KIỂM THỬ XÂM NHẬP

1. Sử dụng chức năng script của nmap để kiểm thử lỗi SQL injection của 1 máy chủ nào đó

* nmap vku.udn.vn

A computer screen with white text

Description automatically generated

* nmap vku.udn.vn -script default

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

* nmap -Pn -script=dns-brute vku.udn.vnA screenshot of a computer

  Description automatically generated

1. Tim hiểu cấu trúc của nmap script và phát triển một script đơn giản cho phép quét các dịch vụ và phiên bản phần mềm của một máy chủ nào đó.

* Định nghĩa : Nmap Script Engine (NSE) là một thành phần của Nmap, cho phép thực hiện các kịch bản phức tạp để mở rộng khả năng quét. NSE sử dụng ngôn ngữ lập trình Lua, một ngôn ngữ đơn giản và nhẹ, rất phù hợp cho việc viết các kịch bản nhỏ.

Để thực hiện chức năng này của nmap sử dụng tùy chọn : –-script [tên\_script].nse

Trong nmap chúng ta gồm có 4 loại NSE scripts như sau :

* *host script* : là một loại script được **thực thi sau khi nmap đã thực hiện tác vụ** của nó như quét những host, cổng mạng hay hệ điều hành,…
* *prerule script* : là một loại script được **thực thi trước bất kì 1 tác vụ quét** hay thu thập thông tin nào
* *service script* : là loại script chạy để **chống lại 1 service đang lắng nghe** ở trên mục tiêu đang pentest
* *postrule sciprt* : là loại script chạy **sau khi Nmap thực thi** scan mục tiêu
* Cấu trúc :

A screen shot of a computer

Description automatically generated

+ description Field

The description field describes what a script is testing for and any important notes the user should be aware of. Depending on script complexity, descriptions may vary in length from a few sentences to a few paragraphs. The first paragraph should be a brief synopsis of the script function suitable for stand-alone presentation to the user. Further paragraphs may provide much more script detail.

+ categories Field

The categories field defines one or more categories to which a script belongs (see the section called “Script Categories”). The categories are case-insensitive and may be specified in any order. They are listed in an array-style Lua table as in this example:

categories = {"default", "discovery", "safe"}

+ author Field

The author field contains the script authors' names and can also contain contact information (such as home page URLs). We no longer recommend including email addresses because spammers might scrape them from the NSEDoc web site. This optional field is not used by NSE, but gives script authors their due credit or blame.

+ license Field

Nmap is a community project and we welcome all sorts of code contributions, including NSE scripts. So if you write a valuable script, don't keep it to yourself! The optional license field helps ensure that we have legal permission to distribute all the scripts which come with Nmap. All of those scripts currently use the standard Nmap license (described in the section called “Nmap Copyright and Licensing”). They include the following line:

+ dependencies Field

The dependencies field is an array containing the names of scripts that should run before this script, if they are also selected. This is used when one script can make use of the results of another. For example, most of the smb-\* scripts depend on smb-brute, because the accounts found by smb-brute may allow the other scripts to get more information. Listing a script in dependencies doesn't cause that script to be run; it still has to be selected through the --script option or otherwise. dependencies merely forces an ordering among the scripts that are selected. This is an example of a dependencies table, from smb-os-discovery:

dependencies = {"smb-brute"}

* Nmap -sC vku.udn.vn

A screenshot of a computer

Description automatically generated

A computer screen shot of white text

Description automatically generated

* Ping vku.udn.vn

A screenshot of a computer

Description automatically generated

* Phát triển 1 script đơn giản :

+ Tạo file http-check.nse

A screenshot of a computer

Description automatically generated

+ Demo chương trình python : Kiểm tra xem dịch vụ HTTP trên cổng 80 có hoạt động hay không?

* + nmap --script ./http-check.nse -p 80 vku.udn.vn -d

A computer screen shot of a program

Description automatically generated

A computer screen shot of a program

Description automatically generated

+ Chuyển đổi thành cổng 80 để kiểm tra

* + Tạo file http-check.nse

A screenshot of a computer

Description automatically generated

+ Demo chương trình python : Kiểm tra xem dịch vụ HTTP trên cổng 8080 có hoạt động hay không?

* + nmap --script ./http-check.nse -p 8080 vku.udn.vn -d

A computer screen shot of a program

Description automatically generated

A computer screen with white text

Description automatically generated