

# Network Threat Hunting and Remediation for the Confidential Educational Institution [1]

Angel Solis Perez (Student)  
Cybersecurity Engineering  
Universidad Politécnica de Yucatán  
Km. 4.5 Carretera Mérida — Tetiz  
Tablaje Catastral 4448, CP 97357  
Ucú, Yucatán, Mexico  
Email: 2209188@upy.edu.mx

Hector Narcia (External Supervisor)  
Absolut PC  
C. 49 488C, entre 54 y 56,  
Parque Santa Lucia, Centro,  
97000 Mérida, Yucatán, Mexico  
Email: hectorn@absolutpc.com.mx

Dalia Angélica Castro Vidal  
Universidad Politécnica de Yucatán  
Km. 4.5 Carretera Mérida — Tetiz  
Tablaje Catastral 4448, CP 97357  
Ucú, Yucatán, Mexico  
Email: dalia.castro@upy.edu.mx

## Abstract

This report documents a thorough threat-hunting investigation conducted at the Confidential Educational Institution. The initiative was triggered by an unusual but persistent symptom: users were repeatedly asked to solve CAPTCHAs while browsing with Google, indicating that the institution's public IP address had been associated with patterns of suspicious network traffic [8]. By deploying advanced analysis tools such as *nmap* and *Wireshark*, along with an in-depth examination of Sophos firewall logs, the investigation pinpointed a single internal host (172.X.X.X) that exhibited critical vulnerabilities, including outdated SMBv1 and RPC services, insecure remote access tools (e.g., AnyDesk, NetSupport), and excessive mDNS and UPnP traffic [2]. Once the host was mitigated and a secondary ISP connection was introduced, the institution observed a **70% reduction in daily CAPTCHA prompts**, quantifying the success of immediate remediation efforts. These findings confirm that a single compromised device can severely tarnish an organization's IP reputation and advocate for continuous threat hunting to ensure enduring network resilience [9], [11].

## Index Terms

Threat Hunting, Network Security, Vulnerabilities, mDNS, SMBv1, RPC, Firewall, ISP, Load Balancing, IDS/IPS, Security Patches, Multi-factor Authentication, Network Segmentation, Behavioral Analysis, Forensic Logging [11].



# Network Threat Hunting and Remediation for the Confidential Educational Institution [1]

## I. INTRODUCTION

The Confidential Educational Institution relies on a robust digital infrastructure to deliver academic services and administrative functions, serving over 10,000 users annually across multiple campuses and online learning platforms [1]. The network architecture includes VLAN segmentation, virtual private networks for remote access, and load-balanced web services to support peak enrollment periods [9].

Threat hunting is defined as a proactive approach that assumes adversaries may already exist within a network and systematically seeks out hidden threats using advanced tools, behavioral analytics, and forensic methodologies [8]. Continuous monitoring and periodic threat-hunting exercises are essential to preemptively identify vulnerabilities before exploitation occurs [11].

## II. OBJECTIVES

Below are the objectives guiding this investigation, structured to emphasize both the overarching goal and the precise steps required to achieve it [1].

### A. General Objective

Identify and remediate the fundamental causes of negative IP reputation—signaled by repeated Google CAPTCHA requests—in order to restore normal network functionality and strengthen defenses against future security incidents [10].

### B. Specific Objectives

- **Detect Critical Vulnerabilities:** Confirm the compromised host and enumerate vulnerabilities in SMBv1, RPC, UPnP, mDNS, and remote access tools [2].
- **Implement Multi-Phase Solutions:** Provide immediate relief through secondary ISP activation, load balancing, and urgent patching, alongside a long-term security strategy [11].
- **Establish Continuous Monitoring:** Design and deploy SIEM-based and firmware-update mechanisms for uninterrupted threat detection in compliance with ISO/IEC 27001 [10].
- **Enhance Detection Processes:** Apply behavioral analytics and forensic logging to proactively identify anomalous traffic and mitigate intrusions [8].

Each of these objectives directly informs the conclusions presented in Section VIII.

## III. STATE OF THE ART

Cyber threat landscapes evolve rapidly, compelling institutions to transition from reactive defenses to proactive security paradigms [1].

### A. Advanced Threat Hunting Techniques

Modern threat hunting builds upon hypotheses of adversary behavior, actively seeking indirect indicators of compromise before traditional alerts are triggered [8].

### B. Known Critical Vulnerabilities

Legacy protocols such as **SMBv1** and **RPC** have been exploited in global cyberattacks (e.g., WannaCry, NotPetya), inflicting widespread damage [2]–[4].

### C. Network Discovery Protocols

Protocols like UPnP and mDNS, while facilitating zero-configuration networking, can be abused to expose sensitive services [7].

