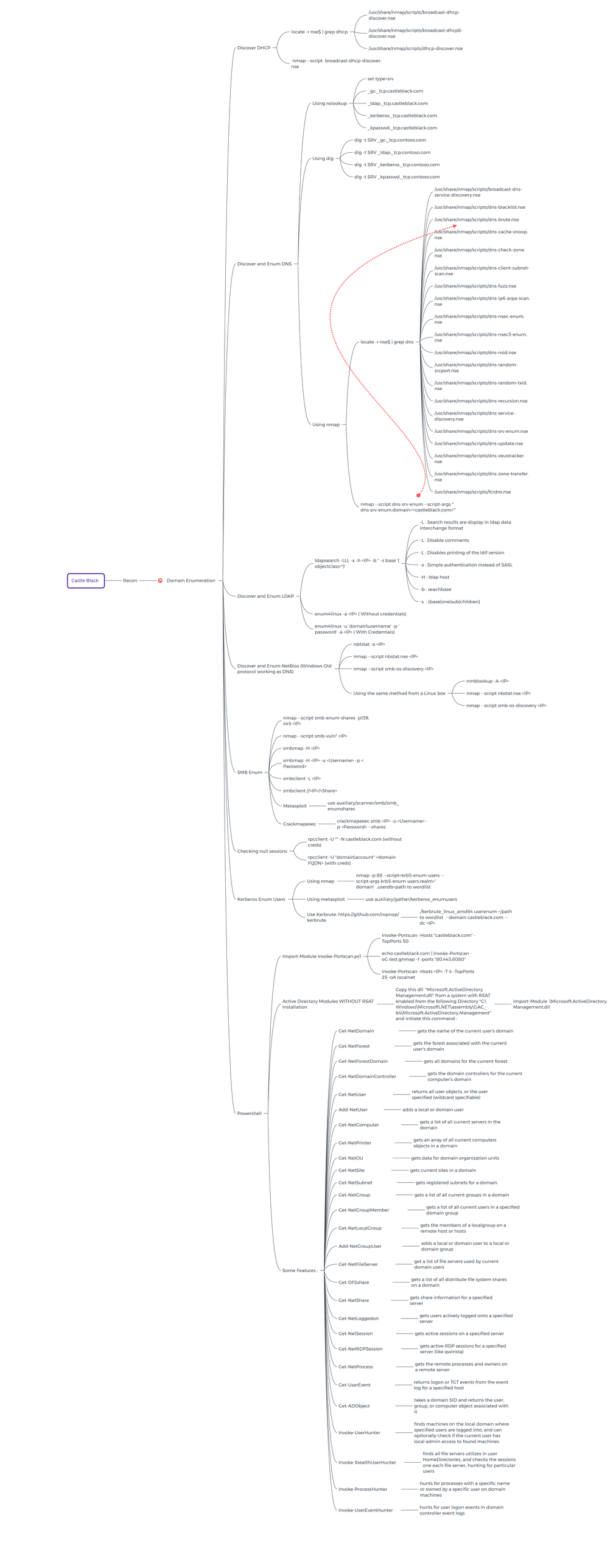
Castle Black
Recon
Domain Enumeration
Discover DHCP
locate -r nse$ | grep dhcp
/usr/share/nmap/scripts/broadcast-dhcp-discover.nse
/usr/share/nmap/scripts/broadcast-dhcp6-discover.nse
/usr/share/nmap/scripts/dhcp-discover.nse
nmap --script broadcast-dhcp-discover.nse
Discover and Enum DNS
Using nslookup
set type=srv
_gc._tcp.castleblack.com
_ldap._tcp.castleblack.com
_kerberos._tcp.castleblack.com
_kpasswd._tcp.castleblack.com
Using dig
dig -t SRV _gc._tcp.contoso.com
dig -t SRV _ldap._tcp.contoso.com
dig -t SRV _kerberos._tcp.contoso.com
dig -t SRV _kpasswd._tcp.contoso.com
Using nmap
locate -r nse$ | grep dns
/usr/share/nmap/scripts/broadcast-dns-service-discovery.nse
/usr/share/nmap/scripts/dns-blacklist.nse
/usr/share/nmap/scripts/dns-brute.nse
/usr/share/nmap/scripts/dns-cache-snoop.nse
/usr/share/nmap/scripts/dns-check-zone.nse
/usr/share/nmap/scripts/dns-client-subnet-scan.nse
/usr/share/nmap/scripts/dns-fuzz.nse
/usr/share/nmap/scripts/dns-ip6-arpa-scan.nse
/usr/share/nmap/scripts/dns-nsec-enum.nse
/usr/share/nmap/scripts/dns-nsec3-enum.nse
/usr/share/nmap/scripts/dns-nsid.nse
/usr/share/nmap/scripts/dns-random-srcport.nse
/usr/share/nmap/scripts/dns-random-txid.nse
/usr/share/nmap/scripts/dns-recursion.nse
/usr/share/nmap/scripts/dns-service-discovery.nse
/usr/share/nmap/scripts/dns-srv-enum.nse
/usr/share/nmap/scripts/dns-update.nse
/usr/share/nmap/scripts/dns-zeustracker.nse
/usr/share/nmap/scripts/dns-zone-transfer.nse
/usr/share/nmap/scripts/fcrdns.nse
nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='<castleblack.com>'"
Discover and Enum LDAP
ldapsearch -LLL -x -h <IP> -b '' -s base '(objectclass=*)'
-L : Search results are display in ldap data interchange format
-LL : Disable comments
-LLL : Disables printing of the ldif version
-x : Simple authentication instead of SASL
-H : ldap host
-b : seachbase
-s : {base|one|sub|children}
enum4linux -a <IP> (Without credentials)
enum4linux -u 'domain\username' -p 'password' -a <IP> (With Credentials)
Discover and Enum NetBios (Windows Old protocol working as DNS)
nbtstat -a <IP>
nmap --script nbstat.nse <IP>
nmap --script smb-os-discovery <IP>
Using the same method from a Linux box
nmblookup -A <IP>
nmap --script nbstat.nse <IP>
nmap --script smb-os-discovery <IP>
SMB Enum
nmap --script smb-enum-shares -p139, 445 <IP>
nmap --script smb-vuln* <IP>
smbmap -H <IP>
smbmap -H <IP> -u <Username> -p <Password>
smbclient -L <IP>
smbclient //<IP>/<Share>
Metasploit
use auxiliary/scanner/smb/smb_enumshares
Crackmapexec
crackmapexec smb <IP> -u <Username> -p <Password> --shares
Checking null sessions
rpcclient -U "" -N castleblack.com (without creds)
rpcclient -U "domain\account" <domain FQDN> (with creds)
Kerberos Enum Users
Using nmap
nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='domain' ,userdb=path to wordlist
Using metasploit
