable and secure network for head and branch offices.
- Tools: GNS3, FortiGate firewalls, and VLAN configuration.
- Focus: Ensure secure communication between offices via a site-to-site VPN.
- Approach: VLAN segmentation, firewall deployment, and intrusion prevention systems.
- Goal: Prevent unauthorized access while ensuring reliable data transmission.

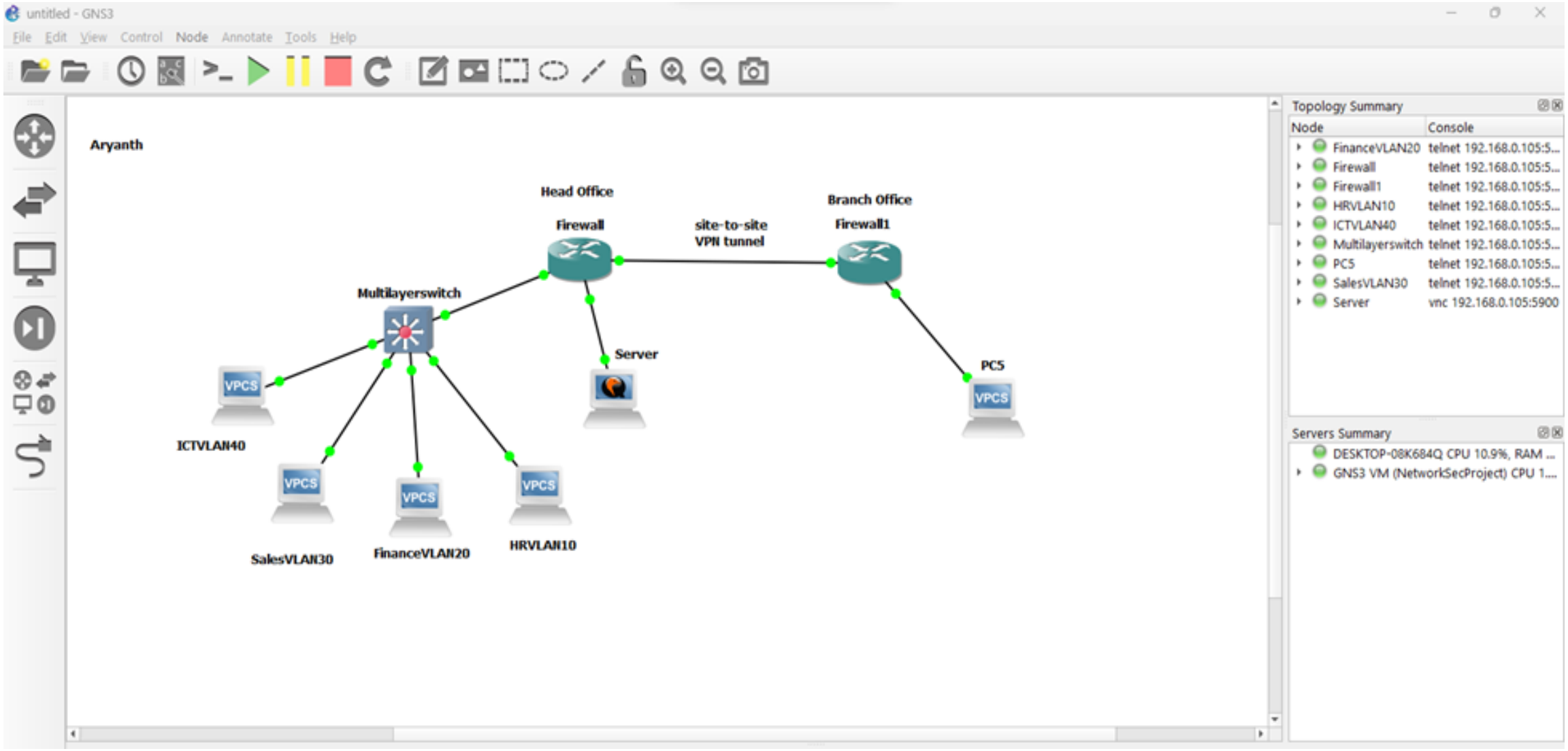
Virtual Lab Setup

- GNS3 was used to simulate the network environment.
- Included components: multilayer switch, virtual PCs, server, and firewalls.
- FortiGate firewalls governed perimeter security for both offices.
- Trunking and inter-VLAN routing configured in the switch.
- Connectivity tests validated the setup with tools like VNC Viewer and Telnet.

