Cybersecurity Essentials

Module 6 & Module 7

Network Security Infrastructure and Windows Operating System Administration

Undergraduate Level — Washington Accord Aligned (Bloom C3 & C4)

Learning Outcomes

After studying this document, students will be able to:

- Explain how network security devices and services protect organizational networks.
- Apply access control, monitoring, and logging concepts to real network scenarios (Bloom C3).
- Analyze security incidents using network and operating system evidence (Bloom C4).
- Use Windows administrative tools safely for monitoring and investigation.

1 Module 6: Network Security Infrastructure

1.1 Security Devices

Network security devices form the backbone of enterprise protection. These devices enforce security policies, detect malicious activity, and limit attacker movement.

Firewalls

A firewall is a network security device that enforces an access control policy between two or more networks. It acts as a controlled transit point where traffic can be allowed, denied, or inspected.

Benefits of Firewalls

- Reduce exposure of internal systems to external threats
- Centralize access control policies
- Filter traffic based on IP addresses, ports, and protocols

Limitations

- Misconfiguration can create security gaps
- Performance bottlenecks may occur
- Attackers may tunnel malicious traffic inside allowed protocols

Firewall Architectures

Inside/Outside Architecture: Internal network is trusted, external network is untrusted. Outbound traffic is allowed and inspected; unsolicited inbound traffic is denied.

DMZ Architecture: A demilitarized zone separates public-facing servers (web, mail, DNS) from the internal network. Internet access to internal systems is tightly restricted.

Zone-Based Policy Firewall: Interfaces are grouped into zones. Traffic between zones is denied by default unless explicitly permitted.

IDS vs IPS

- **IDS (Intrusion Detection System)**: Monitors traffic and generates alerts.
- **IPS (Intrusion Prevention System)**: Monitors traffic and actively blocks malicious packets.

IPS devices must be carefully tuned, as false positives can disrupt legitimate traffic.

Analytical Case Study (C3 + C4)

Scenario: A university hosts a public web portal while maintaining a private student records database.

C3 (Apply): Design a secure placement of firewall, IDS, and IPS.

Solution:

- Place the web portal in a DMZ.
- Keep the database in the internal network with no direct internet access.
- Deploy IPS inline at the internet edge.
- Deploy IDS on a mirrored switch port to monitor internal traffic.

C4 (Analyze): Explain why placing the database directly in the DMZ is risky.

Solution: A compromised web server could directly access the database, leading to data breaches. Separating trust zones limits lateral movement and reduces impact.

1.2 Security Services

Security services provide visibility, control, and accountability beyond security devices.

Access Control Lists (ACLs)

An ACL is a list of rules that permit or deny traffic based on packet header fields.

Standard ACL: filters based on source IP only. **Extended ACL**: filters based on protocol, source, destination, and ports.

```
Standard IP access list 11
 10 deny 192.168.10.0 0.0.0.255
 20 permit any
```

Key Rule: ACLs must be applied to an interface and direction to take effect.

Monitoring Services

- **SNMP**: collects device statistics via managers and agents.
- **NetFlow**: analyzes traffic patterns and flows.
- **Port Mirroring (SPAN)**: copies traffic to monitoring tools.
- **Syslog**: centralizes log messages.
- **NTP**: synchronizes time for accurate event correlation.

AAA and VPN

AAA provides authentication, authorization, and accounting using RADIUS or TACACS+. VPNs create encrypted tunnels over public networks for secure communication.

Analytical Case (C4)

Scenario: Network logs from different devices show conflicting timestamps.

Analysis and Solution: The most likely cause is unsynchronized clocks. Implement NTP across all devices before reconstructing the incident timeline.

2 Module 7: Windows Operating System

2.1 Windows Architecture Essentials

Windows security relies on understanding its architecture.

File Systems

NTFS is the standard Windows file system due to:

- Support for large files and partitions
- Security permissions
- Reliability and recovery features

Alternate Data Streams (ADS)

NTFS supports alternate data streams, allowing hidden data to be attached to files: `file.txt:hidden`

Attackers may abuse ADS to hide malicious content.

Registry

The Windows Registry is a hierarchical configuration database. Key hives include:

- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_USER
- HKEY_USERS

Boot Process

The boot process (BIOS/UEFI) is a high-value attack target because malware here can persist across reboots.

2.2 Windows Administration Best Practices

Least Privilege: Users should operate as standard users and elevate privileges only when necessary.

Users and Groups: Permissions are assigned via groups; improper group membership can lead to data exposure.

Analytical Case (C4)

Scenario: A student account is temporarily made Administrator and not reverted.

Analysis and Solution: This violates least privilege. The safer approach is temporary elevation using authorized credentials or managed software deployment.

2.3 Windows Monitoring and Investigation Tools

PowerShell

PowerShell is a powerful administrative shell using verb-noun commands:

- `Get-Process`
- `Get-ChildItem`

Aliases exist for compatibility (e.g., `dir`).

Netstat and Process Correlation

```
netstat -abno
```

This command maps network connections to process IDs (PIDs), often requiring administrative privileges.

Task Manager

Task Manager allows:

- Viewing running processes
- Monitoring CPU, memory, disk, and network usage
- Ending suspicious processes

Analytical Case (C3 + C4)

Scenario: A Windows host shows outbound connections linked to `svchost.exe`.

C3 (Apply): Map PID using Task Manager and verify file path.

C4 (Analyze): `svchost.exe` hosts many services. Evidence such as non-standard file path, unsigned binaries, or unusual destinations indicates compromise.

Conclusion

This document integrates network and operating system security concepts with practical administrative workflows. By combining configuration knowledge with analytical reasoning, students gain skills aligned with real-world cybersecurity operations and Washington Accord learning standards.