NIDS in Airgapped LANs–Does it Matter?

Winston Messer
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, SD

Part 1: Definitions

Network Intrusion Detection System (NIDS)

- Makes use of a monitor or tap to “sniff” packets as they traverse the network.
- Often thought of as a boundary defense technology.
- Raises alerts in response to signatures.
- Signatures often created to mirror recent Indicators Of Compromise (IOCs).

Airgapped Networks

- An “Air-Gap” is a separation of the network from other networks, especially the public Internet.
- Commonly employed for sensitive networks such as industrial control networks or government networks.
- Commonly lack router, firewall, and NIDS due to no obvious place to position them.

Part 2: Should NIDS be Deployed on Airgapped LANs?

Pros and Cons of Deploying NIDS in an Airgapped Environment

Cons:

- Cost.
- Complexity.
- Is it *really* necessary to deploy a *network intrusion detection* system if we are not concerned about intrusion *into the network*?

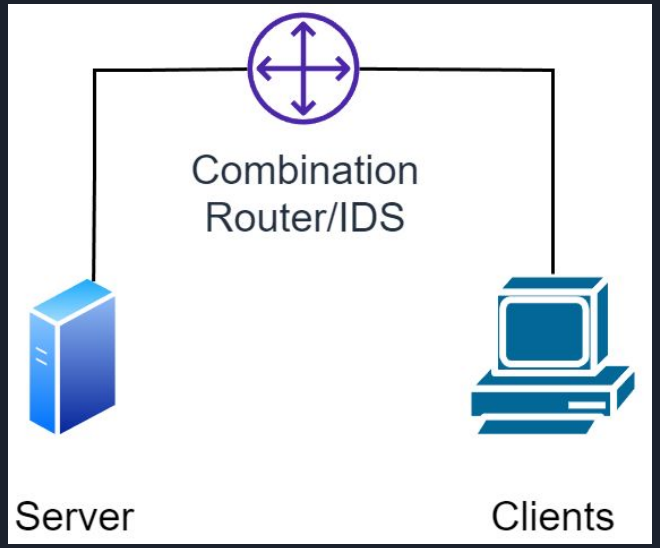
Pros:

- Threat intelligence groups distribute IOCs that get turned into signatures for NIDS.
- By ignoring NIDS, the network misses the benefits of the intelligence.
- Threats can still come from inside the network.

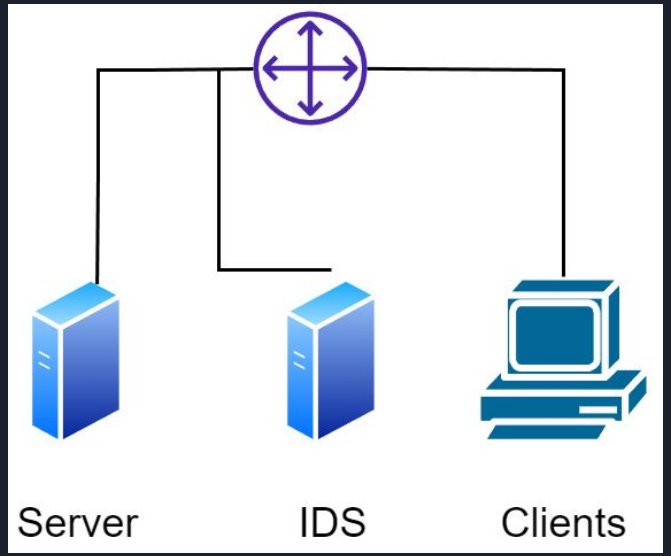
Addressing Cons: Financial Considerations

- NGFW can be purchased for $1,000 or less.
- Software NIDS can run on existing commodity HW or on a typical server or desktop costing $1,000 or less.
- Cost is not insignificant but represents a small part of total security program cost.

