Security automation and optimization using HP-NA

Florian Ecard, Master SNE Student, UvA

January 2015
Abstract

As networks keep expanding throughout time, their management is becoming more and more complex. HP Network Automation (HP-NA) is a software that allows a much easier management of a large network by permitting management centralization, keeping track of the configuration’s modifications, who made these changes and more over.

The first aim of this project has been to automatically gather new CVE vulnerabilities which had then to be chosen depending on the specific equipment and requirements of the company.
Once this step was addressed, a second objective has been to automate the checking of the devices’ security configurations.
A third aim is to change the default authentication certificate of HP-NA, because every purchased HP-NA has the exact same default and self-signed certificate.
Finally, checking the SSH keys performance has also been aimed.

The first three objectives have been achieved while the fourth couldn’t be because of a lack of time.
Acknowledgements

I would like to thank my supervisor Olivier Willm for allowing me to do my research project with this company. It has been a wonderful experience.

I also would like to particularly thank Guillaume Demandier for supporting me all along this project and helping me every time I was in need for it. I am also grateful to the whole team for integrating me so well with the group and for providing help as much as they could do.

Finally, I would like to thank the SNE master for allowing this internship.
Contents

1 Introduction .................................................. 5
   1.1 Research question .................................... 6
   1.2 Ethics .................................................. 6

2 Literature Review ............................................. 7
   2.1 HP-SA & HP-CA ........................................... 7
   2.2 Network Vulnerability Assessment ......................... 8
   2.3 Cisco Prime .............................................. 8

3 Methodology ................................................... 9
   3.1 Software and devices used ................................. 9
   3.2 HP-LNc installation and customization ..................... 11
   3.3 Automate the security configuration checks ................. 14
       3.3.1 Cisco IOS ........................................... 16
       3.3.2 Cisco NXOS ........................................ 18
   3.4 Renew certificate ......................................... 20

4 Results and discussion ....................................... 23
   4.1 Research question & Results ............................... 23
   4.2 Problems encountered .................................... 25
       4.2.1 HP-LNc installation ................................ 25
       4.2.2 Certificates ......................................... 26

5 Conclusion and Future work .................................. 27
   5.1 Future work .............................................. 27
1 Introduction

As networks keep expanding throughout time, their management is becoming more and more complex. In order to manage them properly, it is possible to hire network administrators and/or use automation tools. For example, it is sometimes needed to run a similar command into several hundreds machines, maybe even thousands. In this case, it could be a waste of time and money to enter them manually. As a solution, a few tools are available so far, allowing this single command to be executed in every wanted device in only a few clicks. These tools also provide many other options.

HP Network Automation (HP-NA) is an HP proprietary software that aims to do what has just been explained. It is allowing a much easier management of a large network by permitting management centralization, keeping track of the configuration’s modifications and who made these changes. It standardizes the configurations using scripts. In addition, its policies can test the configuration’s compliances within the organization’s network.

In this research project, the first and biggest aim is to gather new CVE vulnerabilities using the HP-NA software and one of its modules, the Live Network connector (LNC). These vulnerabilities are then to be filtered and chosen depending on the specific equipment and requirements of the company. The found problems along with their solutions have to be automatically passed on to the network administrators so that they can be manually addressed. By doing so and if the administrators fix the given problems, this can help an organization to efficiently improve their security regarding known flaws for their specific equipment. The outcome of this method describes how more secure a company could be using it, by defining how better it could performs in a penetration testing environment at a vulnerability scan level.

Once this step has been addressed, a second objective is to automate the checking of the device’s security configurations. Such verification concerns for example ACLs, authentication configurations. Indeed, it is needed to be sure at any time that all the equipments are correctly configured for their security, have the same behaviour and that the content hasn’t been modified (one cannot check several hundreds of devices manually).

The third aim is to change the default authentication certificate of HP-NA, because every purchased HP-NA has the exact same certificate. An intruder would then be able to easily spoof the identity of the HP-NA and have access to a big part of the company’s network.

This report will first introduce the related work that has already been done concerning this subject. How it has been handled and the methodology will be defined in a third part. The results obtained will then be discussed and analyzed. Finally, a conclusion will provide the outcome and limitations of this research as well as an answer to the research questions.
1.1 Research question

1. Evaluate the "HP Network Automation" (HP-NA) software capabilities to audit the network equipments configurations about potential security issues. Using the editor supplied policies.
   Defining specific policies from the CVE database descriptions.
   Enforce company specific security configuration rules. Make a proof of concepts of this.

2. How to automatically check the security configurations of equipments?

3. How does it fit in an overall network security improvement process?

1.2 Ethics

There are not many ethical issues with this project: no hacking is performed.
However, for security reasons, the name of the company as well as its exact equipment and network topology will not be disclosed. Similar and general schemes will be given instead.
This choice has been made by the organization in order to allow a full transparency on how to reproduce this work for any large network. If the real topology and name of organization are provided, the flaws found (if any) could be used against the organization.
2 Literature Review

This section will introduce some tools that are similar and could meet the same achievements as HP-NA & HP-LNc. They will be described thoroughly and compared with HP-NA in the following sections.

This project being particularly precise, practical and concerning a specific product, not much work related to the outcome of the research exists or has been found.

2.1 HP-SA & HP-CA

HP-SA stands for Hewlett Packard Server Automation. It is another automation product of HP.
As its name says, this software manages both virtual and physical servers using a GUI. It provides similar services to the HP-NA except that the servers of the organization are being managed instead of the network level (switches and routers). It is thus managing the network at an upper OSI layer than the HP-NA.
HP-SA allows for example to automate the server discovery, software provisioning, application configuration and so on.
for more information about it, see the online website and its administration guide [7].