Network Design and Segmentation

- VLANs created for ICT, HR, Finance, and Sales (VLANs 40, 10, 20, 30).
- Each VLAN restricted to specific departmental traffic for security.
- DMZ set up for hosting public services like web servers.
- Site-to-site VPN established between head and branch offices.
- Design ensured scalability, efficiency, and secure data transmission.

Network Segmentation Layout



Firewall Deployment

- FortiGate firewall interfaces configured as WAN, LAN, and DMZ.
- WAN connected to the internet with a public IP address.
- LAN secured internal communications between VLANs.
- DMZ provided limited access to public-facing services (e.g., email, SSH).
- Policies restricted traffic to ensure only necessary services were allowed.

Firewall Interface Configuration

```
vendor-mac                      Show vendor and the MAC address they have.
vip                             Configure virtual IP for IPv4.
vip6                            Configure virtual IP for IPv6.
vipgrp                          Configure IPv4 virtual IP groups.
vipgrp6                         Configure IPv6 virtual IP groups.
wildcard-fqdn                   Configure wildcard FQDN.

FortiGate-VM64-KVM # config firewall

no object in the end
Command fail. Return code 1

FortiGate-VM64-KVM #
FortiGate-VM64-KVM #
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit "dmz"
new entry 'dmz' added

FortiGate-VM64-KVM (dmz) # set ip 192.168.2.1

incomplete command in the end
Command fail. Return code -160

FortiGate-VM64-KVM (dmz) # set ip 192.168.2.1
<class_ip&net_netmask>    IP address and subnet mask (syntax = 1.1.1.1/24).

FortiGate-VM64-KVM (dmz) # set ip 192.168.2.1/24

FortiGate-VM64-KVM (dmz) # set allowaccess ping https ssh

FortiGate-VM64-KVM (dmz) # set role dmz

FortiGate-VM64-KVM (dmz) # set interface "port2"

FortiGate-VM64-KVM (dmz) # next
Attribute 'vdom' MUST be set.
Command fail. Return code 1
```

Desktop 1

Setting Access Ports for VLAN

```
Multilayerswitch(config)#inter
Multilayerswitch(config)#interface e0/0
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport m
Multilayerswitch(config-if)#switchport mode acc
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport acc
Multilayerswitch(config-if)#switchport access vlan 40
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#interface e0/0
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#interface e1/0
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport mo
Multilayerswitch(config-if)#switchport mode ac
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#swi
Multilayerswitch(config-if)#switchport aacc
Multilayerswitch(config-if)#switchport a
Multilayerswitch(config-if)#switchport acc
Multilayerswitch(config-if)#switchport access vlan 30
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#
Multilayerswitch(config)#interface e0/1
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#switchport access vlan 20
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#interface e0/2
Multilayerswitch(config-if)#switchport mode access
Multilayerswitch(config-if)#switchport access vlan 10
Multilayerswitch(config-if)#exit
Multilayerswitch(config)#do wr
Building configuration...
Compressed configuration from 1567 bytes to 919 bytes[OK]
Multilayerswitch(config)#
```

