Network Perimeter Defense

Testing and Verification

August 2014

EnergySec
8440 SE Sunnybrook Blvd., Suite 206
Clackamas, OR 97015
877-267-4732
energysec.org

Executive Summary

It is important to test and verify that your network perimeter is securely configured. The purpose of this paper is to give a general overview of the kinds of tests that should be performed. There are two basic types of evaluations we will consider. The first is passive verification. This involves looking at the configurations of perimeter security devices, specifically firewalls, and ensuring that they are configured appropriately. The Ponemon Institute reports that a majority of next-generation firewalls are used only for reporting and monitoring,[1] which means that people are not using the tools they have to their full capabilities. The second type of tests we will examine are active tests. These allow you to verify that the devices and configurations you are using are behaving the way they are designed to. It is important to note, however, that the testing described in this paper is not the same as an actual, Red Team penetration test.

By having a robust testing and validation system, you are more likely to be able to use the tools you have effectively.

By having a robust testing and validation system, you are more likely to be using the tools you have effectively. For example, effective testing and validation will help to prevent your security operations from being negatively affected due to a high number of false positive alerts.

Audit Firewall Rule Sets

An entire paper could easily be written on how to audit firewall rule sets. Many of the concepts of a rule set audit, however, can be boiled down to a few general ideas. The first is that the firewall should have a "cleanup" rule, or an explicit "deny any" rule. Even if the firewall has an implicit deny rule, having the explicit rule will allow logging to happen, which is beneficial for troubleshooting as well as incident response.

Every firewall should have an explicit "deny any" rule.

You should also check for rules that have no effect. You can check the hit count for the rules, and any which have a zero hit count need to be investigated further. The rule could be entered in the wrong order, or it could be redundant to another rule. Having unused rules in the rule set can degrade the performance of the firewall, as well as cause security holes if it is a rule that should be in place but is not being applied due to a misconfiguration.

The last general thing to look for while auditing a firewall rule set is for the use of rules which include "any." This includes communication between two hosts that allow any service, or rules with a source or destination address of "any." While an edge router may have a reason to allow connections to "any" destination to allow Internet use, these rules should raise a red flag, especially on internal firewalls. If the purpose of a firewall is to segment the network, then allowing "any" traffic to pass through it defeats that purpose.

It is important to note, also, that commercial tools are available which will audit rule sets. Some of the major vendors of these tools are RedSeal,[2] NetAPT,[3] and Firemon.[4] This type of software, automating the process and allowing rule sets to be continuously audited, can help ensure that firewall rules are constantly being monitored, and audits are not just a one-time occurrence.

Perform Active Tests

Performing active tests needs to be done with care, so that operations are not negatively impacted.

In order to ensure that your security program is performing how as designed, it is important to perform tests of that security. There are several things you can do to test your perimeter defenses. In all of these tests, you will want to record how long it takes from the time the test was performed until the security or Information Technology (IT) department responded to the test. These kinds of active tests, including a manual review of the alerts and logs to ensure they are generating appropriate alerts, are useful for ensuring your alert system is operating as expected. Also, NERC CIP-010-1 v5 Requirement 3.2 requires high-impact Bulk Electric System Cyber Systems (BCS) to have an active vulnerability assessment performed at least every 36 months.[5]

Install a Rogue Access Point

Install an access point onto your network at a random location. Your monitoring system should be able to detect the rogue access point and raise an alert that it has joined the network. Additionally, alerts should continue at regular intervals until the rogue access point is disconnected from the network.

Test Egress Filtering

Send unauthorized packets from a trusted network to an untrusted network. You want to check that the unauthorized communications do not get past the firewall. If you have a next-generation firewall, then you could send information which contains fake personally identifiable information, and ensure that the firewall detects the attempt at exfiltrating data. These tests can be done using both encrypted and unencrypted data, to test whether data loss prevention systems are working effectively.

Test Network Boundaries

Send a packet from an untrusted network to a trusted network. Ensure that the packet is blocked and logged appropriately.

Test Malware Detection

Send a test program which appears to be malware, such as an EICAR file,[6] and ensure that it is blocked appropriately. Check that an alert is raised by your security system which includes details about the

attempt to spread malware, such as the source and destination addresses involved. If possible without jeopardizing the operations of your network, verify that the file is blocked by attempting to open or execute the file.

Open a Persistent Connection

Simulate a connection with a Command & Control server by opening a network connection between an internal and external address, and attempt to keep it open for at least 10 hours. Ensure that an alert is raised about the long-lasting connection.

"Red Team" Testing

"Red Team" testing must only be done by an experienced professional. It's not "something cool to try out."

Performing "Red Team" testing is beyond the scope of this paper. The basic premise of a Red Team exercise is to simulate a real-world attack, and to use the simulated attack in order to improve your defenses. There are some important things to keep in mind about performing a Red Team test, however. First of all, care needs to be taken so that the penetration test does not disrupt the operations of the network. There was a gas utility which performed a penetration test, and when the testers "wandered" into the SCADA network, they caused a disruption which kept gas from flowing in the pipeline for four hours. This caused a disruption of service to their customers.[7] Even something as simple as a ping sweep, common in conducting a penetration test against an IT system, can be enough to cause problems on a SCADA system. If you do decide to perform a penetration test, it is important to ensure that the operations team knows it is happening, and to use an expert with experience in conducting Red Team exercises against SCADA networks before you attempt the simulated attack.

Conclusion

There are a variety of ways to perform testing or verification of your perimeter defenses. Passive testing involves projects such as auditing firewall rule sets. Conducting these tests regularly helps to ensure that misconfigurations of devices are revealed and can be resolved. Active testing, on the other hand, helps to ensure that defenses and alert systems are effective and performing the way that they are expected to. In order to help ensure your network perimeter is secure, both types of tests are necessary.

EnergySec
8440 SE Sunnybrook Blvd., Suite 206
Clackamas, OR 97015
877-267-4732
energysec.org

[1] “Efficacy of Emerging Network Security Technologies,” Ponemon Institute, Feb. 2013.

[2] www.reseal.co

[3] www.network-perception.com

[4] http://www.firemon.com

[5] NERC CIP v5. CIP-010-1 Table R3 - Vulnerability Assessments.

[6] A file which is not a virus, yet is detected by antivirus products and reported as if it were a virus. See http://www.eicar.org/86-0-Intended-use.html for more information on EICAR files.

[7] D. Duggan, “Penetration Testing of Industrial Control Systems,” Sandia National Laboratories, SAND2005-2846P, Mar. 2005.