

Inject Scoring Engine 3.8

Traffic Policy Document

Inject Number: 6

Competition: WRCCDC Invitational 10/10/2015

From: IT Director

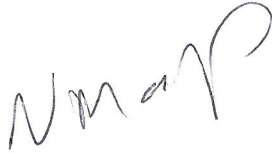
To: Infrastructure Support Group

Subject: Traffic Policy Document

The IT Director requires a document that contains a table of every machine in the company's network and the protocols and ports that should be available on those machines. Submit the completed document to IT Management (White Team)

Thank you.

IT Director



Inject General Information

Duration: 45 Minutes

Inject Start Date/Time: Sat, 10 Oct 2015 17:47:13 +0000

Status: Running

Inject Scoring Engine 3.8

Configure a Centralized Logging Server

Inject Number: 8

Competition: WRCCDC Invitational 10/10/2015

From: Security Ops

To: Infrastructure Team

Subject: Configure a Centralized Logging Server

Security policies require a centralized logging service to be used for auditing purposes.

Configure all networked and Linux devices to forward their logs to a central server. Use the 2008 AD Server to host the logging function

Provide screenshots of a sample of the composite logs

Provide screenshots of the logging configurations from all devices

Thank you.

Security Ops

Inject General Information

Duration: 90 Minutes

Inject Start Date/Time: Sat, 10 Oct 2015 18:05:31 +0000

Status: Running

Due 12:30

Inject Scoring Engine 3.8

Hardening of services

Submission Information

Team Name: Team 4

Inject Number: 9

Submission Name: Hardening of services

Submission Description:

Plan to harden

- 1) We will configure a Fire wall on the host server.
- 2) shut down all unnecessary services.
- 3) Audit configuration set up of current services
- 4) Install and update all anti virus.

Submission File Name: None

Submitted: Sat, 10 Oct 2015 18:32:06 +0000

Inject Scoring Engine 3.8

URL Blocking

Inject Number: 10

Competition: WRCCDC Invitational 10/10/2015

From: Management

To: IT Staff

Subject: URL Blocking

The CISO was walking through the company yesterday and noticed "a lot of employees" surfing the web.

Management Instructions:

You must block all outbound web access to:

- Twitter.com
- youtube.com
- wordpress.org

I'm meeting with our audit group in 60 minutes so I'll need that report by then. Your management memo should include a description of how you accomplished this on the firewall, and screen shots showing the implementation.

The White Team member will validate that they have been blocked.

Dillin
12:50

Thank you.

Management

Inject General Information

Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Oct 2015 19:00:39 +0000

Status: Running

Inject Scoring Engine 3.8

Configure Palo Alto SSL VPN

Inject Number: 16

Competition: WRCCDC Invitational 10/10/2015

From: CSO, CFO

To: IT Management

Subject: Configure Palo Alto SSL VPN

Management would like to have the accounting department to have remote access to the network. Configure SSL VPN on the Palo Alto Firewall for 3 users.; The users are Joe Soldier, Jimmy Kimmel, Colin Farrel

Test functionality of SSL VPN from Ubuntu workstation. Provide instructions for remote user on how to connect.

Also Include screen shots of the relevant changes.

Management

Thank you.

CSO, CFO

Inject General Information

Duration: 80 Minutes

Inject Start Date/Time: Sat, 10 Oct 2015 20:11:23 +0000

Status: Running

Due 2:20

Inject Scoring Engine 3.8

Implement Dos Protection Policies

Inject Number: 17

Competition: WRCCDC Invitational 10/10/2015

From: Sec Ops

To: Network Team

Subject: Implement Dos Protection Policies

The CEO read a report in Network World about how hackers often use DoS Attacks against major businesses.

Be sure your Palo Alto Firewall is configured with a defining Dos Protection Policy together with defining zone protection on the EXTERNAL zone.

Your deliverable is a report to the IT Director on how you accomplished this, with screen shots showing the policy and the zone protection dialogue box.

Thank you.

Sec Ops

Inject General Information

Duration: 60 Minutes

Inject Start Date/Time: Sat, 10 Oct 2015 20:28:30 +0000

Status: Running

Dillon
2:35