VPN Configuration

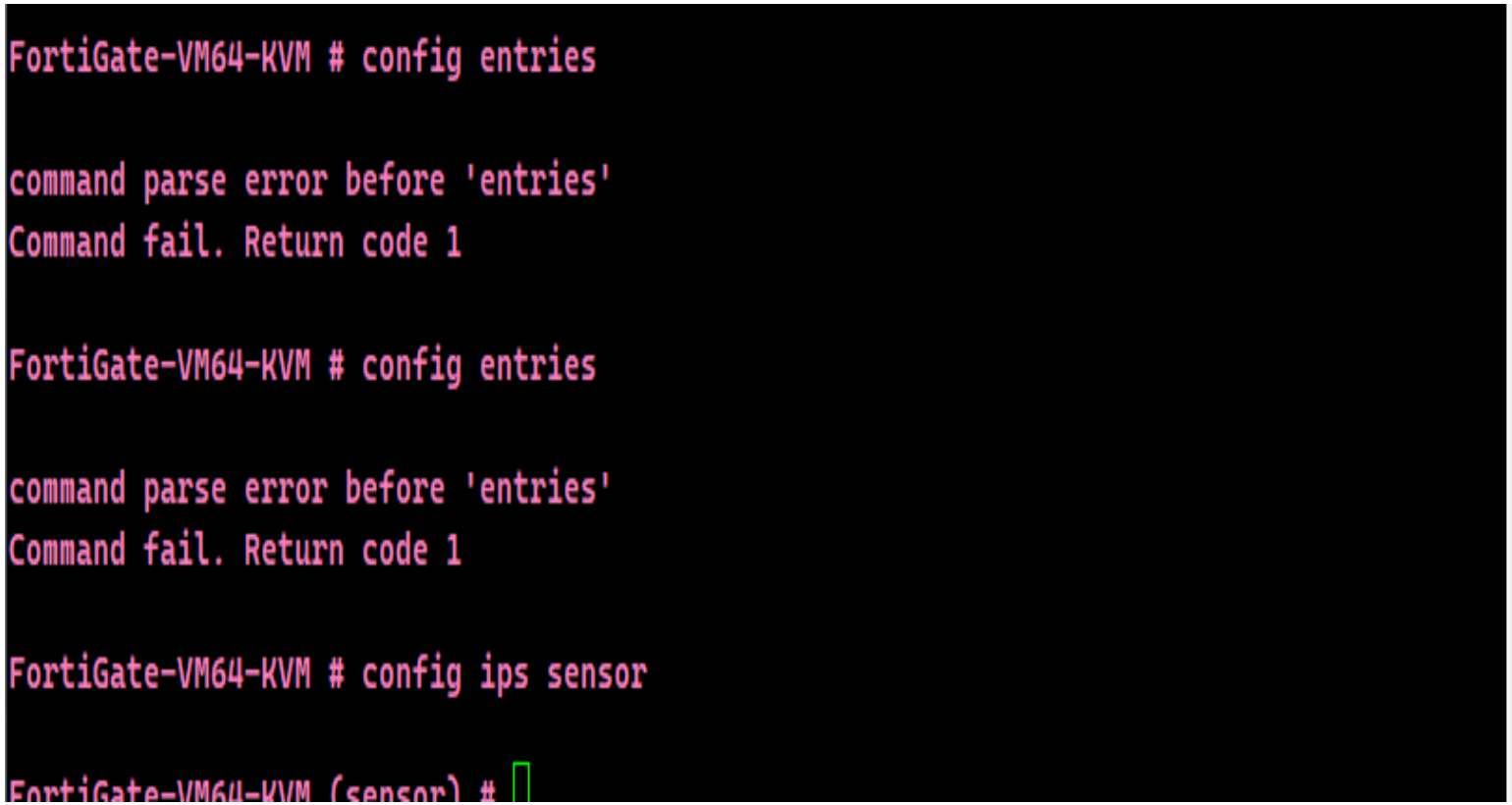
- Phase 1: WAN interface configured with pre-shared key and AES256-SHA256 encryption.
- Phase 2: Subnet traffic routes set for secure communication (192.168.1.0/24 and 10.0.0.0/24).
- Policies allowed two-way traffic between LAN and VPN tunnel.
- Connectivity tests confirmed secure transmission and tunnel status.
- The VPN ensured encrypted data sharing between remote sites.