HP-CA stands for HP-Client Automation. This software concentrates on the management of end-to-end persistent devices, being either mobile or fixed and virtual or physical. It mostly reports on hardware and OSs uncommon activities. It allows thus to be compliant with complex and specific networks regardless of the specificity of it.
This software can reduce the costs on initiatives such as the virtualization, cloud, migration and more.
Refer to the HP-CA web page for more information [3].

By combining HP-SA, HP-CA and HP-NA, one could obtain a large network that is being managed in a much easier way than with a manual management. Considering that each of these three considerably improves the management of a network on their own.

The objective concerning the automatic retrieval of CVEs using HP-LNc could be adapted to the two of them, thus improving their security awareness too. They would obviously be concerned by other CVEs than the Network Automation software.
The integrity checking of the configuration should also be possible in these two. However, no information was found about this possibility and the assumption that it could be possible is thus to be verified.

Concerning the modification of the certificate for safety purposes, it appears that both the HP-SA and HP-CA certificates are default self-signed certificates. They should thus be replaced in the same manner as described for the HP-NA.

For each of these objectives, it is not guaranteed that the steps to follow will be the same as for HP-NA. Further investigation should be done to do so.
2.2 Network Vulnerability Assessment

This software (referred as NVA) is the closest related to the use that has been made of the HP-NA in this project. It is also used within the company.

This tool allows to make a database that gathers every known vulnerabilities of the company’s devices. These vulnerabilities are tested on the equipment using the tool Foundstone which is a free MacAfee proprietary product. See their website for more information [2]. Each vulnerability is then manually processed through an assessment in order to know whether or not the equipment is to be patched. This decision is also recorded in that database.

The company has been using these two software in order to test a same vulnerability on the same device with two different methods. In case one would find a vulnerability but not the other, it is thus to ensure a more coherent and consistent result.

This tool, as well as HP-NA, doesn’t allow by default to automatically check the newer vulnerabilities on the test equipment. The automation of this in HP-NA could be used as a base to obtain a similar result in NVA.

2.3 Cisco Prime

Compared to the NVA that is similar to HP-NA in a security way, Cisco Prime is similar to HP-NA in the management aspect.

This products aims to improve management issues such as the end-user demand for any-where, the use of intelligent devices in workplaces such as smartphones or business operative to save costs and implement green best practices.

Cisco defines its product as delivering ”next-generation management by supporting an intuitive workflow-oriented user experience and integrated lifecycle operations across Cisco architectures, technologies, and networks. ”

However, this tool is made to be used with Cisco devices, and there is no guaranty of the portability of this system.
More information can be found on Cisco’s website [1].
3 Methodology

There are several steps to execute the previously described goals, each of which uses HP-NA.

3.1 Software and devices used

HP-NA

The proprietary HP-NA (Network Automation) software that has been used in this project is the version 9.22. It has been installed into a Linux Redhat 5.3 server. HP-NA allows a company to manage its large network in a much easier way than before by centralizing its administration. It permits to modify the network topology through a Graphical User Interface (GUI). It also permits to easily show what devices are modified, how they are modified, who does these changes and why. In addition, predefined standard can be defined in order to implement policies and thus increase the security at a network level.

Several device providers are supported by the HP-NA such Cisco, Nortel, F5 and Extreme. The support of all these devices can thus be done via a single tool.

Several other core automation products exist. For instance, the HP-SA (Server Automation) has for objective to install and manage the servers applications. There also exist the HP Client Automation (CA) and more.

The HP-NA web page [5] can be used for more information.

HP-LNc

The version used of the HP-LNc is 3.40.

This tool is integrated within a lot of HP software products. It is used in order to dynamically update the content of a product by, for example in this case, download the latest CVE vulnerabilities. The content actually depends on the core automation products used by the organization (NA / SA / CA).

It has an extensible and powerful architecture allowing to safely download the content from the internet and optionally import it in the HP-NA. It can do so at downloading time by using the cutting-edge secure hash technology.

Its aim in this project is to download and import every week the new CVE vulnerabilities into the HP-NA to allow the administrators to have an up-to-date network.

If the LNc is installed within the HP-NA server, then it can be run from its GUI as an external task and thus be configured from there.

The LNc web page provided this information and more can be found in there [4].
The image [1] below shows how the CVEs are being retrieved and added to the server using HP-LNc and HP-NA.

**Management of the security alerts published**

1. New alert published by a security service
2. Alert translated in a rule of conformity management
3. Publication in the HP Live Network
4. Safe update of the NAS referential
5. Review of the rules and alert by the administrators. Association of the rules with servers
6. Conformity alerts are returned to the administrators
7. Selective update using VARS (HP-NA)

Figure 1: CVEs retrieval
3.2 HP-LNc installation and customization

In this first objective, the vulnerabilities are gathered and it is made sure that they are not already existing nor duplicated.

In order to do so, a module being available in HP-NA called HP Live Network connector (HP-LNc) has been used. This module allows to retrieve the vulnerabilities depending on the contract level (Depending on how much one pays) and display them into a software vulnerability report.

It has been possible to install the LNc onto the HP-NA from the SSH interface using Linux CLI. HP-LNc being installed on the HP-NA, the LNc is needed in order to allow the communication with the HP-LNc via the HTTPS interface.

For the installation details of this module, a documentation has been created for the company, which is also containing the problems encountered in order to avoid any similar issue in the future. This documentation is in French and available in Annex A.

