Team: Devry

Inject Number: 1

Inject Duration: 15 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 08:32:51 -0800

From: E. Palpatine

To: Storm Trooper Bata'lion

Subject: Welcome to the Disaster

Welcome to our disaster recovery site. We need to establish what we have

Is all of your hardware powered on and have corresponding monitor, keyboard and mouse as appropriate for the platform?
Are your keyboards, mice and monitors working correctly?
Do we have network connectivity and internet access? Try browsing to Google or yahoo and take a screenshot of this external website to be submitted to this inject in the blue team portal.
Can you log into the inject portal at (https://10.0.0.5) Ask your manager for the user ID arid password if they have not provided it.
Does your phone work? Call the DRP architecture firm at 4111 or 9111.

Check access to the repository the **IP** is 10.0.0.11 and

10.0.0.12 There is no user name but the password is

"changeme"

Thank you.

E. Palpatine

Team: Devry

Inject Number: 2

Inject Duration: 72 Hours

Inject Start Daterrime: Sat, 10 Dec 2011 08:35:49 -0800

Prom: E. PaJpatine

To: Storm Trooper Batallion

Subject: INCIDENT REPORTING

When suspecting an incursion by the Red Team please submit an Incident Report as completely filled out as possible. Up to 50% of the points lost due to Red Team activity can be recouped from diligent and thorough reporting of known and suspected attacks.

URL fs:https://docs.google.comispreadsheetiviewform?
authkey=COWnp[41,3]&authkey=COWnp41J&h1=en_US&formkey=dHk5dXEzWTBXLU5MULJCTWIXM25KcOE6MA#gid=0

Thank you.

E. Pa*!patine*

Team: Devry

Inject Number: 3

Inject Duration: 90 Minutes

Inject Start Date!Time: Sat, 10 Dec 2011 08:36:31 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Inventory

The previous **IT** team did a poor job keeping the management informed on what the **IT** team was doing. As a result, we do not have a clear idea of what resources we currently have available. Please inventory every system: detail the hardware, the applications, the type of accounts they posess, and the services they offer. Provide summary report of all that you find.

Please keep the report updated to reflect changes to our network.

I think there is previous documentation available in our disaster recovery depository. Please start that documentation. We found it inadequate so we're expecting you to improve on it.

Thank you.

E. Pa/patine

Team: Devry

Inject Number: 5

Inject Duration: 90 Minutes

Inject Start DaterTime: Sat, 10 Dec 2011 09:09:47 -0800

From: E. Palpatine

To: Storm Trooper BataIlion

Subject: FTP Disaster Recovery

As you have found, your Debian FTP server (192.168.X.14) went through a failed disaster recovery. You have been provided re-installation media for that server, and you will receive the content media shortly. To restore this server to proper working order, please host the content on an anonymous FTP share. To fulfill the requirements of the Creative Commons license on these audio files, be sure to include the license agreement (LICENSE_AGREEMENT.TXT) in the same directory as the mp3 files within an hour of receiving the media.

Thank you.

E. Pa/patine

Team: Devry

Inject Number: 6

inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 09:15:26 -0800

From: E. Pa'patine

To: Storm Trooper Batallion

Subject: eCommerce Content Engine

I want your suggestion for a new e-commerce platform for either the Fedora, Debian or Windows 2008 box. Do the research and make your choice but provide justification for that choice. You'll need to present your decision before the Board in **1** hours. You'll have 5 minutes to present your ideas. Consider this your elevator pitch. Good luck!

Thank you.

E. Pa/patine

Team: Devry

Inject Number: 7

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 09:41:35 -0800

From: SEC Office of External Communications

To: Storm Trooper BataIlion

Subject: Install New Cisco 7912 **IF** Phone

Communications will be key to the restoration of the markets and consumer confidence. We have been swamped with requests for additional support from our teams. In order to accommodate this, I need for you to implement a new Cisco 7912 phone that is being delivered to you. Have this done in the next 30 min. please.

I will be expecting to reach you at "1x02" where "X" is your Team Number. And make sure that your Caller ID appropriately identifies you when you call out.