Site-to-Site VPN Tunnel Status

Intrusion Detection and Prevention System (IDS/IPS)

- FortiGate IPS sensor monitored traffic for malicious activities.
- Known threats were blocked while all potential incidents were logged.
- Severity and scope set to cover 100% of traffic.
- IPS integrated into the WAN-DMZ traffic zone for proactive defense.
- Logs confirmed real-time intrusion detection and mitigation.

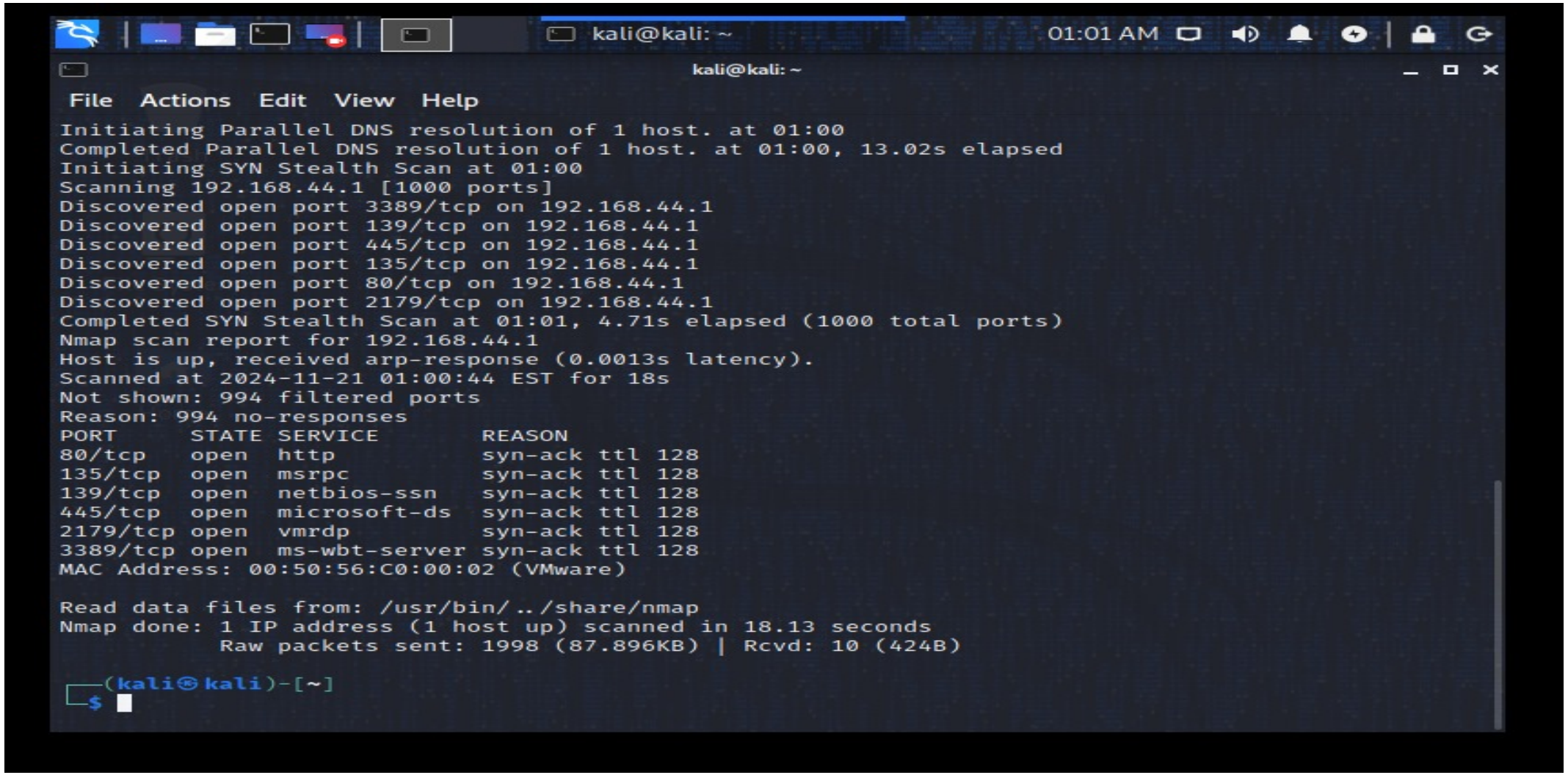
