CSCE 5585

Fall 2025

Gabriele Garulli

Clint Martinez

Bwalya Maele

COMPLIANCE AND RELATED ISSUES IN CYBERSECURITY Scripts and describing them elaborating on what those scripts do.

Compliance and Cybersecurity (specifically the NIST-style functions: Identify, Protect, Detect, Respond) and created a fantastic series of practical shell scripts using nmap that demonstrate the Monitoring and Detection capabilities.

1. Basic Network Discovery Script (network_discovery.sh)

Concept	Explanation
Purpose	To identify which hosts are currently active on the local network (**192.168.1.0/24**).
Script Command	**nmap -sn 192.168.1.0/24 -oN network_hosts.txt**
NIST Function	**Identify** (Asset Management) and **Monitor**
Expected Outcome	A list of IP addresses that respond to an ICMP/ARP request, confirming they are "up" and active on the network.
Compliance Value	**Asset Visibility/Inventory:** Compliance frameworks (like ISO 27001 or CIS controls) require a complete, up-to-date inventory of all network assets. This script provides the raw data to ensure only authorized devices are connected. A newly discovered, unauthorized host could indicate a policy violation or a compromised device.

2. Port Scan Detection Script (port_scan_detector.sh)

Concept	Explanation
Purpose	To perform a comprehensive, full connect (**-sT**) scan against a target to identify all open ports and determine the running service version (**-sV**).
Script Command	**nmap -p- -sT -sV --reason $TARGET_HOST -oN $OUTPUT_FILE**
NIST Function	**Detect** and **Protect**
Expected Outcome	A verbose report of every port (1-65535) that is open, along with the application name and version listening on that port.

CSCE 5585

Fall 2025

Gabriele Garulli

Clint Martinez

Bwalya Maele

COMPLIANCE AND RELATED ISSUES IN CYBERSECURITY Scripts and describing them elaborating on what those scripts do.

Compliance Value	**Vulnerability Management/Attack Surface Reduction**: This scan identifies the complete attack surface of a host. Compliance mandates that services exposed to the network must be minimized (Principle of Least Privilege/Attack Surface Reduction). Finding an unnecessary open port (FTP on a workstation) or an outdated version of a service is a critical compliance failure requiring remediation.

3. Ransomware Behavior Detection Script (ransomware_network_monitor.sh)

Concept	Explanation
Purpose	To specifically check for network indicators often associated with late-stage ransomware activity, focusing on command-and-control (C2) communication and lateral movement.
Script Command	**nmap -p 21,22,80,139,443,445,3389,8080,8443 -sS -Pn -v $TARGET_NETWORK** and filtering for ports **139/445/3389/8080/8443.**
NIST Function	**Detect**
Expected Outcome	A report highlighting any host on the network that has unusual or suspicious ports open, such as: **SMB (139/445)**: Often used by ransomware for lateral movement. **RDP (3389)**: A high-value target for initial compromise. **Uncommon Web Ports (8080/8443)**: Often used for C2 beacons.
Compliance Value	**Incident Detection**: This script acts as a proactive check for unauthorized service usage. Rapid detection of internal SMB/RDP scanning (i.e., a compromised host attempting lateral movement) is a key requirement for modern compliance standards focused on timely response.

4. Stealth Scan for Monitoring (stealth_monitor.sh)

Concept	Explanation

CSCE 5585

Fall 2025

Gabriele Garulli

Clint Martinez

Bwalya Maele

COMPLIANCE AND RELATED ISSUES IN CYBERSECURITY Scripts and describing them elaborating on what those scripts do.

Purpose	To run a "stealth" SYN scan (**-sS**) against a target to fingerprint the OS and services without completing the TCP handshake, making the scan less likely to be logged by basic firewalls or intrusion detection systems (IDS).
Script Command	**nmap -sS -Pn -A -O --host-timeout 5m $TARGET -oX $OUTPUT**
NIST Function	**Detect** (as a stealthy internal check) and **Identify** (OS & Service Fingerprinting)
Expected Outcome	A list of detected Operating Systems ("Windows Server 2019") and running services.
Compliance Value	**Configuration/Vulnerability Management**: Knowing the exact OS version is crucial. If the script identifies an out-of-support OS (Windows 7), this is an immediate, high-priority compliance violation due to unpatched security vulnerabilities. This also demonstrates internal audit effectiveness as the scan bypasses perimeter defenses.

