1 Introduction

This exercise continues the theme of the first two exercises. The big differences? Your web servers will now feature fully configured web applications, including back-end databases. The attackers will now try not only to gain access to your systems, but also to your data. If they can get the customer data out of your web applications, then ...

On the good side, you now have access to a fully featured firewall system that will allow you to create virtual private networks for your internal system where they can be protected.

In this exercise, you have just been tasked with building the computer network infrastructure for a new company. The company is divided into two groups- the sales staff, the IT group (that includes you!), and of course the CEO.

You will need to correctly set up the network, then determine how other teams set up their networks, attacking them if you wish. You need to maintain your network, in the face of use and attacks from the other teams over two nights of live use, scheduled for May 13 and May 15. When the exercise completes, you will need to determine what happened on your network, including if and how your systems were compromised. These results will be included in a single team report that is due at 5:30 p.m. on May 20. That report my be submitted electronically. If you do, please do not assume that the report has been received until you receive an acknowledgment from me. With large files, failing email accounts and other surprises, make allowance for the possibility that the file you sent never arrives to be graded.

1.0.1 Timing

Note that the second day of the exercise on May 15 will be held during our scheduled final exam, from 5:30 - 7:30.

2 Exercise Design

The network is built in two parts. The headquarters, or corporate group has a DNS server to resolve external names to the corporate network; it also has an Active Directory domain controller and a Windows file server for the workstations in the corporate network. For simplicity, there are only two such workstations; let’s agree to pretend that there are plenty more where those came from. Also in the corporate network is a Joomla web server together with a back end database, and a Snort Report system, together with its back-end database and a sensor. This comes together with a Splunk log monitoring system.

The sales group is essentially the same, but instead of having a Snort report system, it instead has a Zen Cart sales web site.

To this network, you must add additional systems as you see fit. For example, where are the sensors that will feed the data into the Snort Report?

You are required to develop an appropriate IPFire firewall architecture to protect these systems. This architecture should include one or more internal networks and one or more DMZ networks.

If you wish you can set up a single internal network and a single DMZ network, and connect these via VPN tunnels. Instead, you could construct a pair of internal networks- one internal for the corporate network and one internal network for the sales network; in the same way you may set up one DMZ for the corporate network and one DMZ for the sales network. Regardless of the final architecture, your network must use at least one VPN.

Though it is possible to use IPFire and NAT to set up multiple external IP addresses to point to a single internal host, each listed system on the team sheet must be a separate system.

Not every system needs to be behind a firewall.

Otherwise, the internal structure of your network is up to you.

2.1 Systems & Services

Details of the network, including the required host names, IP addresses, and other details are provided in a separate spreadsheet. This sheet provides information about your network from an external point of view. You can implement this external structure in a wide variety of ways at your discretion.
• The external DNS servers are running BIND, and must be able to resolve any external hostname or address in your network. To be clear, this includes both the headquarters network and the sales network! These systems can be built from any provided Linux distribution.

• Requests of your DNS system for any name outside your namespace or any address outside your address space should be forwarded to Exercise Control at 10.0.2.250.

• You can set up one domain for your entire organization, or two domains (one for the corporate network and one for the sales network) at your discretion.

• You will likely need DNS for your internal and DMZ network. Feel free to either build additional systems or use the BIND or Active Directory systems. You can use any naming scheme and any addressing scheme you wish.

• The file servers must provide a single common shared directory for all corporate users, a single common shared directory for all sales users, and individual private directories for all users. The CEO needs access to both common shared directories as well as an individual directory.
  – Note that the shared directories only need to be shared internally, not across the external network.
  – Systems on the local network should be able to access these shares at
    * \SalesFiles\Share
    * \CorpFiles\Share
    * \HomeFiles\Username
    You will likely need to be somewhat creative with your host naming scheme to make this work.
  – These may be checked via Nagios. If so, it will be done by Nagios logging into a Windows or Linux workstation, and executing an appropriate check.

• The Joomla systems must be fully functional.
  – Install the sample data set
  – The location of each web site is indicated on the setup sheet.
  – The setup sheet provides the admin user name and admin password.
  – The integrity of the web site will be checked.