IPS Monitoring Logs



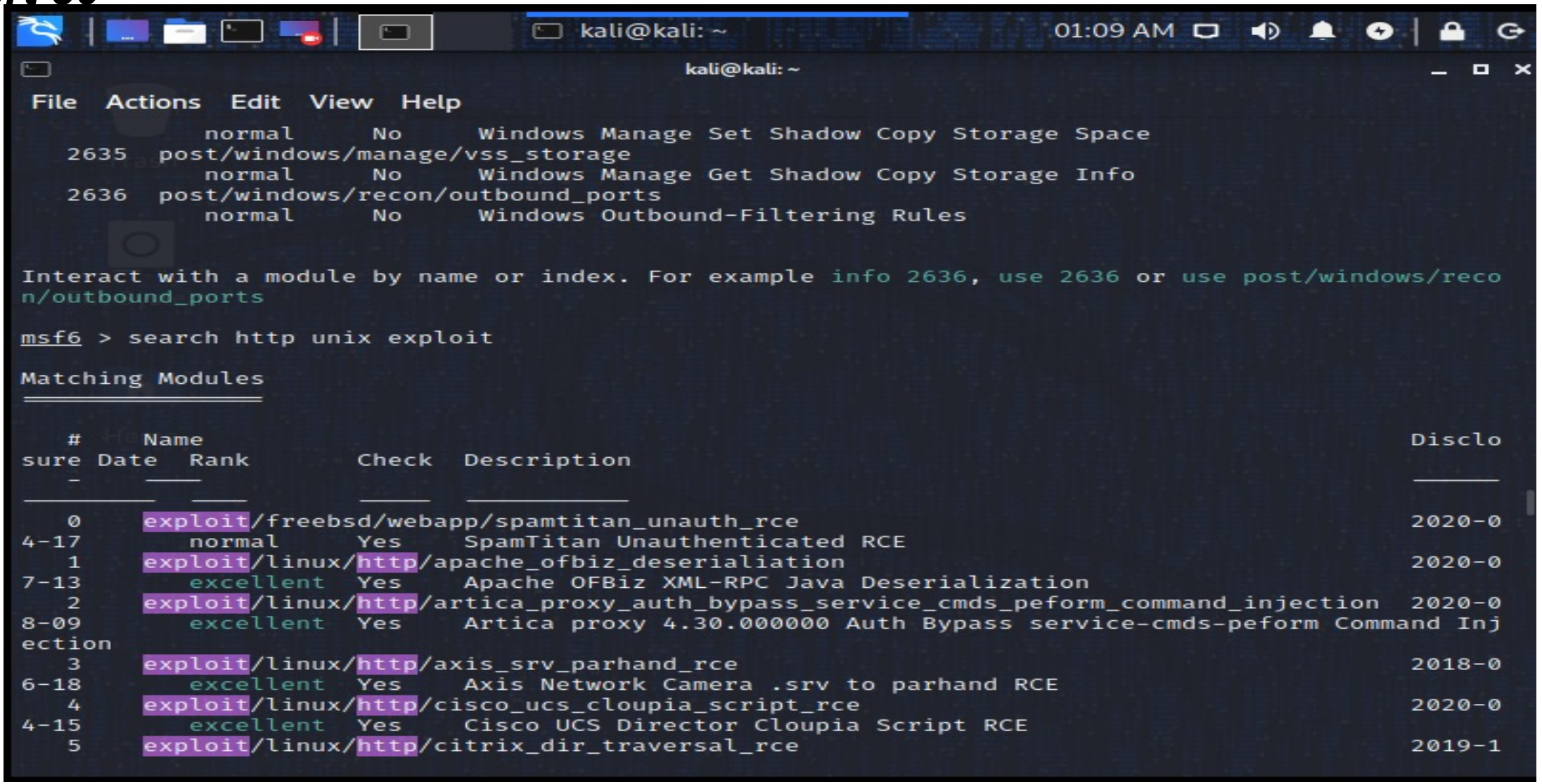
Vulnerability Testing and Exploitation

- Nmap scan revealed several open ports, including port 80 (HTTP).
- Metasploit framework was used to exploit the exposed HTTP port.
- The exploit failed, possibly due to detection by the Intrusion Prevention System (IPS) in the firewall.
- Testing highlights the need to optimize firewall policies for better security.