As explained earlier on, The HP-LNc can be correctly configured by selecting the correct equipment family. These are called "streams", a list of the ones available in the LNc are shown in the figure below:

```
[root@talisbackcloud26 /tech/cloud/lnc/lnc/bin]$ ./live-network-connector list-streams

<table>
<thead>
<tr>
<th>Product</th>
<th>Service</th>
<th>Stream (stream name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.legacy (security.vc_legacy)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.juniper (security.vc_juniper)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.hp (security.vc_hp)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.nortel (security.vc_nortel)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.cisco (security.vc_cisco)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.f5 (security.vc_f5)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.checkpoint (security.vc_checkpoint)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.cisco_diag (security.vc_cisco_diag)</td>
</tr>
<tr>
<td>nas</td>
<td>security</td>
<td>security.vc.pol.cisco (security.vc_pol.cisco)</td>
</tr>
<tr>
<td>nas</td>
<td>content</td>
<td>content.na_drivers (content.na_drivers)</td>
</tr>
</tbody>
</table>
```

Figure 2: List the available streams in the HP-LNc

In this project, the organization is interested in the Cisco products.
To correctly configure the LNc, each configurations has to be entered using a CLI and not a text editor, the name of the command is live-network-connector. Indeed, HP-NA doesn’t support this method of configuration. As an example of command to add the products that the organization is interested in is:

```
./live-network-connector write-config --stream=security.vc.cisco --enable
```
To verify that they are effectively added to the Lnc, the command `list-locales` is used, as shown in the figure below.

```
[root@tlasebcloud26 /tech/cloud/lnc/lnc/bin]# ./live-network-connector list-locales
No product version detected, displaying all available content locales.

<table>
<thead>
<tr>
<th>Product</th>
<th>Stream</th>
<th>Locales</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas</td>
<td>security(vc_cisco)</td>
<td>en_US</td>
</tr>
<tr>
<td>nas</td>
<td>content.na_drivers</td>
<td>en_US</td>
</tr>
</tbody>
</table>
```

Figure 3: Enabled streams

Once the streams enabled, two usernames have to be entered. One is used to allow the Lnc to securely download the content from the HP website, this username is an HP username. The second one is one of the administrator’s username of the company that is needed to permit the Lnc to import the CVEs, once downloaded, the content of the newly retrieved CVEs. Another parameter must be entered in order to specify where the HP-NA is installed on the Linux server.

This separation between usernames needs to be known and well configured because if not the Lnc will not work at all.

Now that the Lnc should be running, if it isn’t the errors that have been encountered throughout this project are defined with their solution in the next chapter, in the "Problems Encountered" part.

Once running and that the first CVEs have been retrieved, a way to automate these retrievals had to be found. To do so, the HP-NA allows to run as an external task the Lnc (only because the Lnc is installed onto the same server as HP-NA). It has to be defined by going in `Tasks → New Tasks → External task`. The fields have to be fulfilled and the schedule chosen (Wednesday is advised as new CVEs are released on Tuesdays). An example of configuration is shown in the next figure where the absolute path shown is the one used in order to launch the Lnc.
Now that the LNc is configured to retrieve the new CVEs every Wednesday, the next step is to automate their checking with the device family concerned. These new vulnerabilities should be automatically filtered and then tested onto the concerned equipment only.

Doing so has not been possible in this project because it would have needed the development of a Perl Script.

An example on how to do this would be to take some test devices and add them in new groups, representing a device family. Then the next step would be to retrieve the family group concerned in the newly discovered vulnerabilities (i.e. Cisco NXOS). Having these, running the vulnerability only on the concerned equipment should be possible. The final aim would be to alarm the administrator only with the devices that are vulnerable.
3.3 Automate the security configuration checks

This section will describe how it has been possible to automatically check the integrity of the security configuration of the Cisco devices. It will thus be made sure that nobody (intruder or not) has modified the configuration of the equipment without any knowledge or maybe cancel/detect any human mistake. This is done using HP-NA but not the HP-LNc.

Each device has a type of operating system. In the organisation’s network, only Cisco IOS and Cisco NXOS (Nexus) have been treated. The concerned equipment potentially gathers over 2000 Cisco devices. Being a specific configuration for the production environment, it concerns so far about 60 switches but can be adapted to the whole park if needed.

Two different OSs being checked, two policies have been created and are described below. Two groups have also been created, containing sample devices. For the NXOS device, only a Nexus 5000 has been checked as it is the only available in the company, the name of its group is ”Test NXOS security integrity”. Concerning the IOS devices, there are two different kinds: the Catalyst 4500 and 2960. The name of this group is ”Test IOS security integrity”.

To start with, a retrieval of the standard configurations that have to be in place per equipment has been done. Doing so allowed to distinguish the security configurations from the routing ones. Once retrieved, the different rules have to be made in order to quickly identify where from the errors come, in case such mistake / attack happens.

The rules that have been made are:

- ACLs are an essential security configuration. Indeed, it allows to filter and access a specific range of IP address, simply dropping non-authorized connections. If modified, an intruder could get in the network or damage it.
- The features are functions to be enabled only in Nexus switches, they are defined before the configuration to avoid ”useless” lines of code. As an example, one can disable Telnet from there. If an intruder could modify these features, he/she could for instance enable a service having a known flaw that would then be used by the hacker.
- AAA (Authentication, Authorization and Accounting) is mainly responsible of the authentication. The devices define who can authenticate and to whom (which servers). If an attacker can change these parameters, an example of attack would be to define the AAA server as being your own and a range of attacks are possible from there.
- NTP (Network Time Protocol) is the server being responsible of the network’s synchronization. An attacker taking control of this part of the configurations could as an example change the clock of one device and all the switches would have to synchronize themselves again, this could in very bad case crash the whole park.
- Change the username access is of course a serious problem as they provide direct access to several critical equipments. They thus must be well protected.
- The VTY parameters are the enabling of protocols such as Telnet and SSH. It is known that Telnet isn’t safe any more and it must be made sure that no telnet is enabled, SSH should be.
- The logging facilities must be well protected: if for some reasons they are moved to somewhere else or deleted, it becomes impossible to troubleshoot what has happened.
All these reasons show that it must be sure that these parameters haven’t been modified. The way to do so for each OS is described in the following subsections. The rules can be chosen to be done using Regular expressions or not in order to be more flexible. A simple box has to be checked to enable it.

