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 credit card 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 three groups- a sales staff, a production group, an 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 14 and May 16. 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 by 5:30 on Tuesday May 21. 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 16 will be held during our scheduled final exam, from 5:30 - 7:30.

2 Network Structure

The external structure of your network is provided on the individual team handout. This will be verified via Nagios checks.

You are required to develop an appropriate IPFire firewall architecture to protect these systems. This must include a VPN for your internal network, and a VPN for your DMZ network. You can divide the systems across the physical hosts as you see fit, and you can select which system(s) belong in the internal network and which belong in the DMZ. You can also put hosts outside the firewall if you wish.

I recommend (but do not require) that the external DNS systems be placed outside the firewall and that they contain only external DNS entries. This greatly aids in the initial setup of the network. You may place the domain controllers inside the firewall and use their DNS systems to record your internal IP addresses. You can put all of your systems on a single domain, or you can use separate domains for your internal and DMZ network, as you see fit.

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. I know that there are, (for example) two different hostname / external IP addresses for a Linux web server, however you are not allowed to configure your firewall so that they point to the same internal host in an attempt to reduce your overall build size. Nice try though.

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

2.0.2 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.

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.

If you end up breaking your own network because of your restrictive outbound firewall rule sets, I will chuckle, point to the section in the notes where I explained how this problem has bitten me on more than one occasion, how I don’t recommend it, and grab my red pen.

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.

2.0.3 Time Servers
Your VPNs will be using IPSec, and as you know IPSec is sensitive to variations in time settings. It is highly recommended that you set up one or more systems to act as time servers for your network; I would take a long look over at those external DNS servers, and think about setting them up as NTP servers as well.

2.0.4 Remote Access
When remote access is specified to a system, this means that any user (IT Staff, CEO, Sales, or Production) can access the named resource with their account name password from any external system. Exceptions to this rule will be noted.

2.1 Systems & Services
• The Primary and Secondary DNS servers are running BIND, and must be able to resolve the external hostname or external address for any system in your network. They can be developed from any of the provided Linux images. Both forward and reverse lookups may be checked. These systems are also running SSH.
• The internal domain controllers can be set up on a single domain, two domains, or three domains as you see fit. They can lie on the internal network, the DMZ, or both, at your discretion. You may set up one or more organizational units (OUs) as you see fit. These systems are not required to provide active directory or DNS to the public; these services can be blocked at the firewall. The only external service they must provide is RDP.
• Similarly, the Windows file server should provide individual file shares for each user on your network and a single file share that is in common to all company users. These file shares do not need to be exported to the public however, and only need to be visible to the workstations on the internal network. The only required external service the file server must provide is RDP.
• Two web servers are to be set up as “corporate information”. These should have the following components:
  – The external URL www.teamx.tu should resolve to one of these servers.
  – The external URL www2.teamx.tu should resolve to the other of these servers.
  – Each should contain a generic information page that describes your company; that page should also contain hyperlinks to each of the four Zen Cart shops, as well as the public certificate for all of your team’s SSL connections.
  – These sites should contain a protected web folder; this page should be accessible to all company employees. This page should contain generic corporation sensitive information. If another team gains access to this data, it will be considered a (very) successful attack.

These systems will provide external access either via SSH or RDP as indicated.
• Four Zen Cart shops will be set up; each will connect to a different MySQL instance.
  – Shop #1 stores its results on Database #1 and so on.
  – No single student can set up more than one Zen Cart shop.
– No single student can set up more than one shop database.
– The Zen Cart hosts and the database hosts provide remote access via SSH or RDP as indicated.
– The databases must allow remote access.
  * 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 seldon should have access to the database, from any host, with the password provided on the Team Set Up Sheet.
  * The user seldon should have all privileges on the ExerciseControl database.
  * Access to another team’s ExerciseControl Key will be considered a (very) successful attack.
– The Zen Cart shops should be (lightly) customized.
– The Zen Cart shops should be pre-populated with 10 customers and 10 orders. If another team gains access to this data, it will be considered a (very) successful attack.

• Each team must set up and run a suite of intrusion detection sensors appropriate for their network.
  – All of the intrusion detection systems must report their results to the same database.
  – A single instance of Snort Report must be able to access the alerts generated by any intrusion detection sensor.
  – The Snort Report interface does not need to be externally accessible.
  – The intrusion detection database does not need to be externally accessible.
  – Both the Snort Report host and the Snort Report database host must allow remote SSH access.
• The workstations are standard, and must allow SSH or RDP access as appropriate. No Vista. You may replace one Windows 7 machine with an XP image if you wish.
• The Linux workstations for the IT staff can be developed from any Linux image save for the Ubuntu Server. They must be running SSH and allow password authentication.
  – The CEO workstation only needs to be accessible to the CEO and the IT Staff.
  – The IT workstations only need to be accessible to the IT Staff.
  – The Sales workstations only need to be accessible to the Sales Staff and the IT Staff.
  – The Production workstations only need to be accessible to the Production Staff and the IT Staff.
• You must set up a single log server for your network. It need not be publicly accessible. You may set up additional logging servers at your discretion.

Details of the network, including the required host names, IP addresses, and other details are provided in a spreadsheet.

