Responder là 1 framework mã nguồn mở giúp thực hiện tấn công và thu thập thông tin trong mạng nội bộ, dựa vào việc khai thác giao thức LLMNR, NBT-NS hay MDNS.

1. Khởi động Responder

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Đăng nhập vào tài khoản Sec560student/Clark bên Window
2. Opening Explorer window

Mở Eplorer window và thử mở 1 kết nối SMB với 1 hệ thống không tồn tại.

**Giao thức LLMNR được sử dụng để phân giải tên máy trong mạng nội bộ khi DNS ko có kết quả**

Ta sẽ thử đánh lừa giao thức LLMNR, máy window sẽ cố gắng giải quyết hostname bằng cách gửi đi rất nhiều request LLMNR và khi đó Responder sẽ trả lời lại request này.

Ta sẽ thử mở File Explorer và tạo 1 SMB session với [\\WINDOWS01](file:///\\WINDOWS01). Đợi 1 lúc ta sẽ thấy trả về 1 “ Access denied” và yêu cầu gửi thông tin xác thực

A screenshot of a computer

AI-generated content may be incorrect.

Đợi 1 lúc ta sẽ nhận được thông báo như sau

A screenshot of a computer security

AI-generated content may be incorrect.

1. Review NTLMv2 challenge/response hash

Chuyển sang máy Linux ta sẽ thấy thành công thu thập được NTLMv2 challenge-response

A screenshot of a computer error

AI-generated content may be incorrect.

*Phân tích kĩ hơn: Máy window đã cố gắng kết nối đến máy chủ windows01.local nhưng ko tìm thấy trong DNS và nó sẽ chuyển sang giao thức LLMNR để tìm kiếm. Windows sẽ gửi request đến toàn mạng Lan. Skipping…. Tức là responder đang bỏ qua các hash trùng lặp*

Thu thập được hash, thoát Responder

1. Use John The Ripper to crack the obtained hash

Phân biệt sự khác nhau giữa NTLM hash và NetNTLMv2 hash

* NTLM là sử dụng MD4 hash ko có salt và được Windows lưu trữ trong file SAM(người dung hệ thống) hoặc NTDS,dit file ( tên miền của người dung). Có thể dung được với Pass-the-hash
* NetNTLMv2 là challenge-response và có thể bị tất công brute force offline. Không thể dung được với Pass-the-hash nhưng có thể bị Relay Attack nếu SMB signing ko bật

Những hash đã được Responder bắt được sẽ được lưu trong /opt/responder/logs với tên file như ở dưới

**john --format=netntlmv2 /opt/responder/logs/SMB-NTLMv2-SSP-\***

format=netntlmv2: sử dụng John the Ripper với định dạng hash là netNTLMv2

/opt/responder/logs/SMB-NTLMv2-SSP-\*: vị trí lưu hash thu thập được từ **giao thức SMB**

A screenshot of a computer program

AI-generated content may be incorrect.

John sẽ sử dụng bruteforce hoặc dictionary attack để thực hiện crack.

1 điều chú ý là John sẽ ko crack lại những hash đã được crack trước đó. Nếu muốn xem lại ta sử dụng option **show**

1. Logout clark, login as sec560
2. Capturing hashes with a sniffer

Sử dụng smbclient để kết nối từ máy Linux đến máy Windows và tcpdump để bắt gói tin trên cổng 445 ( SMB) và lưu vào tệp /tmp/winauth.pcap

A screenshot of a computer

AI-generated content may be incorrect.

Tạo kết nối thất bại vì mật khẩu hết hạn. Tuy nhiên tcpdump vẫn bắt được 1 số gói tin. Ctrl C để dửng theo dõi và thực hiện ghi những gói tin vào trong file

1. Extract hashes from Pcap file

Sử dụng PCredz để trích xuất những hashes mật khẩu từ file pcap.

A screenshot of a computer program

AI-generated content may be incorrect.

Ta thu được hash trên màn hình. Ngoài ra công cụ cũng sẽ tạo ra những file với tên là những hash mà ta tìm thấy. Ví dụ ở đây là NTLMv2



Đọc file

A number and text on a white background

AI-generated content may be incorrect.

Sử dụng John để crack

A screenshot of a computer screen

AI-generated content may be incorrect.

Sử dụng Hashcat để crack bằng cách dictionary attack bằng từ điển rockyou

A screenshot of a computer

AI-generated content may be incorrect.

-m 5600 : NetNTLMv2 mode

-w 3: tốc độ xử lý cao

-a 0: dictionary attack

Xem kết quả

