Soạn kịch bản

Xin chào thầy và các bạn

Em tên là Lê Hải Đăng

Hôm nay em trình bài...

Chủ đề...

**I- ARP spoofing**

**- địa chỉ luận lý:** ip - gồm 2 phần địa chỉ mạng và máy, việc phân chia này nhằm giúp cho việc tìm ra các đường kết nối từ hệ thống mạng này sang hệ thống mạng khác dễ dàng hơn.

**- đia chỉ vật lý:** mac, nsx gán cho phần cứng, địa chỉ phẳng không phân lớp, khó giao tiếp giữa các máy tính

**(slide 5)**

- arp là viết tắt của ...

**(silde 6)**

b1: ... => để xem có địa chỉ ánh xạ từ ip->mac của máy nhận không,

- nếu có địa chỉ ánh xạ thì chuyển sang bước 5

- nếu không chuyển sang bước 2

b2: ... => máy gửi sẽ gửi broadcast cho toàn mạng với nội dung là: ai đang giữ địa chỉ ip nhận, cho nó xin lại địa chỉ mac

b3: ...=> máy đang giữ đc ip sẽ trả lời lại máy gửi: dc ip và mac của nó

b4: ...=> máy gửi nhận được arp reply của máy nhận sẽ cập nhật lại arp cache của mình

b5: ...

**(slide 7)**

Giả sử host A thuộc lớp mạng A và host B thuộc lớp mạng B, host A muốn gửi gói tin cho host B, host a xác định host b khác lớp mạng, mặc định gói tin sẽ được gửi đến default gateway

b1:...=> host A gửi ARP request hỏi địa chỉ MAC của route C

b2:...=> router C gửi phản hồi đ/c MAC của mình bằng gói ARP reply

b3=> gửi gói tin đến router C thông qua địa chỉ MAC vừa nhận được

thông qua router C đến lớp mạng B

b4=> router C sẽ gửi ...

b5=> ...

b6=> ...

**(slide 9)**

- chấm thứ 3: gói tin reply và request hoạt động độc lập nhau,(không có trạng thái nối kết giữa gói gửi và gói nhận)

nhận bất kì arp reply nào được gửi đến ngay cả khi nó không yêu cầu,

nếu mục arp chưa hết hạn thì nó sẽ ghi đè arp reply mới,

- chấm thứ 4: không có phương thức chứng thực nào giúp nhận biết địa chỉ nguồn của ARP

**(slide 10)**

sử dụng lệnh arp -a,

Nếu xuất hiện mục arp có cùng địa chỉ IP nhưng khác địa chỉ MAC thì có một cuộc tấn công ARP đang diễn ra

**(slide 11)**

- arp tĩnh: cấu hình trước arp để không nhận bất kì arp reply nào được gửi đến

- packet filtering: kiểm tra xung đột địa chỉ MAC

- SARP: sử dụng chữ ký số trong giao thức arp

- DAI: kiểm tra địa chỉ ánh xạ từ IP-MAC thông qua giao thức DHCP

- VPN: mã hóa dữ liệu gửi đi để dữ liệu không có tác dụng với kẻ tấn công

- thực hiện tấn công ARP để kiểm tra các giao thức bảo mật có hoạt động hiệu quả không

**II-DNS**

**(slide 14)**

giúp chuyển đổi tên miền mà con người dễ nhớ thành địa chỉ IP mà máy tính có thể hiểu và sử dụng để kết nối đến các máy chủ trên Internet.

**(slide 15)**

- tên miền cấp 1: .vn, .us

- tên muền cấp 2: .edu, .gov

- cấp nhỏ hơn: .ctu

=> ví dụ như tên miền này: tên miền được phân giải từ cuối về đầu: khu vực Việt Nam ở hệ thống giáo dục của trường ĐHCT tại trang elearning

**(slide 16)**

**(slide 17)**

ISP là nhà cung cấp dịch vụ

**(slide 18)**

b1:=> kiểm tra cache trình duyệt xem có địa chỉ ánh xạ tên miền-> ip hay không

b2:=> kiểm tra cache hdh

b3:=> Gửi yêu cầu đến DNS nội bộ hoặc nhà cung cấp dịch vụ(nếu có)

nếu 3 bước trên không có sẽ gửi truy vấn ra ngoài internet

b1:=> yêu cầu được tiếp nhận bới DNS resolver

b2:=> DNS resolver sau đó truy vấn đến rootname server

b3:=> rootname server phản hồi resolver bằng địa chỉ của máy chủ TDL

b4:=> …

b5 … b10:=>

**(slide 21)**

Máy chủ DNS nội bộ (Internal DNS Servers) → Chia sẻ thông tin với bất kỳ ai nếu không được cấu hình đúng.