Once all the rules have been created to allow the checking of the integrity of these two Cisco OSs, they must be associated to the correct devices. To do so, Each set of rules (about NTP, ACLs etc.) has been added in a policy (one per OS), and this policy will associate the compliance of these rules with the associated group of devices. this group will obviously be containing the test devices of the concerned OS. In order to automate this policy (if not an administrator would have to run the policy himself), a new task needs to be created in a similar way as in the first aim.

The following will describe in details how this has been done both for Cisco IOS and Cisco NXOS operating systems.
A policy can be created from the HP-NA in the menu bar "Policies → New policy". The way to do so is shown in the figure 5 below.

For Cisco IOS operating systems, the AAA authentication integrity has been checked first, using regular expressions: A line is present in some devices but isn’t in others and thus has to be made optional. The concerned line is "aaa authorization console". It also checks the integrity of every line.

The second part of rules concern the ACLs. To check the STATICOSPF ACL, the regex was used because the final line could be either a "!" or an expression. For SNMP-RO and SNMP-RW ACLs, no regex were used. Indeed, only being sure that all the lines aren’t changed and that their order is the same.

The telnet-vars ACL is different, its policy is based on block recognition. This kind of policy finds every block of a configuration file that is starting and ending by a particular expression.
What should be in between is thus defined in a separate field, also allowing to specify what
should NOT be in there (also available when the block mode isn’t enabled). Here it is
checked that SSH is used by controlling that each line finishes with a 22 (for the port num-
ber), and that Telnet isn’t by making sure there is no 23.

The logging facility, using the regex, could be detected in two ways, depending on the equip-
ment. It could be done by either detecting the first line as being a "!", or as being a "deny
ip any any" from another ACL. The same applies to find the last line.
There were in some cases 3 or 4 configuration lines, one of them being optional.
Simply checking the configuration lines about the logging could have been done, but if lines
were added to this part, simply checking them couldn’t allow to see that.

As you can see in the figure below, the integrity of the NTP has been checked also using
regex. In there, It is shown that the clock period can be any number of 8 figures, with any
source as it could change depending on the device.
There also is an optional line which is the update of the calendar, followed by the addresses
of the two servers and finally ended by the word "end".

Figure 6: NTP integrity
The usernames can be defined in two different ways, either using the combination "secret 5 [30 charac passwd]" or "password 7 [16 charac passwd]". Regex are used to make the distinction between these two as follow:
secret—password 5—7 ([§]30)—([A-Z,0-9]16)
Like for the other policy rules, the first and last line are concerning other blocks, to be sure nobody modified the lines.

3.3.2 Cisco NXOS

An example of the policy rules created, available in the HP-NA GUI is shown in the figure below:

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Rule Type</th>
<th>Device Family</th>
<th>Importance</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Configuration</td>
<td>Cisco NXOS</td>
<td>High</td>
<td>Checks if all the authentication rules haven't been modified</td>
<td>View &amp; Edit</td>
</tr>
<tr>
<td>features</td>
<td>Configuration</td>
<td>Cisco NXOS</td>
<td>Medium</td>
<td>Check the integrity of the features</td>
<td>View &amp; Edit</td>
</tr>
<tr>
<td>ntp</td>
<td>Configuration</td>
<td>Cisco NXOS</td>
<td>Medium</td>
<td>checking the NTP integrity</td>
<td>View &amp; Edit</td>
</tr>
<tr>
<td>usernames</td>
<td>Configuration</td>
<td>Cisco NXOS</td>
<td>High</td>
<td>Check the integrity of the usernames (no need to modify if only the password has changed as long the encryption is on 34 characters)</td>
<td>View &amp; Edit</td>
</tr>
<tr>
<td>vty</td>
<td>Configuration</td>
<td>Cisco NXOS</td>
<td>Medium</td>
<td>Check the integrity of the vty and makes sure ssh is enabled and telnet isn't</td>
<td>View &amp; Edit</td>
</tr>
</tbody>
</table>

Figure 7: Test NXOS integrity

Concerning AAA rules, They are very similar to the ones in the IOS policies. The ACLs rules are simply cut and paste in the policy rules as they are similar in each device. They concern SNMP-RO, SNMP-RW and SSH and being one after another, simply check the "Lines in exact order" is used to check that nobody modified them.

SNMP-RO stands for Read Only and is destined to be used in a public manner while SNMP-RW (for Read and Write) aims to be used in a private manner.
The features is specific to this OS. As explained earlier, they allow to enable some features without having to do so later in the configuration. To check them, the lines are simply cut and pasted and it is checked using a regex that the first and last line are spaces.

Concerning NTP, there apparently is no clock defined and the lines are fixed for each of them. A simple copy-paste can then be done in the same way as for the features rule.

VTY policies are checked in a similar manner, only using a copy-paste of the configuration and checking the “Lines in exact order” box.

The username rule is quite similar to the IOS OSs but it is easier. Indeed, there is only one kind of password introduction, there is thus no need to provide a regex alternative. However, thanks to the regex it is still possible for a user to change its password without becoming vulnerable to this integrity check. It allows not be forced to change the rule every time a password is changed. This rule is seeable in the figure [8] below.

Figure 8: Username rule
3.4 Renew certificate

This objective was done based on the HP-NA administration guide [8] and userguide [9].

SSL certificates are used to allow a secure connection between a server and a web browser. They are used to authenticate one another.

By using only certificates, one could create a certificate saying that he is Alice whereas he is in fact Trudy. In order to prevent such thing to happen, A Certificate Authority (CA) can be used. This authority is a third party that assures to both sides that if Alice claims she is herself, then the CA can assure it and thus avoid an identity theft.

