SMB Cheat Sheet

General

- SMB= Server Message Block
- SMB is a Windows implementation of a file-sharing
- SMB uses ports 139 and 445

Nmap Scripts

*** Always check both TCP and UDP ports using Nmap**

smb-protocols

- Shows SMB Protocol dialects
- Issue: SMB v1

SMB-os-discovery

-To determine the operating system

smb-security-mode

- To determine the security mode of SMB service
  - NONE: No security mode.
  - SHARE: Share-level security mode.
  - USER: User-level security mode.
  - DOMAIN: Domain-level security mode.
  - ADS: Active Directory security mode.

Issue: Messege_signing: disabled

smb-enum-sessions

- Shows Active sessions

smb-enum-shares

- enumerate the available shares on a target system
- Shows permissions to the shared accounts

smb-enum-sessions --script-args smbusername=administrator,smbpassword =password IP_address

smb-enum-shares,smb-ls --script-args smbusername=administrator,smbpassword =password IP_address

- “smb-ls” tells us what's inside each of the shares like finding directory

smb-enum-users --script-args smbusername=administrator,smbpassword =password

- To enumerate user accounts on a target system

smb-enum-stats --script-args smbusername=administrator,smbpassword = password

- Server statistics:
  - How many files are sent
  - Failed Logins
  - Permissions etc.

smb-enum-domains --script-args smbusername=administrator,smbpassword =password

- To enumerate domain information from target systems
- May retrieve details such as domain names, domain controllers, trusts and other relevant information about the Windows domain environment.

smb-enum-groups --script-args smbusername=administrator,smbpassword =password

- Provides list of users in Groups
- May retrieve group names, memberships etc.

