From Chump to Trump

Privilege Escalation By Stealing Elect^H^H^H^H Domain Credentials

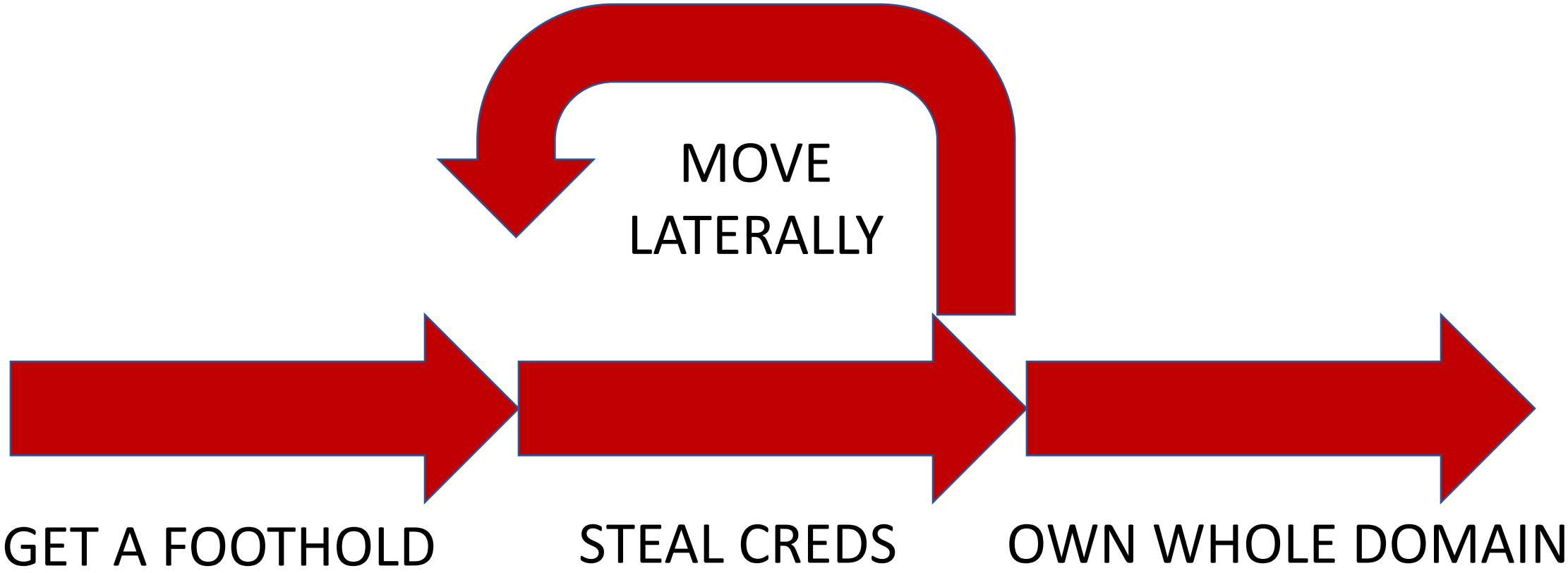
Who Am I?

- @mikeloss
- Used to be a stupid Windows/AD admin.
- As a result I know how stupid admins think.
- Now I use that superpower for ~~evil fun~~ good.
- I work at a company called Asterisk
  - They’re seriously great.

What **are** we talking about?

- Privilege escalation in MS Active Directory
- Current methods and techniques
- Inch deep, mile wide
- Abuse of intended functionality so no patches exist (mostly)
- Shit so stupid many people don't think to try it.
- I'm gonna have to talk fast so I'm going to stumble on my words, forgive me.

How to steal an elec^H^H^H^H AD domain.



Tools.

- You don’t need many.
- R = responder
- E = empire
- M = metasploit
- Z = mimikatz
- S = sysinternals
- C = crackmapexec
- … and BloodHound

Tools.

- You don’t need many.
- R = responder
- E = empire
- M = metasploit
- Z = mimikatz
- S = sysinternals
- C = crackmapexec
- … and BloodHound

R
E
M
Z
S
C

Make friends with Russians.

- Russinovich sounds Russian to me…
- Sysinternals suite
  - Know it, love it.
  - Popular with sysadmins so already on many Windows servers
  - AV won’t trip
  - Incredibly useful
    - Procdump lsass.exe then mimikatz offline!
    - Accesschk for file/service/reg key permissions!
    - Psexec is classic for a reason!

R
E
M
Z
S
C

Get stupid.