• Each database system must be configured as follows:
  – Create a database, named “ExerciseControl”.
  – This database should have one table: “Signature”.
  – This Table should have one field: “Key” (a 16 character key).
  – The Key field should have as value the key included on the Team Set Up Sheet.
  – The user lmollari should have access to the database, from any host, with the password provided on the Team Set Up Sheet.
  – The user zathras should have all privileges on the ExerciseControl database.
  – Note that not all databases need to be accessible from the external network. Checks of the database may be made by exercise control first logging in locally or to another internal system before the check.

• The SnortReport system should be connected to an appropriate suite of sensors that cover the entire network, both corporate and sales.
  – The data should be appropriately protected.
  – Access to the data should be granted only to domain administrators.

• The ZenCart systems must be fully functional.
  – The shop should be located at http://shop.teamx.tu; be sure your DNS can handle this.
  – The location of the shop’s admin page is specified; it will be at http://shop.teamx.tu/yyyyyy for some string “yyyyyy”.
  – The user and password for the admin page are specified.
  – Be sure to install the sample shop; it will be checked for integrity.
  – Data for 10 Zen Cart shoppers are provided, including passwords. Each such shopper should complete at least one order.
• Systems listed as running an SSH server must allow password authentication to the system.
• The log monitors must receive the logs from all of the required systems in that component of the network (Corporate or Sales).
• Times should be synchronized across your network. Exercise Control (see below) will provide a time server for your use.
• A fully functional web application firewall should be set up in front of each web server.
  – Create a custom rule for each web application firewall. If the string “shibboleth” appears in a web request, either in GET or POST data, then the request should be blocked and a 503 error returned.
  – Proper function of this rule may be checked via Exercise Control.
• Snort sensors must be configured with a custom rule for each Snort system should be built that fires off an alert whenever the text “lollapalooza” appears in a packet.
• Note that, though separate /24’s have been reserved for the external addresses for your corporate and sales network, you are free to use the entire /16. As an example, the external address for an IPFire system does not need to be on either of the specified /24’s.

2.2 Defensive Techniques

You may want to harden your systems to make it more difficult for attackers.

2.2.1 Firewall Rules

You may use whatever firewall rules you wish on your IPFire systems. However, you are responsible for the result, so if Nagios cannot reach your system because of your firewall rule settings, then the problem falls on your team.

Blocks on traffic must block all IP addresses or none. You cannot block inbound traffic based on the source IP address or membership in a windows domain. These rules on blocking inbound traffic also apply to other tools, like hosts.allow and hosts.deny.

Though you can configure IPFire to block outbound connections, you may not block all ports. In particular, the following ports must always open for outbound traffic to arbitrary IP addresses:

- TCP / 20
- TCP / 21
- TCP / 22
- UDP / 53
- TCP / 80
- TCP / 110
- UDP / 123
- TCP / 143
- TCP / 443
- TCP / 989
- TCP / 990
- TCP / 993
- TCP / 995

At least you can block TCP / 4444 if you wish.

All systems on the Team Setup Sheet must respond to pings to their external address. Note that this does not include the IPFire systems themselves.

Countermeasures The rules against blocking connections by IP address can be relaxed. If a team can provide compelling evidence of an attack more threatening than a simple port scan to the instructor from a known IP address, then the team may receive permission from the instructor to block communication to and/or from that IP address.

2.2.2 Local Policies, Group Policies, and Software Restrictions

The use of Group Policies or Local Policies to secure systems is encouraged. However all users must have the right to

- Visit arbitrary web pages.
• Run any already installed program; this includes web browsers, command shells, Java, Adobe Reader, and Adobe Flash.
  – Blocking network connections to/from these programs or otherwise interfering in how they run is not permitted.
  – The requirement to run already installed programs excludes programs solely for system administration like regedit.exe.
• Download and run any program that does not require elevated privileges.

You may also set up and use Software Restriction Policies or AppLocker.

Note: Software Restriction Policies and AppLocker restrict where programs can be run; they cannot be used to block all downloaded programs. Moreover, we assume that the user is smart enough to know where programs can be placed to run. If you receive an email asking you to download and run a program, your settings must allow the user to do just that.