smb-enum-services --script-args smbusername=administrator,smbpassword =password

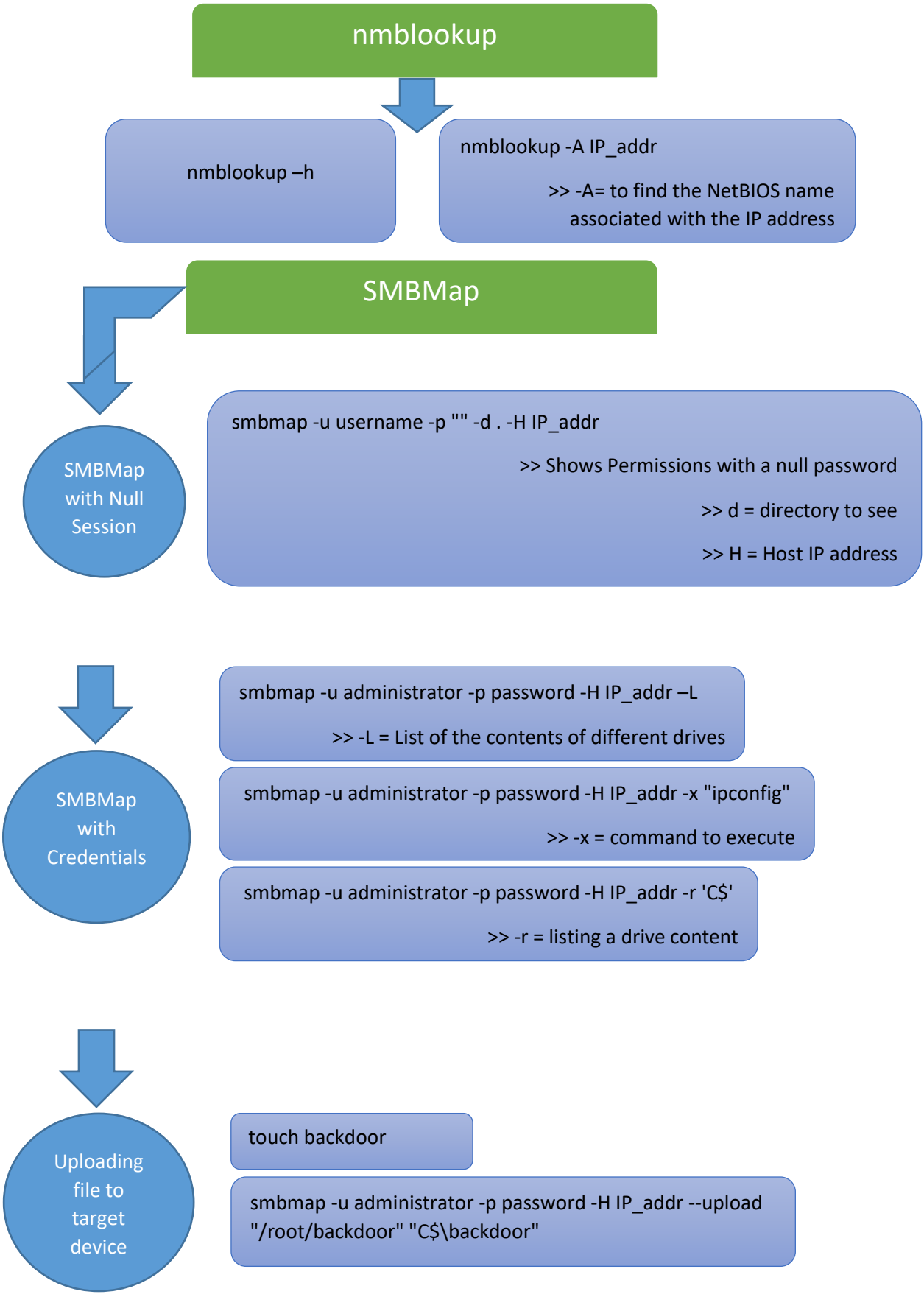
- enumerate running services

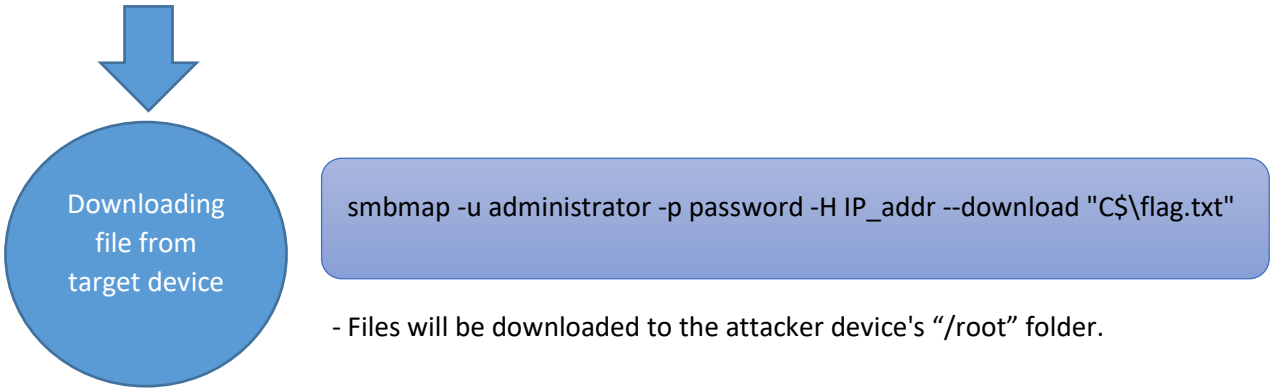
Metasploit Scripts

- auxiliary/scanner/smb/smb_version
- auxiliary/scanner/smb/smb2
- auxiliary/smb/smb_enumshares

enum4linux

- enum4linux –h >> Help
- enum4linux -S IP_addr >> -S =Share
- enum4linux -o IP_addr >> -o = Get OS information
- enum4linux -G IP_addr >> -G = Group Information
- enum4linux -U IP_addr >> -U = Get user list
- enum4linux -i IP_addr >> -i = network interface


nmblookup
nmblookup –h
nmblookup -A IP_addr
>> -A= to find the NetBIOS name associated with the IP address
SMBMap
SMBMap with Null Session
smbmap -u username -p "" -d . -H IP_addr
>> Shows Permissions with a null password
>> d = directory to see
>> H = Host IP address
SMBMap with Credentials
smbmap -u administrator -p password -H IP_addr –L
>> -L = List of the contents of different drives
smbmap -u administrator -p password -H IP_addr -x "ipconfig"
>> -x = command to execute
smbmap -u administrator -p password -H IP_addr -r 'C$'
>> -r = listing a drive content
Uploading file to target device
touch backdoor
smbmap -u administrator -p password -H IP_addr --upload "/root/backdoor" "C$\backdoor"



smbclient Connection with Null Session

smbclient –h

>> Help

smbclient -L IP_addr –N

>> -N= No password = Null session

>> -L = List of Hosts

rpcclient Connection with Null Session

rpcclient –h

>> Help

rpcclient -U "" -N IP_addr

>> -N= No password = Null session

After connecting with rpcclient

?	<<< help
Srvinfo	<<< Getting info from remote server
enumdomusers	<<< getting user list
enumdomgroups	<<< getting group list
lookupnames username	<<< Get full SID of admin
exit	

SMB Dictionary Attack