CMPUT 333, Assignment 2, Fall 2016

(firewalls, network services, public key encryption, certificate authorities)

Services & Firewall Configuration (70%)

Part 1 (5%)

Your first step to completing this assignment is to choose non-trivial *root* passwords for your virtual Linux firewall host and non-trivial *Administrator* passwords for your virtual Windows host. Use your experience from the previous assignment and the readings of this course to choose strong passwords. Your chosen passwords and the reasons you chose them are to be included in the deliverables of this assignment.

Part 2 (30%)

In this task you will configure services from your own group's virtual network and make them available to "outsiders" (other groups and the TAs) in a manner which is controlled by your firewall host. In this assignment you may need to recompile the Linux kernel and/or load kernel modules on your firewall host to enable adequate **`iptables`** support. The process of kernel modification and how to configure the recompiled kernel's properties and modules will be presented in the labs.

Install and/or configure adequate software to provide http services from your Windows host as well as ftp and tftp services from your Linux host. In doing so, ensure you satisfy the following requirements:

- Create two new regular user accounts on your Linux host to be able to demonstrate that the users have **ftp** access.
- The **ftp** service should allow access for each user with an account on your Linux host except for **`root`** (**`root`** should *not* have ftp access). The **ftp** service should also **not** allow `anonymous` access.
- The **ftp** server should have at least one file of content available called **`myftpcontent.pdf`** at the top directory of the space accessed by 'anonymous'.
- The **ftp** server should allow each regular user to upload and download files from a directory. This directory should be different for each regular user.
- Additionally, your Linux host must be able to support a **tftp** service allowing read-only access to the contents of a specific directory (not associated with any user). The directory should have at least one file named **`mytftpcontent.pdf`**
- On your Windows host, create two regular user accounts to be used for testing **http** access to per-user directories.
- Your http server **must** be listening to port 8080 and **not** on port 80.
- The **http** service should have at the very least a single web page accessible as **`mywebcontent.html`** at the top level. Also, under the top level there should be two sub-directories, each with the name of the regular user you created.
- Access to each of the two subdirectories should only be allowed to the corresponding user, and only after the user provides username/password.

In your writeup report, you have to address the following questions: How did you select the passwords for the two regular Linux user accounts and for the two regular Windows user accounts and why? Compare and contrast how the authentication in the case of the web server works, and how does it work in the case of the ftp server and also in the case of the tftp server? [Answers to these questions as well as information to help the TAs test that you have correctly executed the specifications, e.g., the usernames and passwords, etc., should be included in the deliverable writeup.]

Part 3 (35%)

Your task is to introduce **`iptables`** forwarding rules to enforce the following policies, assuming you are group X (where X=1,2,3,4,5,6,7,8,9,10,11,12,13):

Inbound restrictions:

- Allow any host from the network 10.229.*.* to access the **ftp** service of your Windows host EXCEPT for connections coming from hosts belonging to group X+1 (or group 1 if X=13) AND connections coming from hosts 10.229.100.96 and 10.229.96.*
- Allow any host from the network 10.229.*.* to access the **http** service of your Linux host EXCEPT for connections coming from hosts belonging to group X-1 (or group 13 if X=1) AND connections coming from hosts 10.229.100.97 and 10.229.97.*
- An http request that is arriving from a network outside of your group and is allowed access (as per the previous rule) should be able to access your web server regardless if it attempts to connect to port 80 or 8080. That is, to networks outside of your group your webserver appears to **also** be listening on port 80.
- Allow any host from the network 10.229.*.* to access the **tftp** service of your Linux host EXCEPT for connections coming from hosts belong to group X+2 (or group 1 for X=12 and group 2 for X=13) AND connections coming from hosts 10.229.100.96 and 10.229.96.*
- Allow any host from any network to connect to the **ssh** service port on any of your group's hosts as well as allow ICMP echo messages and responses (pings) from any host from any network.
- It is implied that all hosts within your group's network should be allowed complete access to your group's hosts.
- If none of the above rules apply, the default is to refuse all other inbound traffic (that is, unless the inbound traffic is caused by your own group's permitted outbound traffic).
- Log violations of the above rules.

Outbound restrictions:

- Prohibit your Windows host from accessing any services provided by the hosts belonging to group X+1 (1 if X=13) and all services provided by hosts 10.229.100.96 and 10.229.96.*
- Log any violations of the above restriction.