Addressing Cons: Complexity and Possible Network Designs

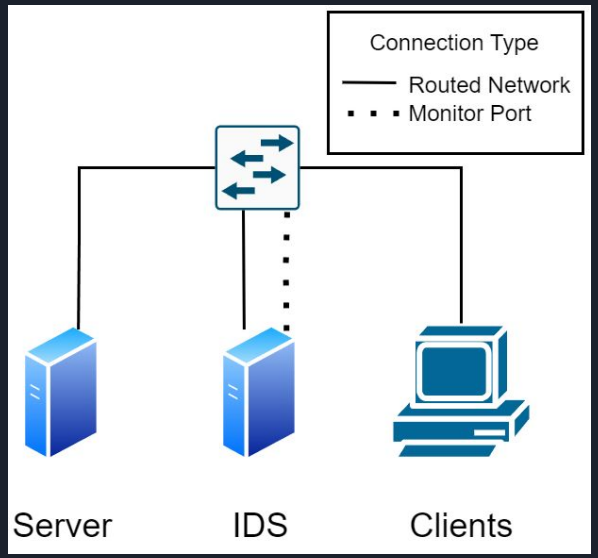


- IDS on Combination Router/IDS

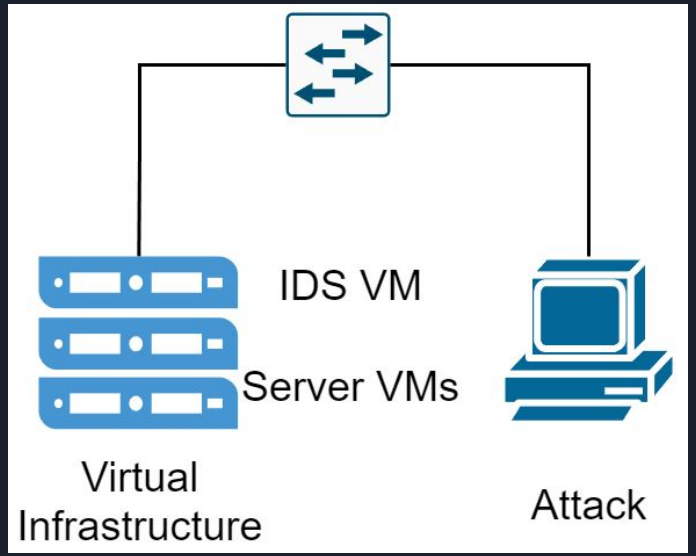


- IDS on Subset of VLANs in Routed Network

Addressing Cons: Complexity and Possible Network Designs



- IDS Monitor Port



- IDS on Virtual Infrastructure

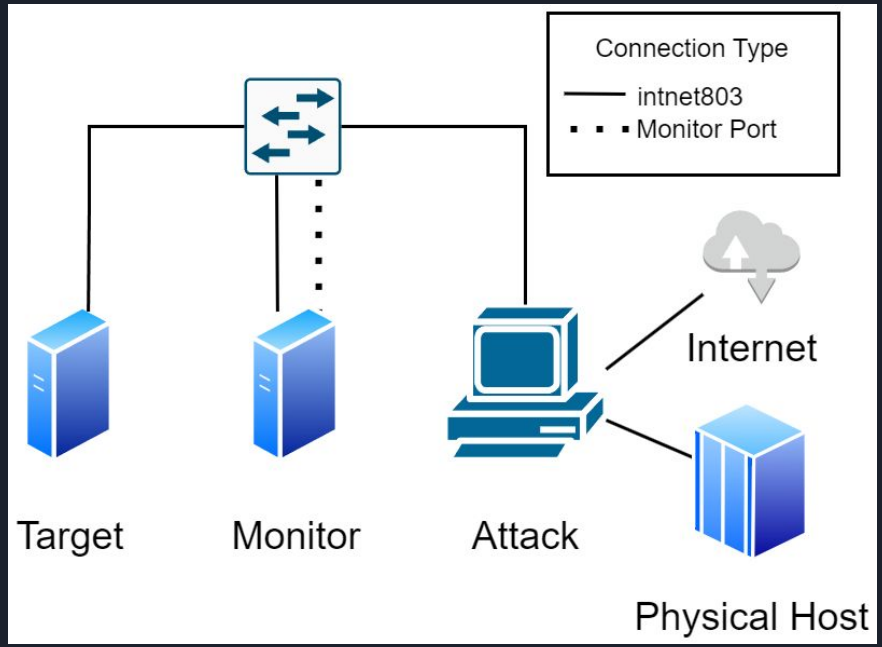
Part 3: Let’s Test It!

Let’s Test It!

- An experiment was run by attacking a virtual network with and without NIDS.
- A virtual network was constructed to support experimentation consisting of:
  - “Monitor” System: Security Onion, an integrated NIDS solution.
  - “Target” System: OWASP BWA, a deliberately vulnerable server.
  - “Attack” System: Kali Linux, a penetration testing distribution.
  - All systems set on a virtual bus network.

Virtual Test LAN

- Designed to simulate a small LAN with the addition of NIDS.
- All operating systems were open source software available at zero cost.
- Internet connectivity was disabled to simulate air-gap once setup was completed.