2.3 Users

The actual users you are to use has been provided in a spreadsheet, together with the passwords that they are to use. Given a user, form the user name as the first letter of the first name followed by the full last name, all in lower case. For example, the user Londo Mollari should have the user name lmollari.

There are four groups of users

• The CEO
• IT Admins
• IT Staff
• Sales Staff

The following rules are in effect:

• The CEO must be able to log on to the CEO workstation, as well as the Sales workstations.
• The IT Admins must be able to log on to any system. They should also be domain admins.
• The IT Staff must be able to log on to any system.
• The Sales staff must be able to log on to any Sales workstation.

There are many possible architectures that satisfy these requirements; you are free to choose how to ensure the requirements are met.

You may set up other accounts as you see fit.

Service checks that use account / password combinations will not specify the domain. The only exception are Windows specific services, like RDP and File Sharing.

2.3.1 Passwords

The passwords on your systems are selected from a finite (and small) list of allowable passwords. This restriction makes brute-force attacks on your passwords feasible in the time allotted for the exercise.

If you set up additional accounts beyond those required for the exercise, they must use one of these passwords.

2.4 Exercise Control

A system is provided by the instructor for exercise control; it is named babylon5.classex.tu, and is located at 10.0.6.250.

• Exercise control provides a DNS server (TCP/53, UDP/53) for the classex.tu namespace and the 10.0.6.0/24 address space. You may set your forwarders to it if you wish.
• Exercise control will forward requests for all class domains and IP address spaces that belong to a team to a DNS server for that team.
• Exercise control will be providing an NTP server (UDP/123) that can (and should) be used to synchronize the times on your systems.
• Exercise control will be running a Nagios server. This tool will check to see what hosts are up and responsive and what services they are providing. This information will be used for grading.
– Service checks will be different for different services. Some may check that a service is listening, others may authenticate to the service, and others may verify the integrity of the data.
– Authentication for service checks may use the credentials provided to you and your team.
  * Systems that are running SSH must provide an additional non-root account named “nagios” with full login privileges. [Don’t set the shell to /bin/nologin or the equivalent!].
  * Windows domains and windows systems must provide a non-administrator account named “nagios”.
  * The password for the user nagios is included on your setup sheet.
  * SSH authentication for the nagios user may also take place via public key encryption. The public key for the nagios user will be provided on exercise control.
  * The “nagios” user should have the privileges and restrictions of a user in the sales domain. Thus, they should have access to the file share in the same fashion.
– Service check failures can occur for any number of reasons, sometimes unrelated to the service being checked. For example, if SSH is being checked on host.teamx.tu and your DNS server does not have the correct record for host.teamx.tu, then the service check will fail.
– It is your responsibility to ensure that all service checks are passed. This is a key component of the exercise!

• Exercise control system will provide in-class email.
  – Each team will have two email accounts, one (teamxadmin@classex.tu) will be used for communication with other teams and with Red Team. The second (teamxnagios@classex.tu) will receive all warnings and alerts from the Nagios server that is checking your network.
  – Team email can be checked from a webmail interface (babylon5.classex.tu/mail). Exercise control also provides IMAP (TCP/143, TCP/993) and POP3 (TCP/110, TCP/995) servers, with and without SSL to receive mail. Exercise control provides authenticated SMTP with SSL (TCP/25) for the sending of mail. The Thunderbird e-mail clients or Evolution e-mail clients on your systems can easily be configured to read and send email.
  – Email account passwords are provided on the setup sheet.
  – Email for the class instructor should be sent to lmollari@classex.tu

• Exercise control provides an SSH server. You may log into Exercise control to get a view of your network from outside your network. However, Exercise control cannot be used to to launch attacks or scans.

• Exercise control provides a web site (http://babylon5.classex.tu) with the latest and most up to date information about the services provided by exercise control. That site will include
  – The public certificate for the CA that was used to sign all SSL certificates used by exercise control (e.g. https, IMAP/SSL, POP3/SSL, SMTP/SSL). It is recommended that you import this certificate into your clients (browsers, email clients) as appropriate.
  – The fingerprint for the SSH server provided by exercise control.
  – The SSH public key for the user “nagios” that may be used for service checks.
  – The list of all possible passwords used for systems other than those on/or for exercise control.

