IT Security, Assignment 2
Firewalls and passwords

DIKU, block 4, May 12 2014

You're still an IT security consultant, and you've done such a good job BIOchem is still requesting your services.

1 Network segmentation

The internal servers at BIOchem are placed on the same network segment as the workstations. This is undesirable, and it has been decided to split the internal network into two parts by introducing a new firewall (fig. 1).

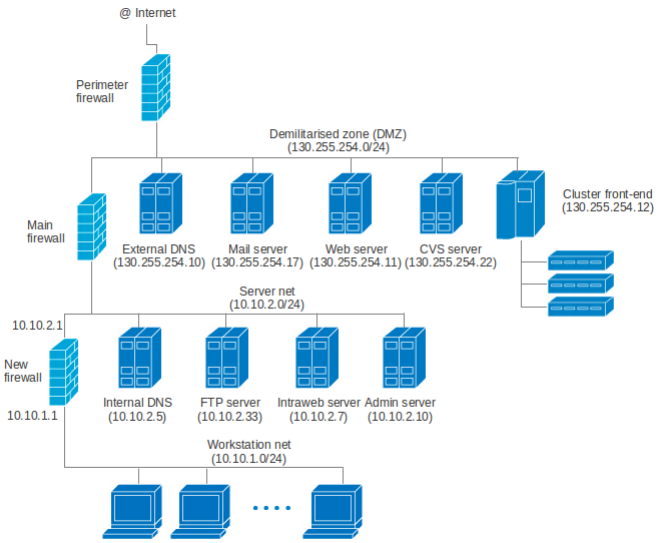

Figure 1: Part of BIOchem' network, with the new firewall.

The new firewall has two interfaces with IP addresses allocated as shown in figure 1. All IP addresses shown are static.

Argument for such a separation of the servers and the workstations, and suggest a set of firewall rules for the new firewall using the firewall rule specification language `iptables`, in order to enforce the following policies:

1.1. DNS lookups from the workstation net are allowed and should be dealt with by the internal DNS server.

1.2. HTTP and HTTPS communication initiated from the workstation net to either the intraweb server or web servers on the internet is allowed.

1.3. Users on the workstation net are allowed to send mail by sending it to the mail server which forwards mails to both internal and external recipients. And the users are allowed to fetch mail sent to them by connecting to the mail server using POP over SSL.

1.4. Users on the workstation net are allowed to send calculations to the cluster by logging on the front-end using SSH and uploading and downloading files with the secure copy feature of SSH.

1.5. Users on the workstation net are also allowed to connect to the FTP server and upload/download files.

1.6. The admin server is allowed to test the integrity of the workstation net by `ping`'ing it and to connect to the new firewall using SSH.

For `iptables` syntax, consult the `man` pages or find a suitable tutorial on the internet. A reference for port number assignments is http://iana.org/assignments/port-numbers. Enclose with your solution a commented shell script containing the appropriate sequence of `iptables` commands and any other necessary shell commands. Testing the rule set is *not* a requirement. A sample shell script is available on Absalon.

2 Compromise of the cluster front-end?

The DMZ contains a front-end giving access to a large computer cluster which the company's scientist use for computer simulations. Users log on to the front-end using SSH, either from the internal net or when working

from home, and upload calculations or download subsequent results with the secure copy feature of SSH.

While reviewing logs the admin of the front-end suspects it may have been compromised. Analysing the relevant excerpt of the front-end's audit log you concur. Get a copy of the excerpt on Absalon and try do determine how the breach occurred. What user account(s) were compromised? Make a proposal for how to avoid—or reduce the effect of—similar attacks in the future. How could you leverage `iptables` to that end? You suspect the THC Hydra tool might have been used in the attack. Reflect on how the attack could have been carried out differently in order to complicate your analysis. What, if any, effect would those changes have on other avenues of detection?

3 Cracking SAM

Speaking of authentication, you decide to review BIOchem's password policy for its Windows-based workstations (figure 2).

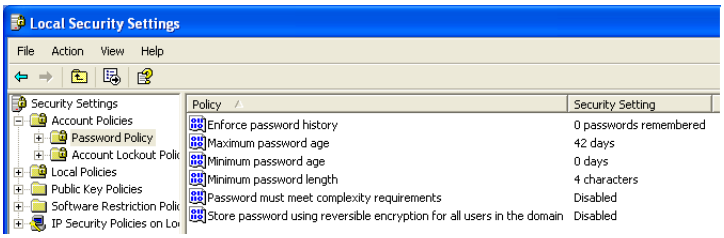

Figure 2: BIOchem's workstation password policy.

Copying out the Security Accounts Manager (SAM) file of one of the workstations, with, say, `pwdump7`, you want to show this policy is insecure. Try to crack the passwords stored in the SAM. Suggest ways to improve the password policy. What, if anything, should you ensure before and after such password audits? (Get a copy of the SAM on Absalon.)

Note: You do not need to program or script a utility to find the passwords youself. You may research and use existing tools. You should provide a brief explanation of how the tool you choose work and document your steps used to crack the passwords. As always be sure to clearly mark work included in your solution that is not your own personal work and make a reference to its source.

General requirements

There are 3 assignments during the course, intended to give you hands-on experience in how to analyse information security risks, implement (parts of) security systems, break such systems, analyse attacks and provide recommendations to prevent future similar attacks.

Your solution to each assignment should be documented in a short report. Your report may follow the usual structure for scientific reports, starting with a summary followed by a description of the problem and the solution and finishing with a conclusion and a list of references.

Reports must be submitted in PDF format via Absalon no later than two weeks after the assignment in question is posted. Reports are graded as 'pass' or 'no-pass'. Resubmissions are allowed once per assignment. You must pass all assignments to sit in for the exam.

Limited written feedback is given via Absalon. Additional feedback may be given at exercise classes.

You should keep your hand-in as short and precise as possible. If you are in doubt about the interpretation of some of the requirements, or feel it necessary to make some assumptions, you should explain what you did and why. Be sure to clearly mark work included in your solution that is not your own personal work and make a reference to its source.

You may solve the assignmets in groups of 1-3 students. The first page of your report must contain the assignment number, your name and the name of any other group members.