HP-NA uses certificates. However, every HP-NA uses a default and known certificate. This means that even if HP-NA is only accessible from the inside of a company’s network, if an intruder manages to get in, he could act as if he was HP-NA and thus retrieve usernames and passwords.

In addition to it, every time the HP-NA is accessed, a pop up saying that the navigation isn’t private appears as shown in the figure below[9]. So every time a network administrator accesses it, he has to accept it and thus could be under attack without even noticing it.

![Figure 9: Navigation not private](image-url)

Figure 9: Navigation not private
This flaw had to be fixed as it could be a serious problem. Generate a new certificate using one of the company’s CA has thus been done. It allows to be sure that the HP-NA actually is itself and also that no error appears when connecting to it. If an attack on the certificate occurs then this very problem (navigation not private) will show up and this time the network administrator will be aware that a problem is happening and could react in accordance.

A detailed documentation has been created so that the next time the organization wants to change the certificates they can do so by simply following the steps provided, This documentation is seeable in the Annexe 2. If more details about the actual implementation with the commands to execute and so on are wanted, please refer to it.

To change this certificate, it is needed to connect to the HP-NA via the SSH interface and go into the directory containing the certificates called truecontrol.keystore and truecontrol.truststore. The .keystore contains the certificate for the serveur in itself and the .truststore contains the chain of trust, corresponding to the CA. Create a backup before doing anything.

From there, a new asymmetric RSA key has to be generated using the command keytool (2048 bits is great compared to the actual technology), it is by default valid for a year. At the generation time, some values are asked such as the name of the organization (it HAS TO BE the Fully Qualified Domain Name of the server), the country and so on. Only the first field concerning the FQDN has to be exact, the others are only informational.

The figure below shows concatenated certificates of the chain of trust and is explained in the next page.

Figure 10: Concatenated certificates
Once the key has been created, it is used to create a CSR (Certificate Signing Request). This certificate is sent to the CA so that the latter can sign the certificate and return the final certificate.crt that is to be used to verify the identity of the server. At least two certificates are returned, one is for the .keystore and the other for the truststore. If more are sent the others are used to create the chain of trust for the truststore. If more than two are received, then the chain certificates have to be concatenated into a single file in order to still have only two files. Each certificate is put one after another where the first one HAS TO BE the root certificate. An example of this is shown in the figure from the previous page.

Before importing these certificates into the .keystore and .truststore, the actual alias(es) have to be exported and deleted. Once this and the importation done, the certificates are ready to be used and a simple restart of the service should make everything work. To be sure it did work, it is just needed to go to the URL of the server and if the error from the figure above isn’t coming but instead showing straight away the login page such as below, it means that everything works.

To double check it, click on the lock next to the "HTTPS" in the URL and verify that information about the certificate is true.

![Figure 11: Navigation not private](image)

It can happen that it doesn’t work the first time or that the HTTPS in the URL still is marked red rather than green. This would be because the root certificate provided by the certificate isn’t yet validated in the hosts desktops. To avoid waiting that it gets validated, the administrator using HP-NA should add the root certificate to the certificates trusted by the web browser.
4 Results and discussion

4.1 Research question & Results

1. Evaluate the "HP Network Automation" (HP-NA) software capabilities to audit the network equipments configurations about potential security issues. Using the editor supplied policies.
   Defining specific policies from the CVE database descriptions.
   Enforce company specific security configuration rules. Make a proof of concepts of this.

2. How to automatically check the security configurations of equipments?

3. How does it fit in an overall network security improvement process?

Other objectives were added during the project. One was found during the project itself in order to improve a bit more the company’s security.
The creation of a new CA signed certificate has thus been done in order to provide a trusted certificate. Indeed, even if HP-NA shouldn’t be accessible from the outside, if an intruder manages to get into the network where HP-NA has a default certificate, it could be very dangerous for the organization.
Changing this certificate has thus been done and an extra objective achieved.

The second added objective was to check the length of the SSH keys and be sure that they are regenerate at each use. This objective hasn’t been achieved as there wasn’t enough time to do so.

Concerning the first objective, the expected results were to detect and show to the security team the newest known vulnerabilities in an automatic manner and only for the desired equipment.
this aim has been a success using the HP-LNc to retrieve the CVEs and the HP-NA to retrieve them in an automatic manner every week. This result could be expanded as explained in the next chapter.

In a second time, the automation of a created integrity check for several device families was aimed. This objective has also been a success by creating policies in the HP-NA that would check the configuration of some Cisco IOS and NXOS OSs.
The same automation method as the retrieval of CVEs has been used to automate this task every Thursday.
The image shown in the next page shows when a policy and its rules are in compliance with the selected devices.
To answer to the last research question, the findings and implementation of the project have allowed to have a much secure HP-NA and thus a more secure network. However, these improvements will be useful only if an intruder manages to get into the organization’s network. Indeed, these improvements are only internal but could save a lot of things in case somebody manages to get into the network.
4.2 Problems encountered

Throughout this project, a lot of problems had to be solved. Firstly, it took a week before all the access (four different accounts were needed) to the equipments was provided, significantly delaying the time to be operational on the devices.

4.2.1 HP-LNc installation

Another problem showed up when the HP-NA’s manipulation started. There are two HP-NA in the company’s network, one of them is used for testing and the other one for the operational network. The whole project was based on the HP-NA test which had just been upgraded to a newer version and was under test before putting it to the operational HP-NA. This Lead to synchronization problems in between this project and the upgrade checking as we were several people implementing things on the same server.

The first real problem was when trying to install the LNc. The port to connect to the HP-NA through putty was changed (reactivated the port 8022 to allow direct access to the HP-NA from the web). After a manipulation of one of the engineers, the HP-NA wasn’t accessible through SSH for a few hours, slowing down the tests once again.