2.2 Users
The actual user names you are to use has been provided in a spreadsheet, together with the passwords that they are to use.
There are four groups of users
• The CEO
• The IT Staff
• The Sales Staff
• The Production Staff

You may set up other accounts as you see fit. They can use any password from the list provided on the labshare.

2.3 Exercise Control
A system is provided by the instructor for exercise control; it is named trantor.cosc.tu, and is located at 10.0.2.100.

• The exercise control system provides a DNS server for the cosc.tu namespace and the 10.0.2.0/24 address space. You may set your forwarders to it if you wish.
The exercise control system will be checking your network to determine which systems are up and responsive, and which are not. This information will be used for grading. The exercise control system will be providing a mail server; it can be accessed via the web at trantor.cosc.tu/mail. Your team has a single account, named team1, team2, team3, or team4 as appropriate. The password to the mail system is provided on the spreadsheet. The system account for exercise control information is seldon@cosc.tu; you may send exercise requests to that address.

### 2.4 SSH Keys
To assist exercise control to determine which systems are up and running, all systems that are running SSH must provide a non-root account named “seldon”. Remote SSH access to this account must be permitted, via public key authentication. The public key is provided on the Exercise Control system.

### 2.5 Deadlines & Documentation
- Your network must be complete and functional prior to the start of the exercise at 5:00 on May 14.
- As part of the report, each student must indicate which systems that they set up. Each student must set up three or more systems from the Team Set Up Sheet, and at least two must be servers (i.e. not a workstation).
- Each student must set up an IPFire firewall.

### 2.6 Services
It is expected that all hosts are responsive and providing their required services. Systems that provide data, like Web servers and DNS servers will have their data checked for integrity. It is expected that the data these servers provide will not be altered from their required, correct state.

Penalties for down services or down hosts are significant. Having a system or a service down for one or two Nagios checks is a minor issue- this could be caused by network congestion, trouble with Nagios, or a problem with your system, and no significant penalty will be assessed. However a system or service that is consistently down for an extended period will result in a significant penalty.

### 3 Exercise Instructions
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 internal and external IP addresses used by the team.
- For each host, attempt to determine the OS version.
- For each service provided by a host, attempt to determine the version.

Attacks on the opponents’ data (as opposed to their hosts) is encouraged. Can you obtain and/or modify the data in their database? Can you steal their customer list or their credit card data? Can you craft a phishing email that will compromise their data?

Attacks on the underlying network infrastructure, like IP spoofing, ARP spoofing, and WPAD attacks are prohibited. Sorry. I like the thoughts, but it just causes too much network mayhem.

You are free to engage in any other offensive activity, however it should be cleared with Prof. O’Leary to make sure that it does not interfere with the learning environment.

Systems on the 10.0.0.0/24 subnet are physical hosts, and considered out-of-bounds for attacks, as is the exercise control system at 10.0.2.100. Other hosts may be deemed out-of-bounds. Hosts on the 10.0.3.0/24, 10.0.4.0/24, 10.0.5.0/24, and 10.0.6.0/24 networks will always be in-bounds.

Team 1 may use any address on 10.1.0.0/16, Team 2 on 10.2.0.0/16, Team 3 on 10.3.0.0/16, and Team 4 on 10.4.0.0/16.

### 3.1 E-Mail
You may use the email system to aid your attacks. In particular, you can send an email (cc’d to seldon@cosc.tu) to another team asking them to either

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

The team receiving the email must perform the indicated actions, provided they follow the rules set down. If there are questions, the receiving team should check with Prof. O’Leary. Once the action is taken, the team must reply to the sender (cc’d to seldon@cosc.tu) indicating that it has occurred.

Rules of the game:

• The receiver may not deliberately re-set, re-start or re-boot a system just because another team asked it to perform an action.
• The sender must specify the host on which the action is to be performed. If the host does not exist, the receiver can simply state that the action was performed without providing additional information.
• The sender may specify an account, or an account type (CEO, Sales, Production) to perform the action. Senders may not ask the IT staff to perform an action; presumably they are smart enough not to click on random links or run emailed programs. Regular users, well, that’s a different story. If the specific account does not exist, the receiver can simply state that the action was performed without providing additional information.

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.

A network diagram, indicating the internal and external IP addresses of each system on the network must be developed and included in the report. You are highly encouraged to share draft versions of this diagram with Dr. O’Leary well before the start of the exercise for comments and suggestions.

Prior to the start of the exercise on May 14, a complete Machine Information Sheet must be completed for each system on your network (required or optional). These sheets must be included in your final report. If a machine changes state (e.g., IP address) between May 14 and 16, this should be explained in the report, and separate sheets provided for each date.

4 After the Exercise

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

• How well did your shops perform? Were customers able to place orders?
• Were your shops attacked? Were the attacks successful?
• Did your team experience a data breach? In particular, were other teams able to exfiltrate data about your customers?
• 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 final report will be neat, organized, and well-written. It will contain:

• A copy of the Machine Information Sheet for each of your machines.
• A complete summary of all network activity your performed against other teams.
• An evaluation of the functioning of your network.
• The results of your reconnaissance as described above.
• The analysis of your logs, described above.

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.