5. Comprehensive Ransomware Network Scanner (comprehensive_ransomware_scanner.sh)

Phase	Description and Compliance/Mitigation Relevance
Phase 1: Host Discovery	**Action**: Uses **nmap -sn** to find all live machines. **Relevance**: Essential for **Identify**. Confirms the total scope of the network scan, ensuring no assets are missed in the security monitoring.
Phase 2: Port Scanning	**Action**: Scans a defined list of **ransomware-critical ports** (including common C2 and lateral movement ports). **Relevance**: Direct **Detection** capability. It proactively checks for active listeners on ports associated with ransomware communication (SMB/445, RDP/3389).

CSCE 5585

Fall 2025

Gabriele Garulli

Clint Martinez

Bwalya Maele

COMPLIANCE AND RELATED ISSUES IN CYBERSECURITY Scripts and describing them elaborating on what those scripts do.

Phase 3: Service Detection	**Action**: Intense service version scanning (**-sV --version-intensity 5**). **Relevance: Identify/Protect.** Finding active, vulnerable services like **smb**, telnet, or database servers (**mssql**, **mysql**) is vital. These are common targets for exploitation. This information leads to the Protect stage by prioritizing patch management and service disablement.
Phase 4: OS Detection	**Action**: Attempts to accurately determine the Operating System (-O). **Relevance: Identify/Protect**. An essential compliance requirement is ensuring all OSes are supported and patched. This phase flags end-of-life systems and confirms inventory accuracy.

Firewall and Switch Commands: Compliance and Protection

These commands directly address the Protect (Mitigation) component by tightening network security and ensuring high availability.

1. Firewall Commands: Geo-Blocking

These commands demonstrate a security control known as Geo-Fencing or Geo-Blocking.

Command Set	Explanation	Compliance/Mitigation Value
config firewall address edit "**non_us_countries**"	**Creates a single address object** that represents all	**Threat Reduction (Protect)**: This rule minimizes the attack

CSCE 5585

Fall 2025

Gabriele Garulli

Clint Martinez

Bwalya Maele

COMPLIANCE AND RELATED ISSUES IN CYBERSECURITY Scripts and describing them elaborating on what those scripts do.

	countries except the United States.	surface by reducing the number of external networks that can attempt to connect. If the company does no business with specific regions, blocking their IP ranges eliminates a source of many automated threats, thus aligning with the principle of "Deny by Default."
edit 100 set name "**Block-Non-US-Inbound**"	**Creates an inbound denial policy**. It blocks all connections originating from the **non_us_countries** object trying to reach the internal network (**lan**).	**Perimeter Defense (Protect)**: Prevents external attackers from high-risk regions from initiating connections into the corporate network. It is a proactive step in a Defense-in-Depth strategy.
edit 101 set name "**Block-Non-US-Outbound**"	**Creates an outbound denial policy**. It blocks internal users from initiating connections to the **non_us_countries** object.	**Preventing C2 & Data Exfiltration (Protect/Respond)**: This is critical for ransomware. If a machine is compromised, the ransomware often needs to "phone home" to a command-and-control server (often hosted overseas). This policy acts as a tripwire and block on suspected C2 traffic and data exfiltration.

2. Switch Commands: High Availability and Segmentation

CSCE 5585

Fall 2025

Gabriele Garulli

Clint Martinez

Bwalya Maele

COMPLIANCE AND RELATED ISSUES IN CYBERSECURITY Scripts and describing them elaborating on what those scripts do.

These commands address network resilience, availability, and internal compliance with segmentation policies.

Command Set	Explanation	Compliance/Mitigation Value
set type aggregate set member "**port1**" "**port2**"	**Creates a Link Aggregation Group (LAG)**, also known as a trunk or bonding, by combining two physical 1Gb interfaces (**port1** and **port2**) into one 2Gb logical pipe (**agg1**).	**High Availability & Resilience**: By bundling interfaces, the network gains redundancy. If one physical cable or port fails, traffic continues over the other link. This is a direct answer to the NIST Recover function. The "correct bandwidth" is maintained, preventing capacity issues
config system zone edit "**LAN**" set interface "**agg1**"	**Assigns the new aggregated trunk** to the LAN security zone.	**Security Policy Enforcement:** Ensures that traffic coming across the high-speed trunk is correctly subject to the security policies defined for the LAN (firewall policy, access control lists).
edit "**VLAN10**" set vlanid 10 set interface "**agg1**",	**Creates a Virtual Local Area Network (VLAN)**. It creates a logical network segment (VLAN 10) on the aggregated trunk.	**Network Segmentation (Protect)**: This is the single most critical modern security control. It segregates systems (separating user devices, servers, and IoT). If a user PC is infected with ransomware, the attacker cannot easily spread to the Server or Database VLANs, thus limiting the blast radius and aligning with major compliance requirements (like PCI-DSS or HIPAA requirements for network separation).