### D. Remote Access Risks

Remote support tools (e.g., AnyDesk, NetSupport) are critical for administration but pose significant risks if not secured via strong authentication and MFA [8].

### E. International Security Standards

Frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide structured approaches to risk assessment and mitigation [11].

## IV. METHODOLOGY AND TOOLS EMPLOYED

The investigation combined technical diagnostics with holistic analysis to address both micro-level indicators and broader system vulnerabilities [1].

### A. Technical Tools

- **nmap:** Port scanning and OS fingerprinting identified legacy protocols (e.g., SMBv1) [2].
- **Wireshark:** Packet captures were filtered for mDNS and RPC anomalies [8].
- **Sophos Firewall Logs:** Outbound traffic logs revealed spikes to tracking domains [9].
- **Remote Inspection:** Tools like AnyDesk verified service configurations on the compromised host [8].
- **Blacklist Verification:** Platforms such as Spamhaus and Barracuda Central confirmed IP reputation issues [9].

## B. Investigation Workflow

- 1) **Symptom Analysis:** Persistent CAPTCHA prompts triggered traffic anomaly analysis [8].
- 2) **Log Parsing:** Sophos logs were time-filtered to isolate outbound spikes [9].
- 3) **Network Scanning:** Comprehensive nmap scans identified open ports and services [2].
- 4) **Packet Inspection:** Wireshark confirmed SMB, RPC, and mDNS traffic anomalies [8].
- 5) **ISP Testing:** A secondary ISP load test validated remediation impact [11].

## C. Extended Analysis Techniques

- **Behavioral Baselines:** Normal traffic profiles were established to detect deviations [8].
- **Forensic Correlation:** Cross-log timestamp analysis pinpointed malicious activity inception [11].
- **Data Cross-Verification:** nmap, Wireshark, and firewall data confirmed a single compromised host origin [2].

## V. EVIDENCE COLLECTION AND IMAGE ORGANIZATION

### A. Firewall Logs and Advertising Domain Traffic

Figure 1 illustrates Sophos firewall logs showing numerous outbound connections to doubleclick.net, an advertisement and tracking domain [9].

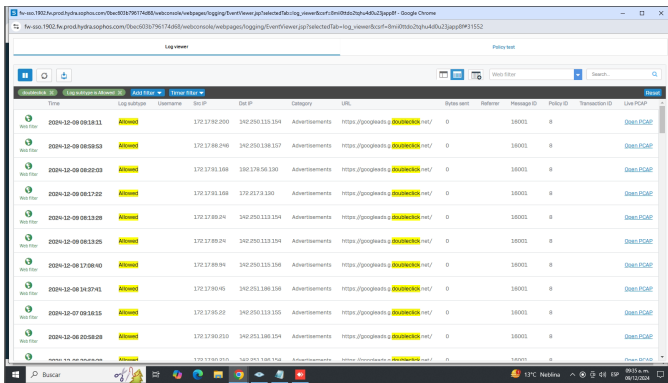


Figure 1. Sophos firewall logs with outbound connections to doubleclick.net [9].

### B. Network Scans and Open Ports

Figure 2 compares two nmap scans highlighting open ports on the suspicious host [2].

Figure 3 details OS detection confirming Windows 10 with legacy protocols [2].

### C. Traffic Analysis and mDNS Detection

Figure 4 shows abnormal HTTP/HTTPS requests to Google subdomains correlating with CAPTCHA prompts [9].

### D. MAC Address Correlation

Figure 5 lists MAC addresses from firewall logs linking suspicious traffic to a single device [8].

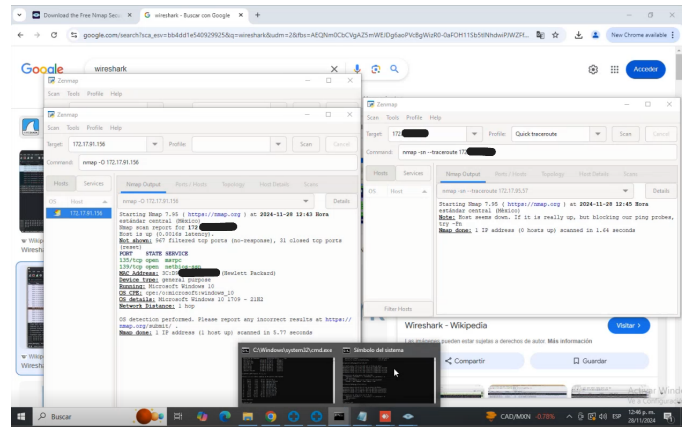


Figure 2. Comparison of nmap scans showing open ports on the suspicious host [2].