Also, the update in the production environment was made during this project and it switched off the access to the HP-NA for about a day (the team disabled the login facility to be sure nobody can connect to it, cutting access to the test server too).

The LNc being finally installed and configured, it was launched in order to try to put the module up-to-date with the latest CVEs. However, it stated that the HP-LNc database was actually up-to-date even if it contained at best CVEs from 2011. The solution to this problem was a bad configuration. Indeed, the settings were added by hand using "vim" whereas it HAS TO BE done using the live network connector CLI.

Once this had been corrected, a new update was tried by enabling Cisco devices, the result gave a new bunch of errors. The most significant one was stating that the connection to the localhost through the APIs was undoable.

A first attempt to solve this was to add a line of code to a file because it was guessed that Java couldn’t recognize the correct IP address running the NA Core. This failed. In the mean time, another team was working on the same server and changed a few things on it (notably the port to access) thus not allowing to access the server for a few hours. It had for effect to slow down the trouble shooting.

Once back in it, it was notified that two different logins had to be used. One for the connection to the HP database (the HP user) retrieving the CVEs and one to the HP-NA server (Specific to the organization) to allow the import of these vulnerabilities. It appeared that only the HP user was used, so the organization’s username was used as well but it still didn’t work for the import of CVEs in the server, saying unable to continue with import.

The solution found was that the user provided in the configuration was ‘only’ an expert and a root account was needed, this problem was definitely solved by switching this account with a root user.

The LNc was now 100% working and more than a hundred newer CVEs were downloaded.

The network team updated the HP-NA’s version in production and therefore, they cut the access to the login facilities for a day. I thus couldn’t work on it for this period.
4.2.2 Certificates

Concerning the certificates, the HP documentation showing how to change it is very badly explained (see [8], p.97) and thus some problems arose.

The first problem encountered was due to a human mistake though. Indeed, when asking for a certificate, the most important thing is to correctly provide the FQDN of the server, which hasn’t been done in a good way. The www was added by mistake in the demand to sign the certificate. Thus it couldn’t be working but once the correct one has been asked it should have worked.

Also, the order of adding of the certificates in the .truststore file wasn’t correctly followed and it was ignored that the root certificate should be placed first. It thus wasn’t done in the first instance but corrected after some trouble shooting of the problem that arose with this situation.
5 Conclusion and Future work

In this project, out of the four objectives that were provided, three have been achieved. The automatic retrieval of the new CVEs concerning Cisco has been achieved using the HP-NA and its module, the LNc (Live Network connector).

Automatically check the devices’ security configuration integrity has also been achieved. This aim has been done using HP-NA only, once the configuration that wanted to be checked and the policies had been defined.

Changing the self-signed certificate present by default in the HP-NA to a CA-signed certificate has also been done.

Concerning the final objective with SSH, it hasn’t been possible to achieve it because of a lack of time.

To conclude on a personal point of view, this project has been really rewarding because it has been the first time that such a short internship has been performed.

It has brought the ability to adapt quicker to a new environment as well as learned to work efficiently and very quickly.

5.1 Future work

As a future work, it would be possible to improve the first objective. Indeed, using the HP-NA API in Perl, a script could be written so that once the CVEs are retrieved, all of them would be checked on the concerned equipment. Once this done, only the devices reported vulnerable should be returned to the administrators.

If this first improvement was to be achieved, then it would be possible to compare the results returned by it, with the other tool of the company: NVA - Network Vulnerability Assessment. Doing so would allow to ensure that both tools provide the same vulnerabilities and that the same devices are found to be vulnerable.

A last objective would be to do what was wanted to be undertaken with the SSH keys. Which means to check for example the key length of the keys, or be sure that they are regenerated at each connection and further on.
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CVEs retrieval</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>List the available streams in the HP-LNe</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>Enabled streams</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>Example of recurrent task to retrieve the CVEs</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>Test IOS integrity</td>
<td>16</td>
</tr>
<tr>
<td>6</td>
<td>NTP integrity</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>Test NXOS integrity</td>
<td>18</td>
</tr>
<tr>
<td>8</td>
<td>Username rule</td>
<td>19</td>
</tr>
<tr>
<td>9</td>
<td>Navigation not private</td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td>Concatenated certificates</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>Navigation not private</td>
<td>22</td>
</tr>
<tr>
<td>12</td>
<td>Test of the policies</td>
<td>24</td>
</tr>
</tbody>
</table>
References


Appendixes

Appendix A
Configurer Live Network connector (LNc)

Premièrement, certains critères doivent être vérifiés avant de commencer la configuration:
- Être root est obligatoire.
- Si une version de LNc est déjà installée, elle doit être entièrement effacée.
- Le port 443 doit être ouvert car LNc communique avec HPLN via le port HTTPS.
- La variable d'environnement PYTHON_HOME doit NE PAS être fixée.
- Si LNc est utilisé pour Software Automation (SA), DET (DCML Exchange Tool) doit être installé via /opt/opsware/cbt.

L'installation peut être faite en suivant simplement les étapes de la documentation, les étapes ne seront donc pas décrite ici, seulement la configuration sera expliquée.

Une fois ces étapes validées, la configuration peut commencer. Toutes les étapes qui suivront ne concerneront que les serveurs Linux ou Solaris.

Configuration

Dans les commandes montrées ci-après, install_directory fait référence à l'emplacement du LNc, dans notre cas: /tech/cloud/lnc

Le fichier de configuration LNc se trouve à: install_directory/lnc/etc/live-network-connector.conf.
Le fichier contenant les logs est à: install_directory/lnc/log/live-network-connector.log.