Nmap scan identifying open ports, including port 80 for HTTP



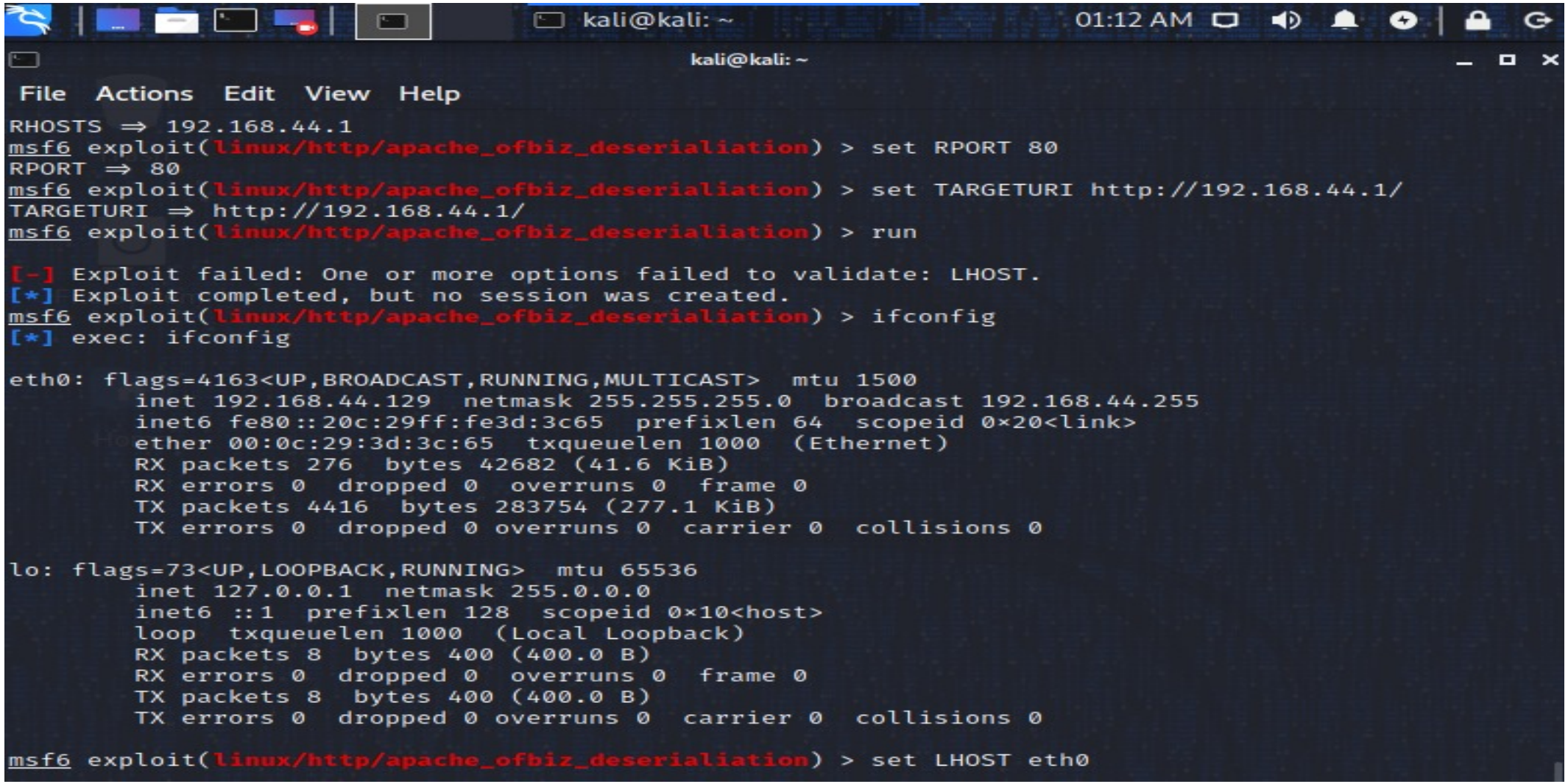
Metasploit framework used to search and configure HTTP exploits for port 80