R
E
M
Z
S
C

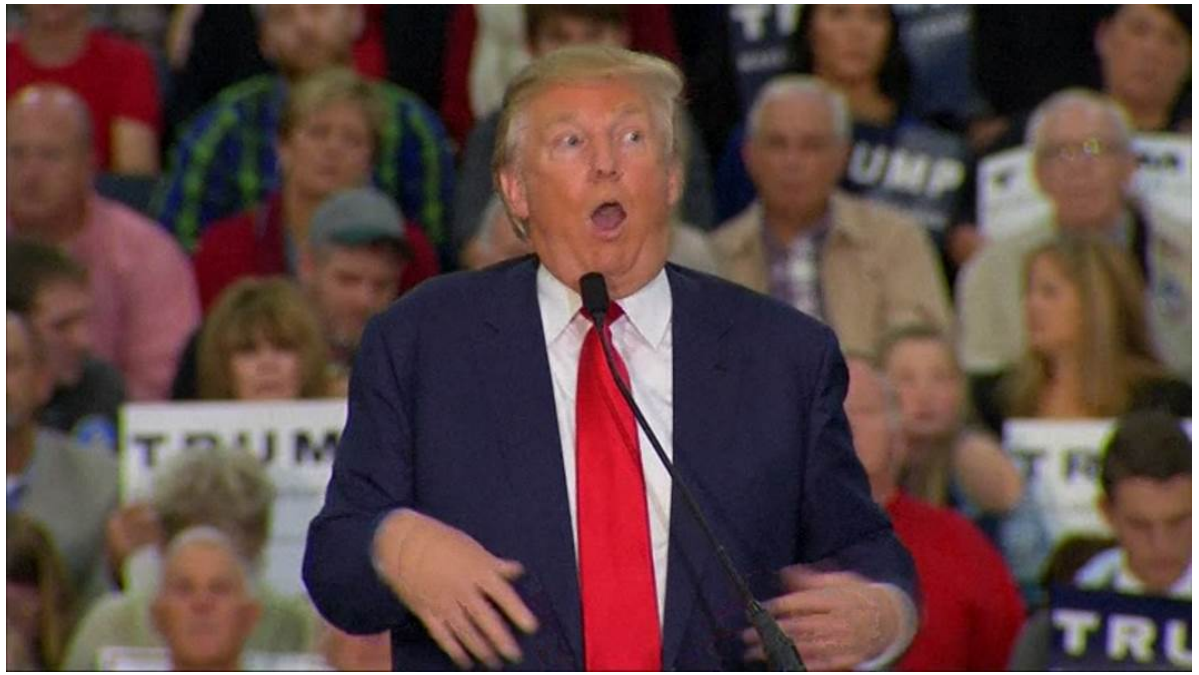
- Password Spraying
  - Find something to auth against
    - OWA, SMB, a domain-connected web app
  - Get domain password policy
  - Think of the worst password you can
  - Make it worse
  - Still too good, make it worse.
    - Password1
    - Welcome1
    - $Companyname1

NB: these are compliant with 'industry standard' (MS default) domain password policy.

  - Try it once with every single account
  - Wait the account lockout cooldown period
  - Repeat

REALLY, REALLY, STUPID

- Dump Username + Description for all accounts from a DC
- Sort by Description
- Weep for humanity



R
E
M
Z
S
C

ADFS [redacted]	User	DO NOT CHANGE PASSWORD - [redacted]
Cert Enrolement	User	DO NOT CHANGE PASSWORD - [redacted]
ADFS [redacted]	User	DO NOT CHANGE PASSWORD - [redacted]
[redacted]	User	DO NOT CHANGE PASSWORD - [redacted]
[redacted]	User	DO NOT CHANGE PASSWORD - [redacted]
Dir Sync	User	DO NOT CHANGE PASSWORD [redacted]
Office 365 Syncronisation	User	DO NOT CHANGE PASSWORD [redacted]
LDAP Remote	User	DO NOT CHANGE PW: [redacted]