IMPORTANT: Les fichiers qui seront modifiés pour la configuration NE DOIVENT PAS être modifiés à la main (vim ou nano par exemple) mais avec la ligne de commande LNc utilisant write-config.
La fonction write-config marche de la façon suivante, où XXX représente la nouvelle configuration à effectuer, le remplacer par --help pour obtenir de l'aide:
install_directory/lnc/bin/live-network-connector write-config XXX

Afin de configurer correctement LNc, le type de produit doit être spécifié dans le fichier de config. Dans ce cas, le module sera utilisé pour NA (Network Automation), l'initiale qui doit être ajoutée à la variable “product” est donc “nas”. Dans le répertoire install_directory/lnc/bin/:
./live-network-connector write-config --product=nas

Une fois ceci fait, le username et mot de passe administrateur de NA doivent être ajoutés en renseignant les champs nas_user et nas_pass. Le compte HP doit aussi être renseigné. Le champs nas_root doit contenir le dossier dans lequel nas a été activé (/tech/cloud/VARS).
./live-network-connector write-config --setting=nas.nas_user=ADMINUSER
./live-network-connector write-config --setting=nas.nas_pass=ADMINPWD
./live-network-connector write-config --username=HPuser --password=HPpwd
./live-network-connector write-config --setting=nas.nas_root=/tech/cloud/VARS

Les marques d'équipements de la compagnie et le driver doivent maintenant être activé:
./live-network-connector write-config --stream=security.vc_cisco --enable
./live-network-connector write-config --stream=security.vc_f5 --enable
./live-network-connector write-config --stream=content.na_drivers --enable
Quelques commandes basiques pour vérifier la configuration

./live-network-connector read-config # Montre la configuration générale
./live-network-connector list-streams # Montre quel équipements sont disponible
./live-network-connector list-locales # Montre quel équipements sont activés
./live-network-connector list-status # Montre le status des équipements validés
./live-network-connector # Lance la récupération de CVEs

Automatisation de la récupération de CVEs

La configuration est maintenant terminée et après avoir lancé la dernière ligne de commande ci-dessus, le Lnc devrait avoir récupéré les dernières CVEs concernées.
La récurrence du Lnc doit maintenant être programmée. Lnc étant sur le même serveur que HPNA, il est possible de l'exécuter comme une application externe depuis l'interface graphique d'HPNA en elle-même. La marche à suivre pour ce faire est décrite ci-dessous.

Depuis l'interface graphique, aller dans Tasks → New tasks → Run external application. Une nouvelle fenêtre va s'afficher “New task / Template”, HPLN sera démarré d'ici. Les différents champs à renseigner doivent être remplis comme sui (ceux n'étant pas spécifiés sont laissés tel quel, par défaut):

- Task name → Synchronize Content Cache
- Start date → Select next Wednesday morning (vulnerabilities released on Tuesdays)
- Run → /tech/cloud/lnc/lnc/bin/live-network-connector
- Task Result → Check “Treat non-zero result code as failed task”
- Retry count → Can be set to whatever value, Once is suggested.
- Recurring option → Select Weekly and Wednesday.
- Task Completed notification can be chosen to be sent by email or not at all, it depends on the preferences of the administrator.

→ Voir l'image en dernière page pour example (screenshot du HPNA “New task / Template”)

Appendix B
Ajouter un certificat signé par une autorité de certification, 
pour HP-NA

NAHOME représente le répertoire d'installation du HP-NA.

- Se positionner via l'interface SSH du HP-NA, dans NAHOME/server/ext/jboss/server/default/conf . C'est dans ce répertoire que se trouvent les fichiers de certificats .keystore et .truststore.

- Une nouvelle clé doit ensuite être créée dans le fichier .keystore (d'abord faire un backup du fichier). Pour ce faire, la commande suivante doit être entrée depuis le répertoire ci-dessus:
NAHOME/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -validity 365 -alias nacacert -keystore truecontrol.keystore

La clé est valable 1an et l'alias choisi doit être le même tout au long de la manipulation. Le mot de passe qui sera demandé est: sentinel
→ Ce mot de passe devrait être changé car c'est le MDP par défaut fourni par la documentation HP. Lors de la prochaine implementation, pour pouvoir le changer, les fichiers truecontrol doivent simplement être effacés et seront regénérés par la commande précédente où le nouveau MDP sera redemandé.

- Les informations demandées doivent être renseignées dans les champs. Il n'est pas obligatoire de les remplir tous correctement mais c'est conseillé, ils existent simplement à titre informationnel.

   Seul le premier paramètre DOIT être vrai pour des raisons de bon fonctionnement. Il sera demandé le “First and last name” qui correspond au FQDN (Fully Qualified Domain Name):

   First name and Last name (FQDN): var-rct.XXX.fr
   C: FR
   OU: DITCID
   O: ORGANIZATION
   L: CITY
   ST: France

   Taper “yes” pour valider les choix. Quand le mot de passe est demandé, taper entrée pour garder le mot de passe précédent ou entrer un nouveau si souhaité différent de celui du keystore.

- Maintenant que le fichier .keystore est modifié, le CSR (Certificate Signing Request) doit être créé. Depuis le même répertoire, taper la commande:
NAHOME/jre/bin/keytool -certreq -alias nacacert -file narequest.csr -keystore truecontrol.keystore

   Ce certificat est utilisé pour que l'autorité de certification puisse le signer et retourner un fichier .crt. Pour ce faire, contacter les responsables de certificats de l'entreprise (généralement l'équipe sécurité).

- Plusieurs certificats sont retournés, 1 sera le certificat de serveur signé et les autres seront la chaîne de certification contenant les certificats root et autres.
Leur mise en place doit maintenant être effectuée. Pour ce faire, rester positionné dans:
NAHOME/server/ext/jboss/server/default/conf

Créer un autre backup des fichiers truecontrol.keystore et truecontrol.truststore car si une erreur est produite plus tard, il est possible de recommencer les opérations à venir depuis cette sauvegarde.
Importeur les certificats reçus dans le répertoire courant, s'ils ne sont pas sur la même machine, les importer en utilisant la commande scp ou une méthode similaire.
NE PAS copier-coller car des pertes de données sont possible.