...

**(slide 22)**

thứ nhất....dẫn đến...

**(slide 23)**

- về phía kẻ tấn công…

- về phía nhân …

**(slide 24)**

thứ nhất...

thứ hai...

thứ ba...

**(slide 25)**

- ... để...

Sử dụng DNSSEC – Cung cấp chữ ký số để xác thực DNS.

Xóa cache DNS thường xuyên – Tránh giữ lại thông tin DNS giả mạo.

Dùng máy chủ DNS tin cậy – Google DNS (8.8.8.8), Cloudflare (1.1.1.1).

Bật HTTPS & kiểm tra chứng chỉ SSL – Đảm bảo trang web là chính thống.

Sử dụng VPN – Mã hóa truy vấn DNS để tránh bị tấn công.

**III- Password attack**

**(slide 28)**

ví dụ như chị em sinh đôi có thể dễ dàng bypass thiết bị của nhau

Đơn giản như khi chúng ta ngủ, có người lấy ngón tay chúng ta để "bypass" chính điện thoại của chúng ta

Hay phức tạp hơn nữa là Face ID của Apple bị một chiếc mặt nạ do BKAV làm giả đánh lừa

**(slide 29)**

Phương pháp này tồn tại rủi ro ...

hay là..

ngoài ra..

**(slide 30)**

Có tính xác định: Cùng một chuỗi đầu vào được xử lý bởi cùng hàm băm, sẽ cho ra cùng một kết quả.

Không thể đảo ngược (một chiều): Không thể tạo ra chuỗi (thông điệp) từ một chuỗi đã được băm từ hàm băm.

Có entropy cao: Khi có một thay đổi nhỏ trong chuỗi thông điệp, sẽ tạo ra chuỗi băm khác nhau

Có tính duy nhất: Hai thông điệp khác nhau thì nhận về 2 chuỗi băm khác nhau.

**(slide 31)**

... nhưng mà các thuật toán mã hóa mạnh...điều này gây bất tiện...giải pháp là...

**(slide 32)**

**(slide 44)**

thu thập thông tin của nạn nhân từ các nguồn trên Internet, mạng xã hội, giả mạo bạn bè và tương tác để lấy thông tin, gửi gmail giả danh người đáng tin nhằm lấy thêm dữ liệu

-> thu thập thông tin để tạo từ điển dành riêng cho nạng nhân

**(slide 45)**

một số công cụ tấn công hàm băm phổ biến như hashcat + john

**(slide 46)**

tùy chọn, nếu chỉ sử dụng CPU thì ưu tiên dùng John, nếu sử dụng GPU thì nên chọn hashcat sẽ tối ưu hơn,

nếu có thể thì nên sử dụng GPU sẽ giải mã nhanh hơn gắp 100-1000 lần CPU

chạy càng nhiều luồng song song sẽ nâng cao đáng kể tốc độ crack

**(slide 47)**

công cụ trích xuất hash từ file đã bị mã hóa

file zip, rar, pdf, 7z

**(slide 48)**

công cụ hỗ trợ xác định giải thuật băm

**(Tổng Kết Phần 3)**

Hacker đã lấy được hàm băm của mật khẩu.

Lấy thông qua SQL injection

Lấy thông qua Metataploit khai thác lỗ hổng hệ thống và truy cập vào một tài khoản thông thường (non-root user), muốn leo thang đặc quyền (privilege escalation) lên admin/root, hacker thường làm cách nào đó để đọc file chứa mật khẩu để bẻ khóa và thực hiện leo than đặc quyền

Sniffing (nghe lén mạng)từ mitm

Lấy thông qua hệ điều hành

Đọc file shadow trên linux hoặc sam & system trên windows

…

Hacker đã lấy được tệp nhưng đã bị mã hóa.

**(Demo ARP)**

\*\*thực hiện demo có 2 máy victim là máy Windows 10 và máy hacker là máy kali, cho 2 máy vào cùng 1 nat netword\*\*

mở cả 2 máy lên...