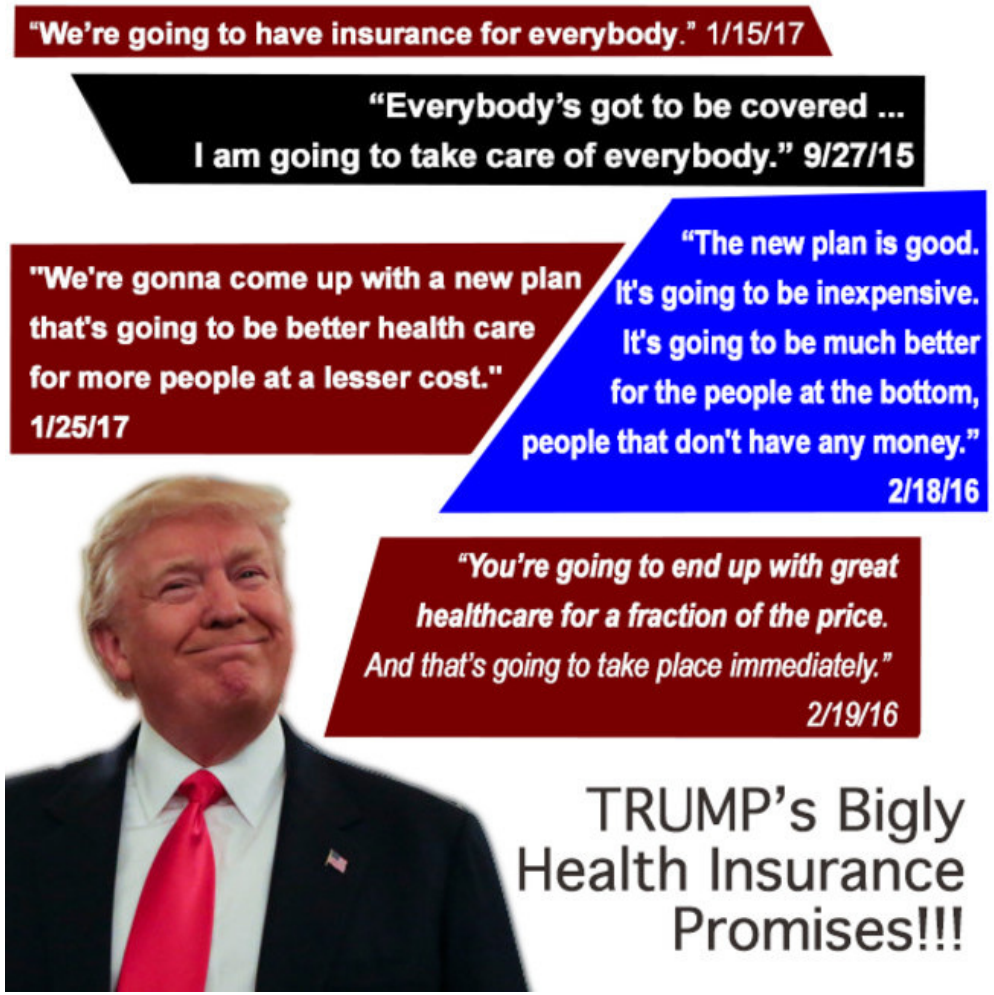
Read other people's emails

R
E
M
Z
S
C

- Use OWA's username enumeration vulns to get valid usernames
- Password spray them
- Search their emails for:
  - password
  - vpn
  - remote access
- Mailsniper is OK
- Ruler is amazing
  - Pop shell using OWA? Yes please!

Make a lot of bullshit promises

- Responder.
- Pretends to be everything to everyone.
- Steals credentials
- Relays NTLM authentication