Experimental Process

- OWASP Bricks, a subset of OWASP BWA was attacked on “Target” from “Attack” while NIDS intercepted traffic on “Monitor.”
- Attacks consisted of:
  - 1 Active reconnaissance scan
  - 5 Login bypass attacks
  - 3 Malicious software upload attacks
  - 6 Malicious code injection attacks
- All attacks were executed using OWASP ZAP, a free penetration testing tool that is pre-installed in Kali Linux.

Experimental Process

- All attacks were executed successfully following a third-party guide.
  - (See references in paper or link at the end of slides for guide).
- Results of a host-based-only incident response investigation were captured.
- Results of a host-based-plus-NIDS incident response investigation were captured.

Part 4: Results

NIDS Detection Alerts vs. Vuln. Scan

Count	Severity	Rule Name
2,252	High	ET POLICY Http Client Body contains passwd= in cleartext
260	Medium	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)
21	Medium	GPL WEB_SERVER 403 Forbidden
21	Medium	GPL WEB_SERVER .htaccess access
16	High	ET WEB_SERVER CRLF Injection - Newline Characters in URL
14	High	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
10	High	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
4	High	ET WEB_SERVER PHP Possible https Local File Inclusion Attempt
1	High	ET DELETED Redkit Java Exploit request to .class file

Host-Based Detection of Vuln. Scan

- Host-Based Alerts:
  - Mod Security Alerted 21 times.
- Host-Based Forensics:
  - Evidence of the scan was found in Apache access and error log and in MySQL log.

Detection of Login Bypass (5 Attacks)

NIDS Results:

- Security Onion's NIDS alerted in all five test cases.
- However, NIDS alerts were specific to a vulnerability in the page and not to the attack itself.
- The alert did include the full text of the attack and sufficient information to discover and attribute it, however.

Host-Based Results:

- No security alerts were raised.
- Two non-critical errors were reported.

Detection of Malicious Code Uploads (3 Attacks)

NIDS Results:

- In each test case, NIDS alerted: “ET WEB_SERVER SQLi - SELECT and sysobject.”
- Additional alerts were raised when logging into the malicious site content.

Host-Based Results:

- In the first test case, no alerts were raised.
- Mod Security raised security alerts in the second and third test case relating to mismatched MIME types of the uploaded content.

Detection of Injection on Site Content (6 Attacks)

NIDS Results:

- Several high-severity alerts were raised by NIDS for the first two test cases.
- In the fifth test case, NIDS raised an alert about a vulnerability on the page but not specifically to the attack itself, although the content of the attack was included in the alert.

Host-Based Results:

- No alerts were raised in any of the six test cases.
- Requests for sensitive files from disk were successfully obfuscated in log files.

Summary of Alert Results

NIDS Results:

- NIDS alerted in 80% of cases. All alerts included evidence of the attack.
- NIDS raised a specific alert that an attack was in progress in 40% of test cases.

Host-Based Results:

- Host-based measures raised an alert in 20% of cases.

Summary of Non-Alert Results

NIDS-based logging for forensics:

- In 80% of cases NIDS alone was sufficient for proving attack and attributing it to attacking machine.

Host-based logging for forensics:

- In 100% of cases host-based logging was sufficient for proving attack and attributing it to attacking machine.

Discussion

- Adding NIDS **doubled** the likelihood of attack-specific alerts being produced.
- Adding NIDS **quadrupled** the likelihood of a security alert with the attack payload in the alert text.
- NIDS also detected vulnerable pages during normal access which could allow an analyst to report and remediate issues before an attack.
- Host-based log files remained the gold standard for incident response once a intrusion was detected by any method.
    - In 100% of cases host-based logs had sufficient evidence to attribute the attack vs 80% for NIDS-only.

Conclusion

- Addition of NIDS is supported by experimental results.
- For a relatively small investment, NIDS can increase incident detection and response capability on LANs.
- NIDS should be run in addition to recording log files.

Questions?

Links to Software and Walkthrough

- Security Onion: https://securityonionsolutions.com/
- OWASP BWA: https://owasp.org/www-project-broken-web-applications/
- Kali Linux: https://www.kali.org/
- Virtualbox: https://www.virtualbox.org/
- Walkthrough of OWASP Bricks: https://pentester.land/blog/owasp-broken-web-apps-owasp-bricks-challenge-walkthrough/

NIDS in Airgapped LANs–Does it Matter?

Winston Messer
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, SD