Please expect calls from SEC and Federal Agencies as well as Brokerage firms for service and customer requests. We have several inquiries about the status of our feeds and status as to our investigations. When the remote site comes back on line, you may also receive IT support requests from those analysts via IP Phone communications.

Stay Vigilant!

SCORING:
Place a call to Management at HQ (ext. 2011).

Management HQ will inform you if your caller ID is in place. And your Room Judge must come on the call to verify the your Team number.

If phone must be programmed by 12 noon on Friday the Black Team will be by to program your phone and there will be a fee.

Thank you.

SEC Office of External Communications

Team: Devry

Inject Number: 8

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 09:49:10 -0800

From: E. Pa'patine

To: Storm Trooper Batallion

Subject: Create NEW DNS server and NEW DNS entries

Please ensure that your DNS services on the CentOS server 192.168.X.15 are available. We will begin scoring them by 10:30.

The following entries need to be created/available on ALL DNS servers being scored (X.15, X.11):

deathstarad.thedeathstarlocal 192.168.X.11
kashyyyk.thedeathstar.local - 192.168.X.14
endor.thedeathstar.local - 192.168.X.15
hoth.thedeathstar.local 192.168.X.16
alderaan.thedeathstarlocal - 192.168.X.12

Thank you.

E, Palpatine

Team: Devry

Inject Number: 9

Inject Duration: 30 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 10:16:58 -0800

From: E. Palpatine

To: Storm Trooper Batailion

Subject: Configure NTP

We really need to have a consistent time on our network. All of our computers use whatever time that they feel like and we have noticed that each server we see has a different time.

Management Instructions:

You are to set up one main clock on the network that every machine will be reconfigured to get the time from. Please do this for all devices and machines and let us know when it is finished.

Provide screen shots including the command run to verify that the time is synced from all machines and devices and upload to the glue Team Portal.

Thank you.

E. Pa/patine

Team: Devry

Inject Number: 10

Inject Duration: 3 Hours

Inject Start Date/Time: Sat, 10 Dec 2011 10:19:11 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Network Management System

We need to have a way to know if services are up or down. The first step towards compliance is to have a network managment system monitoring all our services. Please install a network management system such as Nag los, OSSIM, etc. It needs to be accessable from the branch office. I would like to have this done in 5 hrs.

Thank you.

E. Palpatine

Team: Devry

Inject Number: 11

Inject Duration: 60 Minutes

Inject Start DaterTime: Sat, 10 Dec 2011 10:48:03 -0800

From: E. Palpatine

To: Storm Trooper BataIlion

Subject: Account Creations

The board has decided to hire an external firm to look over our business functions and make recommendations. I need new logon and email accounts created for the auditors so they can access our mail system and addresses lists. Their names are:

Dan Manson
Anna Carlin
Brandon Brown
James Schneider

The audit team will be working remotely for the next few days and we will be spared their meddling for now. BTW, I heard from upstairs that Mr. Schneider is a bit danger prone and lax with security. Keep an eye on network activity. Let me know if you see anything mysterious with these accounts.

Please add these new employees as well:
Joe Public
Aaron Jones
John Bailey

Get me their new email addresses, usernames and logon passwords in the next 30 minutes.

Thank you.

Team: Devry

Inject Number: 11

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 10:48:03 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Account Creations

The board has decided to hire an external firm to look over our business functions and make recommendations. I need new logon and email accounts created for the auditors so they can access our mail system and addresses lists. Their names are:

Dan Manson
Anna Carlin
Brandon Brown
James Schneider

The audit team will be working remotely for the next few days and we will be spared their meddling for now. BTW, I heard from upstairs that Mr. Schneider is a bit danger prone and lax with security. Keep an eye on network activity. Let me know if you see anything mysterious with these accounts.

Please add these new employees as well:
Joe Public
Aaron Jones
John Bailey

Get me their new email addresses, usernames and logon passwords in the next 30 minutes.

Thank you.

***E.** Palpatine*

Team: Devry

Inject Number: 12

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 10:49:00 -0800

From: E. Palpatine

To: Storm Trooper BataIlion

Subject: Secure IRC

We need to quickly implement a Secure IRC server for encrypted chat between our remote site and your data center. Please investigate options, implement, and provide an easy to understand user guide for client installation and use. Provide information for the users so that they know how to:

1. Login
2. Set their Username / Nickname
3. Send Private Messages
4. Logout

Please get this accomplished within the next hour!