1. Nhập lệnh ipconfig trên commandline để xem ip trên máy nạn nhân

ta thấy được địa chỉ ip của nạn nhân là 192.168.1.11

2. Nhập arp -a để xem arp table của nạn nhân

ta thấy được cổng mặc định có địa chỉ mac là ...

3. nhập lệnh ifconfig trên Terminal để xem ip và mac của hacker

4. thực hiện quét lớp mạng xem địa máy nạng nhân có chung lớp mạng với hacker không

ta thấy được địa chỉ ip của nạng nhân -> nạn nhân chung lớp mạng với hacker

5. trên máy hacker bật công cụ ettercap và chọn card mạng

6. trên máy hacker chọn host list để xem toàn bộ host đang hoạt động trong lớp mạng

7. đưa cổng mặc định vào target 1 và máy nạn nhân vào target 2

8. chọn chế độ arp poisoning và tấn công

-> lúc này máy hacker sẽ liên tục gửi arp giả mạo cho máy nạn nhân và cổng mặc định

9. bật wireshark và quan sát gói tin

10. ta gói tin liên tục gửi đến nạn nhân với nội dung như sau

máy gửi là 192.168.1.1

địa chỉ mac của máy gửi là :::::

máy nhận là 192.168.1.11

địa chỉ mac máy nhận là ...

gói tin có vẻ như bình thường nhưng địa chỉ ip của máy gửi là cổng mặc định nhưng địa chỉ mac là của hacker

11. hacker cũng sẽ gửi gói (ARP reply) tương tự đến cổng mặc định nhưng địa chỉ của người gửi là IP của victim với địa chỉ mac của hacker làm cho ARP table của Router bị sửa đổi.

=> lúc này hacker sẽ kiểm soát quá trình giao tiếp giữa nạn nhân và Router

12. trên máy nạng nhân nhập lại lệnh arp -a để xem lại arp table

ta có thể thấy arp của nạn nhân đã bị sử đổi

=> IP là của Router nhưng địa chỉ MAC lúc này là của hacker

13. trên máy nạn nhân, khi nạn nhân đăng nhập vào một trang web bất kỳ

\*em thử đăng xuất và đăng nhập lại 2,3 lần cho chắc\*

14. lúc này trên máy hacker có thể quan sát và đọc gói tin của nạn nhân

- hacker bật wireshark và lọc gói tin, chỉ lấy frame với nội dung là password

- do giao thức là http nên có thể xem nội dung của gói tin trực tiếp mà không bị mã hóa

- ta thấy username và password nạng nhân vừa nhập

\*\*ngoài ra hacker có thể chặn liên lạc giữa Router và máy nạn nhân

\*\*tin vi hơn thì hacker có thể chỉnh sửa nội dung bên trong gói tin

vì đã có ID hoặc cookie sẵn rồi nên gửi đến đích thì máy chủ sẽ không nghi ngờ

**(Demo DNS)**

Tiến hành cho 2 máy vào 1 nat netword và thực hiện kiểm tra ip tương từ quá trình kiểm tra trên demo ARP spoofing

1. mở file etter.dns, thêm địa chỉ IP của hacker và hướng victim vào trang mà hacker mong muốn

file này em đã cấu hình từ trước

nội dung trong file là tất cả tên miền mà nạn nhân nhập, điều trả về địa chỉ ip của hacker

2. bật và cấu hình file index.html, do chỉ demo nên em chỉ nhập nội dung tượng trưng là máy bạn đã bị hack

tinh vi hơn có thể hacker thiết kế form đăng nhập tương tự trang web thật để lấy thông tin đăng nhập của người dùng

hoặc thiết kế tương tự một trang web nào đó và đăng mã độc lên nếu có nạn nhân nào lỡ tải phải thì sẽ bị nhiễm mã độc.

3. khởi động apache

4. tiến hành arp spoofing để mọi yêu cầu phân giải của nạn nhân và trả lời trước máy chủ DNS hợp lệ

5. khi nạn nhân truy cập vào tên miền hợp lệ sẽ hướng đến website của hacker

6. khi hacker đã tắt DNS spoofing thì nạn nhân vẫn sẽ truy cập vào ip giả của hacker vì DNS cache của trình duyệt đã bị đầu độc

đến với phần 3 password attack em sẽ tấn công file đã bị mã hóa bằng brute force

**(Demo Password Attack)**

1. có 1 file lưu trữ mật khẩu

2. mã khóa file zip

3. lấy hash bằng zip2john

4. crack mk bằng …

5. mk đã bị crack ...