Deliverables are the firewall rules you used for the implementation of the above policy. Provide comments that explain the rules you used and why you needed each rule. Also, your ftp server and firewall setup should be configured such that it is capable to work correctly in **both** passive and active modes.

Important: your firewall rules will be tested and marked for strict adherence to the policy as well as for brevity. Rule correctness includes, for example, the ability to allow inbound traffic (as the reverse flow) for a connection that was allowed in the outbound direction, i.e., do not forget that TCP connections are bidirectional. You are expected to release all relevant credentials (e.g., password to your hosts) to the TAs in order for them to accurately test your firewall rules.

Even though we do not talk about UDP services, they should be treated in a manner compatible with the spirit of the above rules. In presenting the rules you decided to use for UDP explain why you thought they are compatible with the provided policy.

It is recommended that you coordinate among groups to have other groups attempt connections (or for you to attempt connections to other groups) so you can check whether your rules are correct. However it is PROHIBITED to share rule files with other groups or to give your passwords to other groups for the sake of logging into your machines.

Your Own Certificate Authority (30%) [sliding part]

From the earlier part of the assignment, you have set up an http server on your virtual Windows host. You will now add an https service which means you will have to add a certificate for the https server, to enable encrypted access to it. The problem is you do not have the luxury for a Certificate Authority to sign your public key. So, you will become your own Certificate Authority. It is recommended that you read about **`openssl`** and how you can use it to generate private keys, etc.

1. Each group will create its own public/private key pair (at least 1024 bit long private key) and create a self-signed certificate. The certificate's organization name should be "GroupXX_F16" where XX is your group number. [Your .crt and .key files are to be submitted as part of the deliverables, as well as the password used to encrypt your private key. Note that you will have files for both your own CA as well as, in the next steps, for the server certificate. All of those files need to be submitted as part of the deliverables.]
2. Generate a certificate request where the organization name is "GroupXX_F16 Web Services" (again XX is your group's number). [The certificate request .csr and the .key file is part of the deliverables.]
3. Sign the certificate request with your "CA" private key. The policy should be set to **`policy_anything`**. [You will have at this point a .crt file which is also part of the deliverables.] In your writeup explain what would have been the impact if the policy was not set to **`policy_anything`**.
4. The next steps require that you configure your web server to use the "GroupXX_F16 Web Services" certificate that was just signed. Describe how you accomplished this step.
5. Use the web browser on the virtual Windows host to access your web server. Verify that it does not recognize the certificate authority that signed the certificate [For the deliverables, take a screenshot of this behavior.]. Show how to convert the self-signed certificate that you have produced into a format understandable by your browser and incorporate it (load it into the browser). Try again to access your server's content and show that it is now successful. [For the deliverables, take a screenshot of this behavior.] The above may sound simple but they have to be performed in the right order and with due care for details. In your report explain what are the different file types you encountered and what is each type used for and why it is needed. Outline any problems you encountered trying to achieve your goal. After you have completed this task:
6. Find how you can use your new power as 'Certificate Authority' to sign code, and in particular Java jar files. Write up the process of how to generate signed Java code and explain what is the purpose of each step (emphasizing the 'why' each step is needed). What (if any) are the differences with respect to the web server certificates? [You do not need to sign any code – this part of the task is mostly a reading exercise – but going through the steps using some example code and the appropriate tools could help you understand the process better.]

Deliverables

Only one of the group members need to submit on behalf of the entire. The sliding part can be submitted at any point in time prior to the deadline for Assignment 3. Your report should include answers to the questions posed in this assignment and should cite any resources that you used to answer the questions. It is recommended that you provide your report in pdf format because you need to include non-textual visual content, e.g. screenshots. It is assumed that all group members equally contribute to the assignment but you have to provide a paragraph in your report which explains how you split the workload. If you need to deviate from this model (“all equally contributing”) of cooperation, explain why and indicate who/what was responsible for what.

[Optional: add a single paragraph at the end of the report indicating whether you found any difficulties with this assignment and if you think there are ways in which it could be improved. In particular, we are interested to know if the assignment forced you to learn something new that you did not know of before, and how much effort it took you. Was the workload reasonable?]

****