Nmap

1. Output format

Nmap có 4 loại output format

* Interactive output: xuất ra stdout. Đây là dạng output thông thường nhất.
* Normal output: xuất ra stdout nhưng bỏ đi 1 số thông tin như timestamp
* XML output: xuất kết quả ra file XML.
  + Có thể sử dụng là input đối với 1 số chương trình khác.
  + Chứa đựng nhiều thông tin hơn các loại output khác.
  + Nmap có DTD tại <http://nmap.org/svn/docs/nmap.dtd>
  + Nmap có thể xuất ra database thông qua nmap-sql nhưng chỉ dùng được đối với MySQL :D
  + Ngoài ra còn 1 khả năng nữa là PBNJ. <http://pbnj.sourceforge.net/>
  + Có 2 project Nmap::scanner và Nmap::parser dùng để đọc thông tin output dạng XML của Nmap sang PERL. <http://sourceforge.net/projects/nmap-scanner/> http://anthonypersaud.com/category/nmap-parser/
* Grepable output: output này được sử dụng chính trên Linux dùng với các editor như awk, grep …

Người dùng có thể xác định mức độ chi tiết của output bằng cách them –v vào dòng lệnh. Mức độ chi tiết này ảnh hưởng nhiều nhất với 2 loại output interactive và normal. Càng nhiều –v thì độ chi tiết càng cao nhưng tốt nhất là < 2. 1 số thông tin sẽ được thêm vào với –v:

* Thời gian scan dự đoán: SYN Stealth Scan Timing: About 30.01% done; ETC: 16:04 (0:01:09 remaining)
* Các port được mở sẽ được xuất ra ngay khi được phát hiện đối với interactive output.
* Các cảnh báo: 1 số cảnh báo chỉ được xuất hiện với từ khóa –v
* Các thông tin thêm về OS : như TCP ISN ??? và TCP ID sequence number ???
* ...

1. Cơ chế kiểm tra service và version của Nmap :

Sau khi thực hiện host scan và port scan, NMap sẽ check các port có status là open hoặc fitered

* 1. Nmap sẽ check các port nếu Exclude thì sẽ không quét. Các exclude port được ghi trong nmap-service-probes.
  2. Nếu port là TCP
     1. Nmap sẽ connect tới. Nếu connect thành công sẽ đổi status sang open.
     2. Sau khi connect thành công, Nmap sẽ đợi 5s. 1 số service sẽ gửi thông điệp đến Nmap trc. Các thông điệp này sẽ được match với nmap-service-probes bằng regex để xác định service và version.
  3. Nếu vẫn chưa xác định được hoặc chỉ xác định được 1 phần, Nmap sẽ gửi các UDP probe để kiểm tra. Mỗi UDP probe chứa probe string gửi tới các port. Các service trên port đó sẽ gửi các phản hồi. Các phản hồi này sẽ được so với nmap-service-probes để xác định service và version. Nếu nhận được các phản hồi thì status của port đó sẽ được chuyển sang open. Chú ý: các probe này có 1 giá trị popular, chỉ các probe có khả năng match cao mới được gửi.
     1. Nếu các trường hợp trên thất bại thì Nmap sẽ gửi tất cả các probe đến port đó để kiểm tra.
  4. Nếu port được xác định sử dụng SSL, Nmap sẽ connect lại và thử lại như trên.
  5. Ngoài ra còn cơ chế RPC.

Dùng Nmap scripting engine(NSE) để xác định version: trong 1 số trường hợp, chỉ sử dụng probe là ko đủ để xác định version – ví dụ như cần 2 probe để xác định version của 1 service. Lúc đó, Nmap sẽ dùng các script để xác định version của service.

description = [[

Detects the Skype version 2 service.

]]

---

-- @output

-- PORT STATE SERVICE VERSION

-- 80/tcp open skype2 Skype

author = "Brandon Enright"

license = "Same as Nmap--See http://nmap.org/book/man-legal.html"

categories = {"version"}

require "comm"

require "shortport"

portrule = function(host, port)

return (port.number == 80 or port.number == 443 or

port.service == nil or port.service == "" or

port.service == "unknown")

and port.protocol == "tcp" and port.state == "open"

and port.service ~= "http" and port.service ~= "ssl/http"

and not(shortport.port\_is\_excluded(port.number,port.protocol))

end

action = function(host, port)

local status, result = comm.exchange(host, port,

"GET / HTTP/1.0\r\n\r\n", {bytes=26, proto=port.protocol})

if (not status) then

return

end

if (result ~= "HTTP/1.0 404 Not Found\r\n\r\n") then

return

end

-- So far so good, now see if we get random data for another request

status, result = comm.exchange(host, port,

"random data\r\n\r\n", {bytes=15, proto=port.protocol})

if (not status) then

return

end

if string.match(result, "[^%s!-~].\*[^%s!-~].\*[^%s!-~]") then

-- Detected

port.version.name = "skype2"

port.version.product = "Skype"

nmap.set\_port\_version(host, port, "hardmatched")

return

end

return

end

Question:

1. TCP ISN với TCP ID là các thông số được sử dụng bởi protocol để xác định các packet, segment thì làm sao có thể xác thông tin của OS được?

NMap có 1 phần về xác định OS. Câu hỏi này sẽ được trả lời sau khi tìm hiểu về phần đó. Khi tìm cách xác định thông tin của OS, NMap sẽ thu được thông tin về TCP ISN và TCP ID. Không phải dùng 2 cái này để xác định OS.

1. Cơ chế RPC của Nmap cụ thể là thế nào?

1 số port có service dựa trên RPC thì Nmap có thể quét ra được. Không phải là Nmap có cơ chế RPC. Nmap sẽ gửi các probe đến để kiểm tra version number cũng như loại service thông qua Nmap grinder ???