Exploit Attempt and Outcome

- The Metasploit framework configured an exploit for the Apache OFBiz deserialization vulnerability.
- The exploit session failed due to SSL/TLS misconfiguration or firewall detection.
- Demonstrates the importance of secure configurations for exposed services.

Failed exploit due to SSL/TLS misconfiguration or IPS detection by the firewall

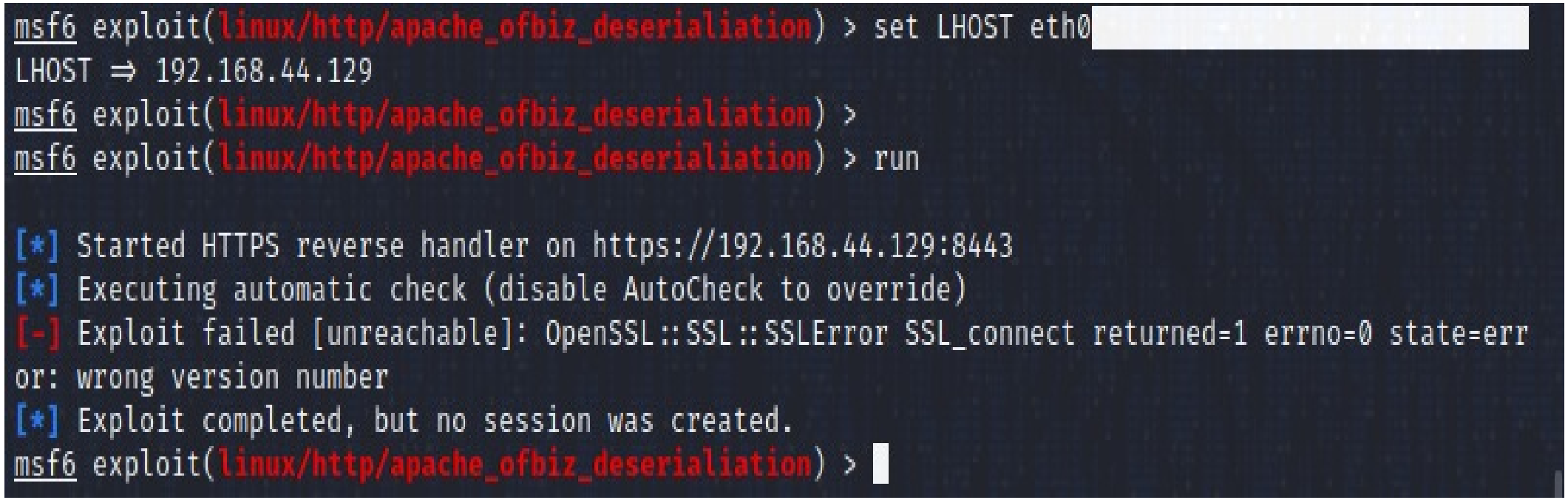


Risk and Remediation

- Risk: Exposing port 80 (HTTP) creates a high-security risk, labeled as a "security misconfiguration."
- Risk: Misconfigured or overly permissive firewall policies leave critical vulnerabilities.

- Remediation: Optimize firewall rules to close unused ports like port 80.
- Remediation: Deploy enhanced monitoring tools to detect and block malicious activity.

SSL error in Metasploit exploit run highlights configuration gaps



Conclusion

- Continuous monitoring and optimization of network security settings are necessary.
- Exposed ports such as port 80 represent a significant risk.
- Immediate action, such as policy/rule optimizations, is required to protect against potential exploitation.