Maintenant que les certificats sont importés et que les fichiers truecontrol sont backuped, les certificats doivent être concaténés les uns avec les autres afin de n'obtenir que deux certificats finaux. L'un est fait pour le certificat serveur et l'autre pour établir la chaîne de confiance.
Normalement, chaque fichier ne contient qu'un seul certificat et si ce n'est pas le cas, seul l'ajout au certificat serveur est nécessaire
Dans le certificat serveur, ajouter à la suite et dans cet ordre (vim peut être utilisé) les certificats Root, Technical et Internal. Le certificat serveur devrait donc maintenant contenir tous les certificats.
Concaténer ensuite dans un seul fichier les certificats de la chaîne d'authenticité et dans l'ordre précisé les certificats Root en premier, les suivants comme bon vous semble.
Pour ce faire, les commandes suivantes ont été utilisées:
cat CAEAirFrance-KLMRootCA.cer CAETechnicalCA.cer CAEInternalInfrastructureCA.cacert.cer >> vars-rect.XXX.fr.cer
vim vars-rect.XXX.fr.cer
cat CAEAirFrance-KLMRootCA.cer CAETechnicalCA.cer CAEInternalInfrastructureCA.cacert.cer > Concatenated.cer
La commande vim est utilisée pour vérifier que les certificats sont dans la bonne position, comme dans l'exemple de .keystore qui est montré ci-après:

Il est visible dans cette figure que 4 certificats sont positionnés les uns après les autres. Le fichier contenant seulement les autorités de certification ne contiendra que les 3 inférieurs. Celui du haut étant le certificat serveur, contenu uniquement dans le truecontrol.keystore.
Une fois ces certificats créés, l'alias présent dans le .keystore (à savoir “sentinel”) doit être effacé:
NAHOME/jre/bin/keytool -export -alias sentinel -file sentinel_from_truecontrol_keystore.cer -keystore truecontrol.keystore
NAHOME/jre/bin/keytool -delete -alias sentinel -keystore truecontrol.keystore

The alias may have changed throughout time, one can check it using the command:
NAHOME/jre/bin/keytool -list -keystore truecontrol.keystore

- Les deux certificats peuvent maintenant être importés dans les fichiers truecontrol.keystore et truecontrol.truststore, contenant respectivement le certificat serveur et le certificat d'autorité créé auparavant:
NAHOME/jre/bin/keytool -import -trustcacerts -alias nacacert -file vars-rct.XXX.fr.cer -keystore truecontrol.keystore
NAHOME/jre/bin/keytool -import -trustcacerts -alias nacacert -file Concatenated.cer -keystore truecontrol.truststore

- Les nouveaux certificats sont maintenant opérationnels. Un fichier doit encore être modifié, celui-ci permettra une navigation plus rapide dans le HP-NA quand connecté.
Pour ce faire, ajouter dans le fichier (dans les options, mais pas à la dernière ligne car celle-ci doit être fixe) NAHOME/jre/adjustable_options.rcx la ligne suivante:
<option name="startup/precompile/http.prefix">https://vars-rct.XXX.fr/</option>

- Toutes les étapes de changement de certificat sont maintenant effectuées, le service truecontrol doit maintenant être relancé:
/etc/init.d/truecontrol restart

- Au moment de l'installation de ce certificat, l'autorité n'était pas encore déployée dans le réseau, générant un message d'erreur mais autorisant tout de même l'accès à la page.
Le nouveau certificat en place sera 'trusté' prochainement sur tous les postes de la compagnie.
Ce problème se reconnaît du fait que la page d'accueil affiche d'abord une popup signalant que le certificat n'est pas bon, et demandant de valider un accès dangereux à la page. La majorité des personnes valide donc cet accès et c'est ce qui fait la dangerosité d'un certificat non-trusté.
Si une erreur similaire se produit, cela veut dire que le certificat Root a besoin d'être ajouté aux certificats de confiance du navigateur de recherche.
Un exemple pour ce faire sous Firefox est décrit ci-dessous:

Dans une fenêtre du navigateur, en haut à droite: Open menu → Preferences → click the tab Advanced → click the tab Certificates → Click View certificate.
On the new popup in the tab authorities → Import → Browse to the root certificate and import it.

En faisant cela, le poste informatique en question ne verra plus la page d'erreur et si elle revient à un moment donné, alors la personne à ce poste saura que quelque chose ne va pas, permettant de suspecter une attaque.
TROUBLE SHOOTING

- Prêter attention à la demande de certificat au moment de la création du CSR (Certificate Signing Request). En effet, si la demande du 'First and Last Name' correspondant au FQDN est mal renseignée, alors le certificat ne marchera pas.
Par exemple lors d'une première demande, le premier certificat était demandé pour le FQDN www.vars-rct.XXX.fr. Cela n'avait donc pas fonctionné car cette VIP n'est accessible qu'en interne et la demande devait donc être vars-rct.XXX.fr.

- Rester vigilant quand à la manipulation des fichier truecontrol.keystore et truecontrol.truststore. En effet, si une erreur similaire à celle décrite ci-dessus arrive, alors ces fichiers devront être manipulés et une mauvaise manipulation peut arriver par la suite. Les commandes effectuées doivent être effectuées sur le bon fichier.
Si le nouveau certificat reçu est appliqué sur les anciens fichiers truecontrol, alors cela ne marchera pas car les clés ne correspondront pas.

- L'ordre d'ajout des certificats doit être respecté comme il l'a déjà été précisé plus tôt. En effet, si l'ordre des ajouts de certificats n'est pas respecté, une erreur “keytool error: java.lang.Exception: Failed to establish chain from reply” apparaîtra au moment de l'importation des certificats.