use auxiliary/gather/kerberos_enumusers
Use Kerbrute: https://github.com/ropnop/kerbrute
./kerbrute_linux_amd64 userenum -/path to wordlist --domain castleblack.com --dc <IP>
Powershell
Import-Module Invoke-Portscan.ps1
Invoke-Portscan -Hosts "castleblack.com" -TopPorts 50
echo castleblack.com | Invoke-Portscan -oG test.gnmap -f -ports "80,443,8080"
Invoke-Portscan -Hosts <IP> -T 4 -TopPorts 25 -oA localnet
Active Directory Modules WITHOUT RSAT Installation
Copy this dll "Microsoft.ActiveDirectory.Management.dll" from a system with RSAT enabled from the following Directory "C:\Windows\Microsoft\.NET\assembly\GAC_64\Microsoft.ActiveDirectory.Management" and initiate this command :
Import-Module .\Microsoft.ActiveDirectory.Management.dll
Some Features :
Get-NetDomain
gets the name of the current user's domain
Get-NetForest
gets the forest associated with the current user's domain
Get-NetForestDomain
gets all domains for the current forest
Get-NetDomainController
gets the domain controllers for the current computer's domain
Get-NetUser
returns all user objects, or the user specified (wildcard specifiable)
Add-NetUser
adds a local or domain user
Get-NetComputer
gets a list of all current servers in the domain
Get-NetPrinter
gets an array of all current computers objects in a domain
Get-NetOU
gets data for domain organization units
Get-NetSite
gets current sites in a domain
Get-NetSubnet
gets registered subnets for a domain
Get-NetGroup
gets a list of all current groups in a domain
Get-NetGroupMember
gets a list of all current users in a specified domain group
Get-NetLocalGroup
gets the members of a localgroup on a remote host or hosts
Add-NetGroupUser
adds a local or domain user to a local or domain group
Get-NetFileServer
get a list of file servers used by current domain users
Get-DFSshare
gets a list of all distribute file system shares on a domain
Get-NetShare
gets share information for a specified server
Get-NetLoggedon
gets users actively logged onto a specified server
Get-NetSession
gets active sessions on a specified server
Get-NetRDPSession
gets active RDP sessions for a specified server (like qwinsta)
Get-NetProcess
gets the remote processes and owners on a remote server
Get-UserEvent
returns logon or TGT events from the event log for a specified host
Get-ADObject
takes a domain SID and returns the user, group, or computer object associated with it
Invoke-UserHunter
finds machines on the local domain where specified users are logged into, and can optionally check if the current user has local admin access to found machines
Invoke-StealthUserHunter
finds all file servers utilizes in user HomeDirectories, and checks the sessions one each file server, hunting for particular users
Invoke-ProcessHunter
hunts for processes with a specific name or owned by a specific user on domain machines
Invoke-UserEventHunter
hunts for user logon events in domain controller event logs