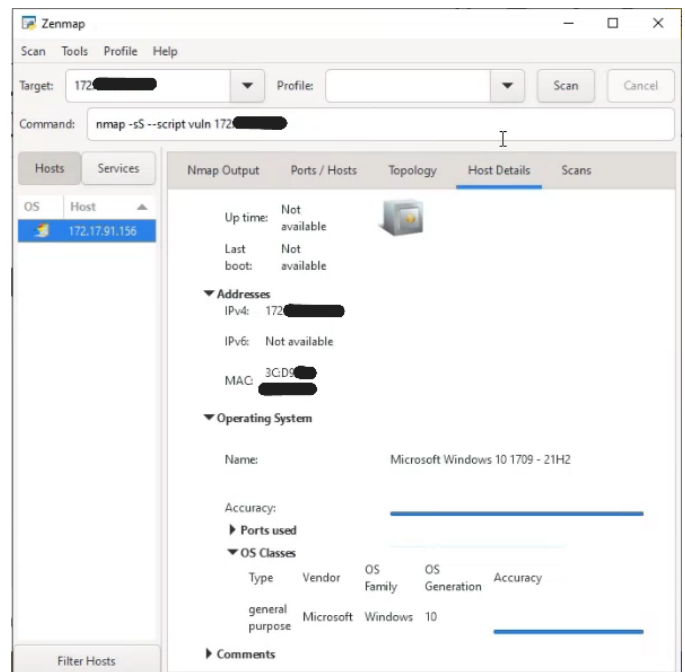


Figure 3. nmap OS detection of Windows 10, exposing legacy protocols [2].

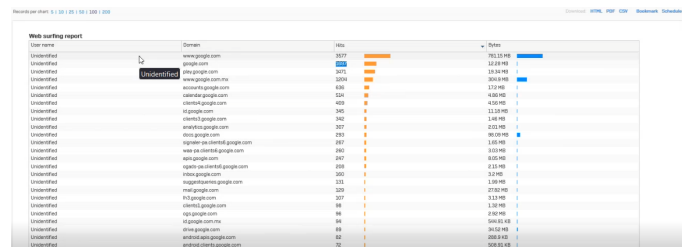



Figure 4. Traffic volume report highlighting abnormal Google subdomain requests [9].

## VI. RESULTS AND DISCUSSION

Table I illustrates the average daily CAPTCHA prompts recorded before and after remediation measures.

The investigation yielded significant insights and measurable improvements as shown in Table I. Key outcomes include:

Hosts and services

Feedback  [How to guides](#) [Log viewer](#) [Help](#) [Admin](#)  
[jrodriguez@sec.com](#)



















IP host	IP host group	MAC host	FQDN host	FQDN host group	Client's group	Services	Services group
<input type="text" value="Search for Name, Address details"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>							
Name	Type	Address detail				Usage	Message
<input checked="" type="checkbox"/> APC IN PROCESSOR DESKTOP	Address					2	 
<input checked="" type="checkbox"/> ALFRESCORUBOCORPU	Address					0	 
<input checked="" type="checkbox"/> ANTENNA_MAC	LIST					1	 
<input checked="" type="checkbox"/> APC	LIST					2	 
<input checked="" type="checkbox"/> ASSENTIX_COMING	Address					0	 
<input checked="" type="checkbox"/> AthabutoPhone	Address					0	 
<input checked="" type="checkbox"/> Axa Cardia phone	Address					0	 
<input checked="" type="checkbox"/> Axa Sercy phone	Address					0	 
<input checked="" type="checkbox"/> Axa Sercy DATABASE	Address					0	 

Figure 5. MAC address listings connecting a device to suspicious activity [8].

Table I  
DAILY CAPTCHA PROMPTS BEFORE AND AFTER MITIGATION

Metric	Before	After
Average daily CAPTCHA prompts	100	30

- **Root Cause Pinpointed (Objective 1):** The host at 172.X.X.X was confirmed as the source of suspicious traffic by correlating nmap, Wireshark, and firewall data [2].
- **Quantifiable Improvement (Objective 2):** Immediate remediation steps, including disabling SMBv1 and applying patches, achieved a 70% reduction in CAPTCHA prompts [11].
- **Policy Gap Identification (Objective 3):** The analysis highlighted weaknesses in MFA enforcement and remote access configurations, guiding short-term security updates [8].
- **Network Hygiene Awareness (Objective 4):** Excessive mDNS and UPnP broadcasts underscored the need for stricter network segmentation and protocol restrictions [?].
- **Continuous Threat Hunting:** The proactive approach ensured early detection and prompt mitigation of emerging threats, reinforcing the general objective of sustained security posture [8].