• Exercise control will provide the game “My Little Pwny”. Red team members who are able to successfully compromise a system have the option of recording their success with this game. It will provide a (partial) list of the systems that Red team was able to compromise.

2.5 Deadlines & Documentation
• Your network must be complete and functional prior to the start of the exercise at 5:00 on May 13.
• As part of the report, each student must indicate which systems that they set up. Each student must set up two or three required systems, and at least one must be a server (i.e. not a workstation).

3 Exercise Instructions
Your primary role here is defensive. Red Team has been given a number of tasks, but their primary task is to dump the customer database from your shop. If they succeed at dumping the database without your knowledge, you will suffer a significant grade deduction.
Your job on offense is to determine as much information as possible about the structure of the networks of your opposing teams.

- Create a network map that indicates the IP addresses used by the team. Ideally, you want information about both the external and the internal structure of their network.
- For each host, attempt to determine the OS version.
- For each service provided by a host, attempt to determine the version.
- Attempt to determine as many valid usernames as possible.

You are free to engage in offensive activity, however it should be cleared with Prof. O’Leary to make sure that it does not interfere with the learning environment. Attacks on the opponents’ data (as opposed to their hosts) is encouraged. Can you modify a team’s web site?

Team 1 will occupy the 10.1.0.0/16 subnet, with team 2 on 10.2.0.0/16 and team 3 on 10.3.0.0/16. Other network addresses are to be considered out-of-bounds for attacks. The only valid systems on the 10.0.0.0/24 subnet are physical hosts. The 10.0.6.0/24 network is reserved for exercise control. Red team may occupy other addresses in the 10.0.0.0/8 subnet. No, I won’t tell you where, but don’t worry- I am sure Red team will let you know soon enough.

3.1 E-Mail

You may use the email system to aid your attacks. In particular, you can send an email (cc’d to lmollari@classex.tu) to another team asking either the CEO, a member of the IT staff (NOT IT Admins) or a member of the sales staff them to either

- Visit a provided web site
- Open a provided file, or
- Run a provided program.

The email may specify a particular host on which this is to occur, and may specify a particular program to open the web site.

The team receiving the email must perform the indicated actions. Once the indicated action is performed, the requesting team must be notified by email that their request has been fulfilled. If the named user does not have the privileges to log on to the named system, or if the named program does not exist on the system, or if the named host or named user does not exist, a simple reply stating these facts must be sent back to the requester. If the request asks for a program to be run, and the program crashes, the crash does not need to be reported back to the requester, only that the program was run.

Regardless, a return email is required, and should be cc’d to lmollari@classex.tu.

The receiver may not deliberately re-set, re-start or re-boot a system just because another team asked it to perform an action via email.

3.2 Records

During the exercise, you must keep a careful record of what activity you perform on the network. This includes detailed summaries of all scans, probes, and attacks. This information should be included in a table or tables in your final report.

Failure to do so will result in a significant grade penalty. You have been warned.

4 After the Exercise

Your report should describe the actions taken by the other teams, including answering the following questions:

- How well did your shop perform? Were customers able to place orders?
- Was your shop attacked? Were the attacks successful?
- Did your team experience a data breach? In particular, were other teams able to exfiltrate data about your customers?
- Did your Joomla sites function correctly?
- Did anyone access your Joomla site without proper credentials?
- Were you attacked in other ways?
• Were any of these other attacks successful? How could you tell?
• For any attack (successful or otherwise), can you determine who launched the attack? What evidence do you have to suppose the claim?
• How well did your logging infrastructure perform?

The report must do a good job explaining your network, both its external and its internal structure. Graphs and/or tables are likely a necessity.

The report must also specify the responsibilities and activities of each team member in reasonable detail.

5 Grading

Your report will be graded out of 25 points. Points will be awarded for the following:

• 5 points for the overall written quality of your report.
• 5 points for the actions you took to prepare your network.
• 5 points for the reconnaissance and attack activities you took during the exercise
• 10 points for your analysis of what took place on your own network.

The report of the responsibilities and activities of each team member will be used together with the report grade to assign the final grade for each student. If, in the judgment of the instructor different team members made substantially different contributions, then members of the team may be assigned different grades.