Thank you.

E. Palpatine

Team: Devry

Inject Number: 13

Inject Duration: 60 Minutes

inject Start Date/Time: Sat, 10 Dec 2011 10:55:28 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Malicious Tool Removal

It's that time of year again - to satisfy the audit folks and comply with our own internal policies we need to scan all our systems for "hacker tools" and unlicensed software.

I need you to:
a.•€C Search every system for network scanning, password cracking,
and vulnerability assessment tools
dee Note who the software belongs to and where you found it (system, folder, etc)
"MC Prepare a report for me listing every system in the inventory, what tools you found on it (name and type), and what user the tool belonged to
&EC Remove those tools from all systems

I'm meeting with our audit group in 60 minutes so I'll need that report by then.

Upload your report(s) to the Blue Team Portal.

Thank you.

E. Palpatine

Team: Devry

Inject Number: 14

Inject Duration: 120 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 11:38:55 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Execute Vulnerability Scan

As part of ongoing security testing there is a need to know where the organization stands in terms of threat exposure, patching and configuration lockdown on servers and workstations. You are asked to provide a report based on security scanning both from a network perspective and from within the operating system.

The security audit scripts will be available **in** the disaster recovery repository. The Windows security audit scripts need to be run on the AD controller, And the Unix security audit scripts against all Linux systems.

Install Nmap on the Windows 7 workstation and perform an assessment of all servers and generate a composite report and save the data to a text file.

Upload the report(s) and the text file to the Blue Team Portal

This should to be completed in 2 hours.

Thank you.

E. Palpatine

Team: Devry

Inject Number: 15

Inject Duration: 90 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 11:44:11 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: AD Security Policies

Just got a memo from our independent auditors that they'll need to see copies of our IT policies during their next audit - the problem is we don't have any. I need you ensure that the domain GPO takes into account AD security best practices.

At a minimum well need the GPO that meets the NIST SP800-53 to apply to AD.
Example criteria is:
MC Enable domain level password complexity requirements
MO Enforce password history (at least 12 months)
'ACC Define a maximum password age (60 days)
AEC Define a minimum password length (8 characters)
&CO Rename the Administrator and Guest accounts
5.€C Enable the "Do Not Require CTRD-ALT+DEL" logon setting
a.'€e Create a legal disclaimer logon banner presented at login
Re Disable Administrative Shares
(HKEY LOCAL MACHINE\SYSTEM‘CurrentControlSet\Services\lanmanserver\parameters)

You will need to download and install the Group Policy Management Console; this will be needed to export the defined policy.

You are to save the generated HTML report from the Management Console and upload to the Blue Team Portal.

Resources:
Download and install Group Policy Management Console (http://www.microsoft.com/downloadsien/details.aspx?Pamily1D=Oa6d4c24-8thd-4b35-9272-dd3cbt81887&displaylang=en)

Thank you.

Team: Devry

inject Number: 16

Inject Duration: 60 Minutes

Inject Start Daterrime: Sat, 10 Dec 2011 11:44:57 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Wireless Hardening

We have had reports that the wireless hot spot has been a target for hackers. Please make a policy for "Guest" wireless use. In parallel to this, incorporate changes to our wireless environment that will allow users to access the wireless network but they will have to request credentials in order to do it. Type up a user guide for this so that it can be handed out to end users.

The wireless and user guide should be submitted via the portal in the next 60 min.

Thank you.

E. Palpatine

Team: Devry

Inject Number: 17

Inject Duration: 150 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 12:11:32 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: e-Commerce Prototype

Management is considering moving forward with your e-commerce recommendation. There is general discussion about getting a prototype site together to demo for stakeholders. We could need this in 2-3 hours to coincide with a scheduled board meeting. Were not sure this is going to happen but I will know more sometime after lunch.

Thank you.

E.

