King Of the Network Challenge

WARNING

The challenge network, systems, and interconnected devices make up a HOSTILE network environment. By connecting your device to this network you may be jeopardizing the security of said device. In simple term's there's a good possibility that your system may be compromised and or "Hacked" while connected to the challenge network. By connecting your device to the challenge network you agree to indemnify and hold harmless NESIT Inc, Security BSides, and all event organizers, and challenge participants.

RULES

1. Do not purposefully deny service to the network challenge (*Except for challenge 33)
2. Connections to the Challenge network must be made via the Cisco 3500 switch, or via the pwngame wireless network.
3. Submit challenge answers to the information booth for validation.
4. All answers must be validated
5. Challenges do not need to be completed in order - the person with the most points wins!

White Hat Mode:

Challenge 1 - 5 PTS

You're a new network administrator that has just setup and connected an HP printer to the network. Locate the HP Jet direct controller on the network, and note it's IP address below.

Challenge 2- 10 PTS

Being a new network administrator and a curious fellow you've been scanning the network for devices. One of the devices you've located is a Cisco router. Attempt to gain unprivileged access to the router. What information can you determine about the network and about how the device from this unprivileged mode? What version of IOS is this device running?

Challenge 3- 10 PTS

An employee has just been terminated for leaking confidential information to a competitor. Your director has asked you to analyse an encoded message and try and determine it's meaning. The encoded text is: Jung vf gur frperg V'z glcvat

Challenge 4- 20 PTS

To learn about application security your director has setup an instance of OWASP's WebGoat (https://www.owasp.org) penetrate and own the WebGoat.

Challenge 5- 20 PTS

You’ve been tasked with the challenge of determining what information might leak from Active Directory. Using your elite skills attempt to enumerate information about the active directory configuration including: OU’s , Groups, and Users.

Challenge 6- 20 PTS

You’ve noticed some one has attached a backtrack Linux distribution to your network. Locate, and penetrate this system. After you’ve compromised this system leave a text file on the systems desktop with your handle.

Challenge 7- 20 PTS

An undocumented legacy BSD system has been left attached to your network to manage critical infrastructure (your Cisco router). Gain root level access to this device, and add an account for yourself.

Challenge 8- 20 PTS

Your director has instructed you to monitor all network traffic between the Windows XP workstation attached to the domain, and the rest of the network. Using what ever remote means necessary monitor traffic to this workstation. What interesting and or anomalous information did you find?

Challenge 9- 20 PTS

Your director has asked you to decipher the following: Ihak eg r ptskscs Crack the code!

Challenge 10- 30 PTS

You’ve been assigned an inventory project. Determine the hostname and cisco IOS version of the Cisco 3500 switch.

Challenge 11- 30 PTS

Your curiosity has gotten the better of you and you’ve decided to investigate the Sonicwall. Attempt to gain “User” level access to the device.

Challenge 12- 30 PTS

Attempt to penetrate the Ubuntu system to prove it’s insecurely configured. What are the contents of “Secrets.txt” ?

Challenge 13- 30 PTS

You've noticed a new unauthorized administrative account on the network with the user name: dynamiter78, determine as much information about the person who owns this account.

Black Hat Mode:

Challenge 14- 30 PTS

What is the cipher key for the following cipher text? Ihak eg r ptskscs

Challenge 15- 40 PTS

Gain file level access to the domain controller holding the global catalog role. What are the contents of password.txt ?

Challenge 16- 40 PTS

Attempt to add a poison DNS record to the primary DNS server.

Challenge 17- 40 PTS

Gain enable level access to the cisco router. What is the enable secret?

Challenge 18 - 40 PTS

Crack the wepkey for the wireless network “pwngame”

Challenge 19 - 40 PTS

Compromise the NESSUS server, create your own policy and name it your handle.

Challenge 20- 40 PTS

Decipher the following: SSBzb21lIHRpbWVzIHR5cGUgbWVzc2FnZXM=

Challenge 21- 40 PTS

Gain administrative access to the HP Jet Direct controller. What is it’s password?

Challenge 22 - 50 PTS

Add a malicuous route of your choice to the routing table of the cisco router. What route did you add?

Challenge 23 - 50 PTS

Get the VTP domain password to the cisco switch. What is it?

Challenge 24 - 50 PTS

Gain administrative access to the wireless access point. Change the SSID to pwngame+yourhandle.

Challenge 25 - 50 PTS

Recover the original text from: 31938a88cea2afbbe652fd241737c8ac

Challenge 26 - 60 PTS

Deface the main home screen and website of the WebGoat challenge (tomcat server)

Challenge 27 - 60 PTS

Use the BSD legacy machine physically attached to the Cisco router to determine the enable password for the Cisco router.

Challenge 27 - 60 PTS

Without rebooting the switch - Get enable access to the Cisco switch. What is the enable password?

Challenge 28 - 60 PTS

Locate the Quickbooks company data file - what is the balance of the checking account? What are the account and routing numbers for checking?

Challenge 29 - 60 PTS

Analyse the PCAP file at the below link https://docs.google.com/leaf?id=0BwUdOEUYYv6hOWE2YjY0YTAtZDA5My00ZGE3LWE4MDgtNDQ5MDEzYzAyODI4&hl=en_US

What conclusions can you draw about the person who generated this traffic and why?

Challenge 30 - 60 PTS

Recover the original text from: sumK1vbrhQjdahTPpwS61/Bfb7E=

Challenge 31 - 70 PTS

Gain domain admin access to the domain - What is the domain admins password and username?

Challenge 31 - 70 PTS

Gain administrative access to the sonicwall. What is the admin password?

Challenge 32 - 70 PTS

Recover the original text from: c277f1d06a972afdf363f173c7c730f4

Challenge 33 - 80 PTS

Use the Jet direct box to attack another devices on the network. Describe your attack.

Challenge 34 - 80 PTS

Redirect routing on the sonicwall to a destination of your choice.

Challenge 35 - 80 PTS

Gain root on itchy - Who is the admin user and what is the admin users password?

Challenge 36 - 85 PTS

Gain root on scratchy - Who is the admin user and what is the admin users password?

Challenge 37 - 90 PTS

Gain root level access on the Ubuntu server.