COMP 012 - Network Administration

Windows + Linux + Packet Tracer + Python Automation

SESSION 8: NETWORK SECURITY AND ACLS

ACTIVITY 8.1: ACCESS CONTROL LISTS (ACLS)

Topic: Implementing ACLs for traffic filtering

Description: Configure ACLs on routers to control network traffic

INSTRUCTIONS:

In Packet Tracer, build network with 3 subnets:
• 192.168.10.0/24 - Employees
• 192.168.20.0/24 - Guests
• 192.168.30.0/24 - Servers
Standard ACL (filter by source only):
• Block Guests from accessing Servers
• access-list 10 deny 192.168.20.0 0.0.0.255
• access-list 10 permit any
• Apply: ip access-group 10 out (on server interface)
Extended ACL (source, dest, protocol, port):
• Allow Guests to access web server only (port 80,443)
• access-list 100 permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.10 eq 80
• access-list 100 permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.10 eq 443
• access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
• access-list 100 permit ip any any
Verify: show access-lists
Test all scenarios and document results

Deliverables: Submit .pkt file with ACLs and test documentation	**35 Points**

ACTIVITY 8.2: FIREWALL CONFIGURATION

Topic: Configuring Windows and Linux firewalls

Description: Implement host-based firewalls for server security

INSTRUCTIONS:

Windows Firewall:
• Open Windows Defender Firewall with Advanced Security
• Review default rules
• Create inbound rules:
  - Allow RDP (3389) from admin subnet only
  - Allow HTTP (80) from any
  - Allow HTTPS (443) from any

- Allow DNS (53) from local network
• Block all other inbound by default
• Export rules for documentation

Linux UFW (Uncomplicated Firewall):
• sudo apt install ufw
• sudo ufw default deny incoming
• sudo ufw default allow outgoing
• sudo ufw allow ssh
• sudo ufw allow http
• sudo ufw allow https
• sudo ufw allow from 192.168.1.0/24 to any port 22
• sudo ufw enable
• sudo ufw status verbose

Test firewall rules from another machine

Deliverables: Submit firewall configurations and test results	**30 Points**

ACTIVITY 8.3: SECURITY HARDENING

Topic: Implementing security best practices

Description: Apply security hardening to network devices and servers

INSTRUCTIONS:

Router/Switch hardening:
• Disable unused ports: shutdown
• Enable port security:
- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation shutdown
• Disable CDP on edge ports: no cdp enable
• Set exec-timeout on console/vty
• Enable logging: logging buffered

Windows Server hardening:
• Rename Administrator account
• Set account lockout policy (3 attempts)
• Enable audit policies
• Disable unnecessary services
• Configure Windows Update

Linux Server hardening:
• Disable root SSH login
• Use SSH key authentication
• Configure fail2ban
• Remove unnecessary packages

• Set proper file permissions
Create security audit checklist

Deliverables: Submit hardening configurations and security checklist	**35 Points**

TOTAL POINTS: 100