Inject #: 05

Category: High

Dear IT Staff,

I promised my good buddy Jeff over at The Big Huge Corporation that we'd help him out with a forensics investigation. You'll need to come see him to get your PIRCS USB drive and user's manuals. The forensics image you will be examining is a VM in a zip file on the portal (10.120.0.9 – look for the Exelis directory at http://10.120.0.9/Exelis/ and download the NCCDC_Windows_7_Pro_PIRCS.zip file). You will need VMWare Player to run this VM – it's on the portal. Give this your best effort – I don't want you embarrassing Warp Core.

Dave

From: Jeffrey Isherwood; Chief Information Security Officer (CISO)

To: IT Staff

Subject: Assessment of Special Purpose System

This morning, the Sharepoint administrators detected a connection from an unauthorized system utilizing credentials that belong to one of our sales engineers, Bob Durham. While connected to the sharepoint, the intruder accessed the schematics for the prototype Railgun Launch System (RLS) that we have been developing. The drawings accessed are from phase 2, and are actually flawed, however they may still give our competitors an advantage by allowing them to learn from past RLS mistakes. The Facility Security Officer (FSO) and her staff were notified immediately. When approached, Bob began to act strangely, and was seen disconnecting a laptop that was for sales work on the road and should never have been connected to our intranet. The FSO seized the laptop and escorted Bob to a conference room to be interviewed. He had no removable media on his person, nor were any found in his office. We believe that the data must still be on that laptop. He claims that he did nothing wrong and that any strange connections must mean that his system is infected with malware. He readily gave up the password for the laptop: Durham

This is not the first time that Bob has been questioned about strange data access that may have resulted in the leakage of corporate intellectual property. In each past case no proof could be found to indicate that he was in the wrong, but the last CISO warned me to be watchful of him. I need you to check out his system for any information that might help us prove that Bob is not acting in the company's best interest. Since you are not certified forensic examiners (I am working with the Board of Directors to get approval to get you certified) we need to proceed cautiously. Everything must be well documented so that if you do discover something amiss, we can use it to take action against him. Administrative Action would be to terminate Bob Durham's employment, Civil Action would allow us to sue him for loss of business or a Criminal Action might allow us to actually prosecute him for theft.

Inject #: 03

Category: High

From: David Tennant

To: IT Staff

Subject: Setup local wireless network

As you might have noticed, we're currently using an external provider for our wireless connectivity. Those tablets in our work area are connected to public provider and frankly I'm not comfortable with our traffic bouncing around the airwaves with other people's traffic. With some of our IT budget, I was able to secure some wireless equipment that will allow us to stand up our own internal wireless network!

Go ahead and start setting up the wireless equipment you have – there should be a Juniper WLC2 (Trapeze MXR-2) and a Juniper WLA522 (Trapeze MP-522) in your room still in their cardboard boxes. Look around and you'll find them. Use those to setup an internal wireless network inside your 10.X.X.0 subnet. Let's use 10.X.20.X and you'll need to NAT connections out of that network so they can connect to our internal network and the Internet. Once you have the wireless network setup, configure both tablets in your area to use your internal wireless network – get them off that public wireless as soon as possible.

Let's get this done ASAP!!

Thanks,

Dave

Competition Note: The equipment for this inject is in your room still in cardboard boxes. Look around your room for them – be sure to check the blue bins as well. You will need to keep this wireless network up and running for the length of the competition. Your internal wireless network will be used for as the primary connectivity for the tablets using during the competition.

Inject #: 08

Category: Medium

From: David Tennant

To: IT Staff

Subject: Data Classification and Protective Standard

It's occurred to me that Warp Core is lacking a data classification and protective standard – one of those documents that tells employees what data is "sensitive", "confidential", "proprietary" , and so on. By 6 PM today I need you to develop a data classification and protective standard for Warp Core. Develop and explain the categories of data, outline what data we currently have that falls into each category, and then outline the steps/protective measures we should be undertaking to ensure the safety of that data.

Thanks,

Dave

Inject #: 09

Category: Low

From: David Tennant

To: IT Staff

Subject: Infrastructure Change Proposal

I've heard some comments from a few of you about how messed up our network is. When you came on board we told you to secure and maintain the network but also asked you not to make any major changes (our CEO is very risk adverse) - but I'll give you a chance to state your case. By 6:30 PM today I want you to tell me what you could do to help secure the network immediately. What operating systems you'd like to change, what services you'd like to migrate from one application to another, what networking changes you'd like to make, and so on. Essentially what do you need to do (if anything) to further secure our network without spending any money on new equipment. Include a risk analysis for each proposed change along with possible mitigation strategies for those risks. Write this up in a proposal and be sure to tell me what you would change and how long you think it will take you to perform the actions in your proposal.

If you do a good enough job on this, you might be able to convince the CEO to let you make those changes as early as tomorrow.

Thanks,

Dave

Inject #: 18

Category: Low

From: David Tennant

To: IT Staff

Subject: Bitcoin payments

Recently, Warp-Core Gaming has received numerous phone calls and emails asking if we will be accepting bitcoins as a payment option. We want to make our customers happy, but before going ahead with this, I wanted to get some feedback from our IT and security staff.

First, please explain to me the security benefits, if any, of accepting payments in Bitcoins. Secondly, I would like to know what security risks are associated with accepting payments in Bitcoins. Finally, please describe the best way to mitigate any known security risks, and a recommendation on whether or not we should begin accepting payments in bitcoins.

Give me a report on this by 5 PM today.

Thanks,

Dave

Inject #: 04

Category: Medium

From: David Tennant

To: IT Staff

Subject: Security Assessment of our Internal Network

By now you should have had the chance to lock down the environment a little and hopefully improve our overall security posture. To see how much progress we've made, perform an assessment of our entire network (core and virtual) – I want to know what vulnerabilities still exist, what systems they appear on, the risks associated with those vulnerabilities, and how we can address or mitigate those vulnerabilities. Be sure to cover **all** the systems in our network and organize the report by system – it's easier for me to see the findings as they apply to each different system that way. List all the systems in the report – if they have no vulnerabilities, state that but list **everything** that has an IP address in our networks in that report. Provide me with a typed report by 5 PM today (include an executive summary and a technical discussion section please). Be sure to list what tool you used to find each vulnerability in your report.

For the report I want to see the following elements at a minimum:

- An executive summary. This should be a high level overview with the most critical vulnerabilities and a high, medium, low ranking for each vulnerability. Be sure to explain why you are ranking the vulnerability as high, medium, or low.
- A technical section listing each system in our network individually, what vulnerabilities exist on that system, what that vulnerability means and how it could be used to compromise our systems, and how we can fix/mitigate those vulnerabilities
- In the technical section be sure to provide a list of the tools you used and an explanation of why you chose those tools
- A prioritized list of recommendations for addressing the discovered vulnerabilities (ie what should we fix first, second, etc)

Thanks,

Dave