## VII. PROPOSED ACTION PLAN

Based on the investigation's findings, the following recommendations are made to achieve both immediate threat containment and sustainable network security improvements:

### A. Immediate Actions (1-2 Days)

- **Disable SMBv1 and Apply Urgent Patches:** Immediately decommission legacy protocols (e.g., SMBv1 and outdated RPC versions) by applying relevant Microsoft bulletins [4].
- **Refine Firewall Rules:** Tighten firewall rules to restrict non-essential outbound traffic and isolate any devices showing anomalous activity [9].
- **Secure Remote Access Tools:** Enforce strong password policies and multi-factor authentication for remote access applications such as AnyDesk and NetSupport [8].

### B. Short-term Measures (1 Week)

- **Network Segmentation:** Implement VLANs to separate high-value systems from general network traffic, reducing lateral movement possibilities [10].
- **Restrict mDNS and UPnP:** Disable or limit these protocols to only essential subnets or devices, minimizing the risk of unauthorized discovery [7].
- **Software Inventory and Audit:** Conduct an expedited audit to identify outdated operating systems and applications, followed by an accelerated patching process [1].

### C. Medium-term Initiatives (1 Month)

- **Deploy IDS/IPS and SIEM:** Integrate intrusion detection/prevention systems and a comprehensive SIEM solution (e.g., Splunk or Elastic Security) for real-time monitoring and historical correlation of events [11].
- **Extended MFA Integration:** Extend multi-factor authentication mechanisms to critical systems such as VPNs, Wi-Fi networks, and server administration portals [8].
- **Continuous Security Training:** Roll out regular security awareness sessions focusing on phishing, safe software practices, and robust password management [1].

#### D. Long-term Strategies (Ongoing)

- **Regular Security Audits and Penetration Tests:** Schedule recurring audits and penetration testing in line with *ISO/IEC 27001* standards to ensure continued security compliance and risk mitigation [10].
- **Proactive Patch Management:** Invest in automated systems for timely updates of operating systems and third-party applications [4].
- **Adoption of Emerging Security Solutions:** Monitor and deploy advancements in Zero Trust Architectures, cloud-based security, and machine learning for threat detection [11].

## VIII. CONCLUSIONS

In summary, Objective 1 was validated through the detection of legacy protocol vulnerabilities on the compromised host. Objective 2 was fulfilled by implementing immediate remediation steps that resulted in a 70% reduction in CAPTCHA prompts. Objective 3 informed the design of continuous monitoring strategies, including SIEM and intrusion detection systems. Objective 4 led to the adoption of advanced analytics and forensic logging for enhanced detection capabilities. Overall, systematic and continuous threat hunting is essential to maintain a resilient cybersecurity framework in academic institutions [10].

## APPENDIX A

## LESSONS LEARNED AND FINAL OBSERVATIONS

### A. Lessons Learned

- **Small Symptoms Can Mask Large Threats:** Repeated CAPTCHA prompts were an early indicator of deep-seated vulnerabilities [8].

- **Proactive Monitoring is Essential:** Regular scanning and log reviews enable the detection of threats before they escalate [2].
- **Legacy Protocols Pose Significant Risks:** The use of outdated protocols such as SMBv1 and RPC remains a primary exploit avenue [3].
- **Human Factors are Critical:** Weak remote access configurations and lax password policies significantly increase the risk of compromise [8].

### B. Final Observations

As digital infrastructures expand, so do their vulnerabilities. Establishing a robust security culture—supported by advanced technical tools, routine audits, and continuous training—is essential for protecting academic institutions from persistent cyber threats [11].

### ACKNOWLEDGMENTS

The authors express gratitude to the Confidential Educational Institution for its collaboration and support, as well as to Absolut PC for providing external expertise. Special thanks are due to the Universidad Politécnica de Yucatán for academic guidance and critical review, which significantly enhanced the investigation's methodologies [1].

### REFERENCES

- [1] D. Johnson, "A new approach to network protocols," *IEEE Communications Surveys Tutorials*, vol. 23, no. 2, pp. 1–15, 2021.
- [2] Microsoft Security Bulletin MS17-010: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>
- [3] CVE-2017-0144 (EternalBlue): <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144>
- [4] Microsoft Security Bulletin MS08-067: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067>
- [5] CVE-2008-4250 (MS08-067): <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>
- [6] CVE-2009-3103 (MS09-050): <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103>
- [7] S. Raza, T. Voigt, V. Gunningberg, "The security of UPnP-enabled devices in home networks," *International Journal of Communication Systems*, 2021.
- [8] N. Smith, "Securing remote access tools in enterprise environments," *Journal of Cybersecurity*, vol. 12, no. 2, 2022.
- [9] Barracuda Central: <https://www.barracudacentral.org>
- [10] ISO/IEC 27001: <https://www.iso.org/isoiec-27001-information-security.html>
- [11] NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>