Palpatine

Team: Devry

Inject Number: 18

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 12:14:46 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: SHAl & MD5 Report

I have had some discussions recently with some of my colleagues at other companies and decided we need to do a better job establishing baselines for our systems. One of my colleagues told me a story about how an attacker got into their network and modified a bunch of their executables to perform malicious actions. To prevent that sort of thing from happening in our network I want you to create a SHAl and MD5 hash of every executable on every TheDeathStarlocal system. Make sure you do this in a manner so we can compare these to known good hashes and then run periodic checks in the future to make sure we catch when changes are made.

Please submit an electronic report of the SHAland MDS hashes in the next 60 minutes.

Thank you.

E. Pa/patine

Team: Devry

Inject Number: 19

Inject Duration: 10 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 12:51:06 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: e-Commerce Prototype Update

Due to ongoing security and hacking issues consuming our **IT** resources the Board has decided to scrap the e-Commerce prototype project.

No need to proceed any

further. Thank you.

E. Pa/patine

Team: Devry

Inject Number: 20

Inject Duration: 1 Hour

Inject Start Date/Time: Sat, 10 Dec 2011 12:51:34 -0800

From: E. Pa'patine

To: Storm Trooper Batallion

Subject: Traffic Monitoring

Management would like to know how much and what kind of traffic is on our network. We would like to install a product called NTOP implemented on one of the Linux machines. Please provide the IP address as well as port number, administration information and a report for evaluation. Include a graphic for Network Load Statistics

Please have this done within **1** hour.

Thank you.

E.

Pa/patine

Team: Devry

Inject Number: 21

inject Duration: 30 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 13:20:39 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Infrastructure Configuration Backup

Capture all of or your infrastructure's configuration files (Routers, Switchs, 84AP) and save it to a tftp server, ZIP or Archive these files and send them via the Blue Team Portal.

Please have this done within 30 minutes.

Thank you.

E. Palpatine

Team: Devry

Inject Number: 22

Inject Duration: 90 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 13:26:54 -0800

From: E. Pa[patine

To: Storm Trooper Batallion

Subject: Create Acceptable Use Policies

Just got a memo from our independent auditors that they'll need to see copies of our Acceptable Use policies during their next audit - the problem is we don't have any.

Management Instructions:

At a minimum we'll need the policies to cover acceptable use of the following:
MC Email
'ACC Internet usage

This should be no longer than 3 pages.

Thank you.

E. *Pa/patine*

Team: Devry

Inject Number: 23

Inject Duration: 1 Hour

Inject Start Date!Time: Sat, 10 Dec 2011 13:33:58 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: Install and Configure WireShark

As part of monitoring network performance there is a need of understanding where a problematic source of data is coming from. You are asked to provide a packet capture file for analysis.

Install WireShark on the Vista workstation and perform a packet capture of 1MB in size

Upload your capture file to the Blue Team Portal Page.

This should be completed in 1 hour.

Download and install WireShark (http://vwvvv.wireshark.org/download.html)

Thank you.

E.

Pa/patine

Team: Devry

Inject Number: 24

Inject Duration: 15 Minutes

Inject Start Date/Time: Sat, 10 Dec 2011 14:13:10

-0800 **From:** E. Palpatine

To: Storm Trooper Batallion

Subject: Password Update

Danger prone Schneider has lost his password.
Username: JIRSchneider
Please reset the password to: jschneider123*
Must be done in 15 minutes

Thank you.

E.

Pa/patine

Team: Devry

Inject Number: 25

Inject Duration: 60 Minutes

inject Start Date/Time: Sat, 10 Dec 2011 14:23:01 -0800

From: E. Palpatine

To: Storm Trooper Batallion

Subject: MD5 & SHAl Hash of all executables

You got this in Paper but we are putting in the engine for submissions.

IT Staff,

We are aware that you were busy yesterday but we really need you to do a MDS and SHAl to see what is compromised. Use gnunetcat 0.71 http://netcat.sourceforge.net/download.php take your MD5 and SHAl hash and run it through the team Cymru malware hash database. http://vvvwv.team-cymru.org/Services/MHR/

command: netcat hash.cymru.com 43‹ hashlist.txt > outputlist.txt

Please complete in 2 hrs

Thanks

If you have questions don't hesitate to call us

Thank you.

E. Palpatine