GUIDE

Perimeter Health Check

Powered by

IT Security
COMMUNITY

CompTIA

Setting up foundational security can be challenging due to the complexity of today's security systems. Sometimes controls get removed accidentally during troubleshooting or policy changes and systems are left open and vulnerable.

This simple guide is an easy way to manually test your foundational security to ensure the proper controls are in place.

1. **What ports are left open?** Did you forward the ports correctly? https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap

   a. You should perform vulnerability scans for any open ports on a regular basis; at least monthly.

   b. Make sure to have proper patch management especially for services exposed to the internet.

2. **DOS defenses: If you have DOS prevention setup such as limiting TCP SYN amounts from 1 IP, test this with tools such as NMAP or Nessus, which are both free.** Other commercial tools are available. You can also test by doing a ping flood and seeing if the UTM will start dropping the requests at a certain point. Another simple free tool is hping3, some documentation can be found at http://www.hping.org/manpage.html and http://odaysecurity.com/articles/hping3_examples.html

3. **Gateway antivirus: Check to make sure your AV is set up properly.** You can use the eicar non malicious virus that is recognized by most AV engines found here http://www.eicar.org/86-0-Intended-use.html. It is best to test with various types of files and compressions, as well to make sure the AV engine isn't only looking for executables or doing a stream based only. Below are samples of the eicar that have already been compiled and are hosted at one of the www.shieldtest.com servers.

   a. Basic eicar virus file: http://www.ishieldu.com/WebInterface/home/b/eicar1.com

   b. 1 x zipped eicar file: http://www.ishieldu.com/WebInterface/home/b/eicar1.com.zip

   c. 9 x zipped eicar file: http://www.ishieldu.com/WebInterface/home/b/eicar1.com.9.zip

   d. Password protected zip with eicar file: http://www.ishieldu.com/WebInterface/home/b/eicar1.com.password.zip

   e. Gzip with eicar: http://www.ishieldu.com/WebInterface/home/b/eicar1.com.tar.gz

4. **IPS: Make sure it is set up properly.** Put something simple in a Web interface field such as a SQL injection command (https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)) or a directory traversal such as ../../../../../cmd.exe in the URL string.

5. **DLP – check to make sure your DLP is doing something.** Go to any form on a web page and type in a sample credit card number. You can also try to send an email (make sure you are using SMTP to test UTM or you have DLP on your mail system if it's an encrypted session to a hosted mail server. Sample numbers can be found here:
https://www.paypalobjects.com/en_US/vhelp/paypalmanager_help/credit_card_numbers.htm

6. **Block embargo countries.** Are you blocking countries that shouldn't be communicated with from US or EU? Can you get to http://www.gnu.rep.kp?

7. **Phishing: Visit several phishing websites published at www.openphish.com and check to see if you get a block page from your UTM.** Because this is a free public list, it is not very up to date, so don't be tricked by the browser blocking it, or tricked if it's not available anymore. Find the ones that are still live (towards the top of the list) and continue past the browser warning to see if your UTM will block it. This will not test the quality and how up to date your UTM or Web filtering are for blocks phishing websites, but will at least check to make sure it is setup correctly and you are getting the UTM block page.

8. **Web filtering test: Check to see if what you set to block is actually being blocked**. Here are some simple categories that are typically blocked:

   a. Pornography.

   b. Potentially liable.

   c. Anonymizer or public proxy.

9. **Safe search: Google safe search has been a bit tricky in the UTM sector and is almost impossible to keep up to date, but you can test with www.bing.com.** Set the content not to filter out explicit and check to make sure it automatically changes the search results back to "filter explicit."

10. **Botnet: Check to make sure your UTM gateway will detect botnet activity or C2 communication.** You can use a simple public list to make a connection and check to make sure your UTM blocks it and triggers a log. As all public lists, they are not the best and most up to date, but one of the better ones is http://rules.emergingthreats.net/blockrules/emerging-botcc.rules. You can use several of the recent entries to test the effectiveness of your UTM configuration.

11. **Patch management testing: Keeping everything patched and up to date is extremely important, especially if it's public facing.** Although UTMs have functions such as IPS to block exploits of known server vulnerabilities, it's always better to make sure your servers are patched. Nessus from Tenable is a free vulnerability scanner that will give you the ability to test if the latest patches have been applied. There are many paid versions out there that are automated and not very expensive. All of these will give you a general guide and do require some tweaking and interpretation, but are very good at revealing anything that could have been overlooked.

12. **Checking Spam Filter/Email File Policy/Email AV: Set manual traps and check if data is able to pass or is being blocked as expected.** The easiest way to check and make sure the spam system is working is to check the spam quarantine and you will see all the blocked emails.

    a. Block a domain or specific email address that you can test. Send the email from to make sure it is being blocked.

    b. Block a specific file type and send an email to make sure the system strips out that file.

    c. Email yourself the eicar test virus to make sure the email AV is picking it up and blocking it. http://www.ishieldu.com/WebInterface/home/b/eicar1.com

    d. Email yourself the eicar in a zip file to make sure it gets blocked. Do not block all zip files, otherwise this test will not be valid. Use all eicar versions in test number 3.

13. **UTM subscription up to date: As part of the process, always verify that the UTM subscription is up to date and you are receiving the latest signatures and updates.** The easy and obvious method is just to login to the management of the UTM and check that it has the latest update, make sure it is set to update hourly and make sure the subscription isn't expiring in the next six months.

About this guide...

How and when to use it: The IT Security Executive Council recommends performing the tests in this guide at least once a quarter on existing managed customers. This procedure is also a great way to engage new customer as part of a free security assessment to reveal the customers' security posture. When you give them a full report of what was blocked and what wasn't, give them an overall score and compare it to your customers on your managed services contract, as well as other businesses out there who are getting breached, paying fines, losing data, etc. It is important to explain that the cyber issue is growing exponentially and only recently has become a widespread problem in the SMB space.

Who should use this guide: While anyone who has the skill-set can use this guide, it is highly recommended all technicians performing these tests be properly trained. The test is useless unless it is performed properly. Even if technicians feel they have the knowledge, this needs to be verified. Going through the training is the only way to reveal gaps in skills and knowledge.

DISCLAIMER

This Testing Foundation Security Posture is for informational purposes only, and any reliance on its content is done at your own risk. Further, this Testing Foundation Security Posture and its contents are provided on an "AS IS" basis, and CompTIA makes no representations or warranties as to their completeness, accuracy or adequacy or that any advice, recommendations, or other content contained in this document will protect systems, networks, infrastructure, and the like from experiencing any cyberattacks or other security incidents. The security assessments and processes discussed in this document should be conducted by professionals experienced in the field of information technology security. The links referenced in this document direct users to third party websites. Any use of the links or the associated third party websites is done at the user's own risk, and additional terms and conditions from the owners of such websites may apply. CompTIA does not own or control these third party websites, and CompTIA does not endorse or assume any responsibility for the third party websites and the information, materials, products, services, and other contents contained therein, including any harmful items or code. CompTIA is not liable or responsible to you or your clients or customers for any results that you or they may experience, and you agree to indemnify CompTIA from and against any losses or other harms that you or your clients or customers may experience based on your use of the information contained in this Testing Foundation Security Posture. By your use of the information contained in the Testing Foundation Security Posture, you agree to the terms of this disclaimer section.