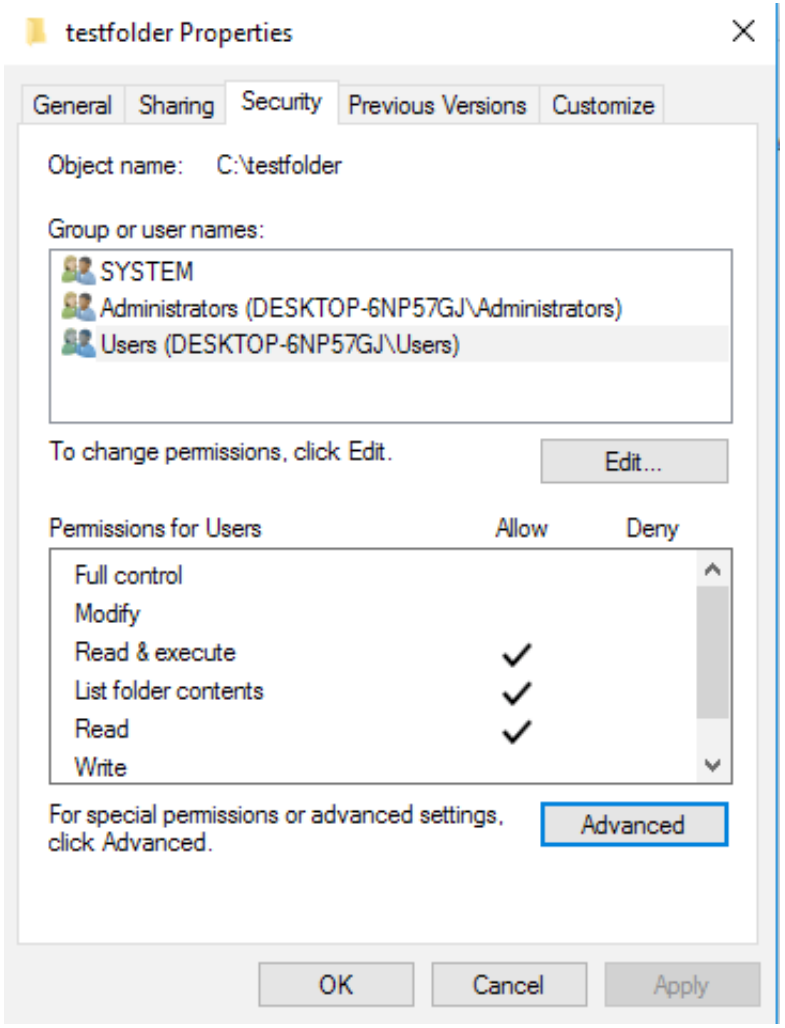
R
E
M
Z
S
C

Dig up your opponent's embarrasing past!

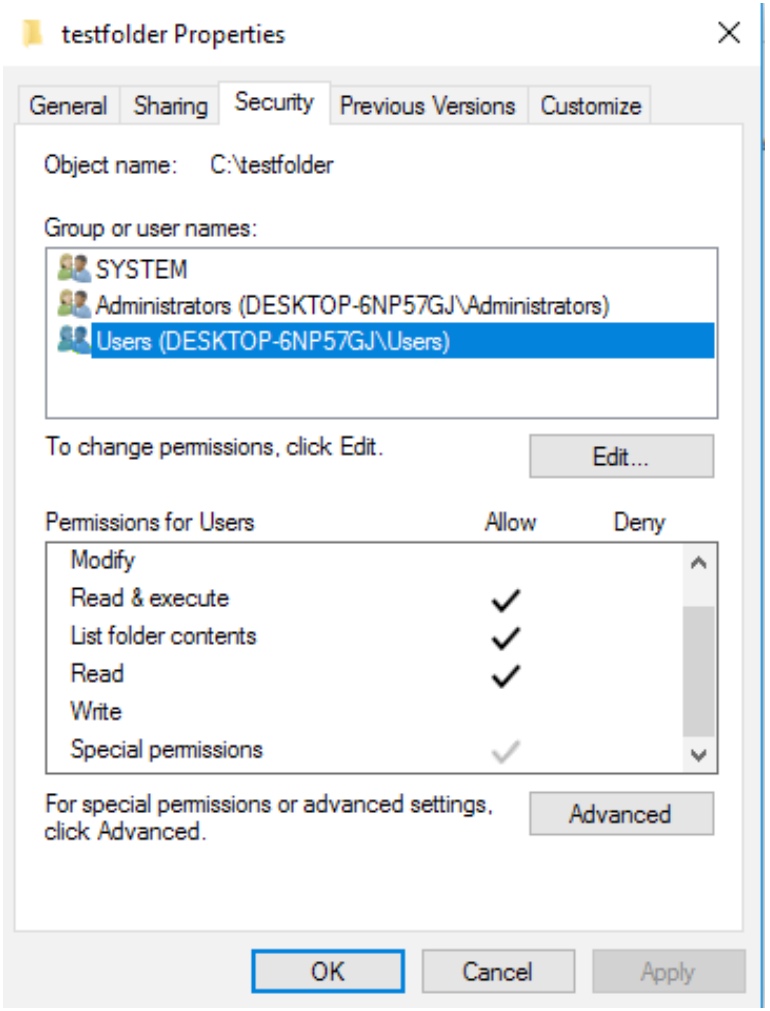
R
E
M
Z
S
C

- Group Policy deserves a talk all of its own
- Use PS Get-GPOReport to dump it all
  - Look for policy that:
    - Runs code
    - Sets reg keys
    - Adds desktop shortcuts or browser bookmarks
  - If code or .lnk file comes from a file share, can you modify it?
    - If it's an .exe and you have 'write' to the dir but not 'modify' on the exe, DLL hijack may still be possible!

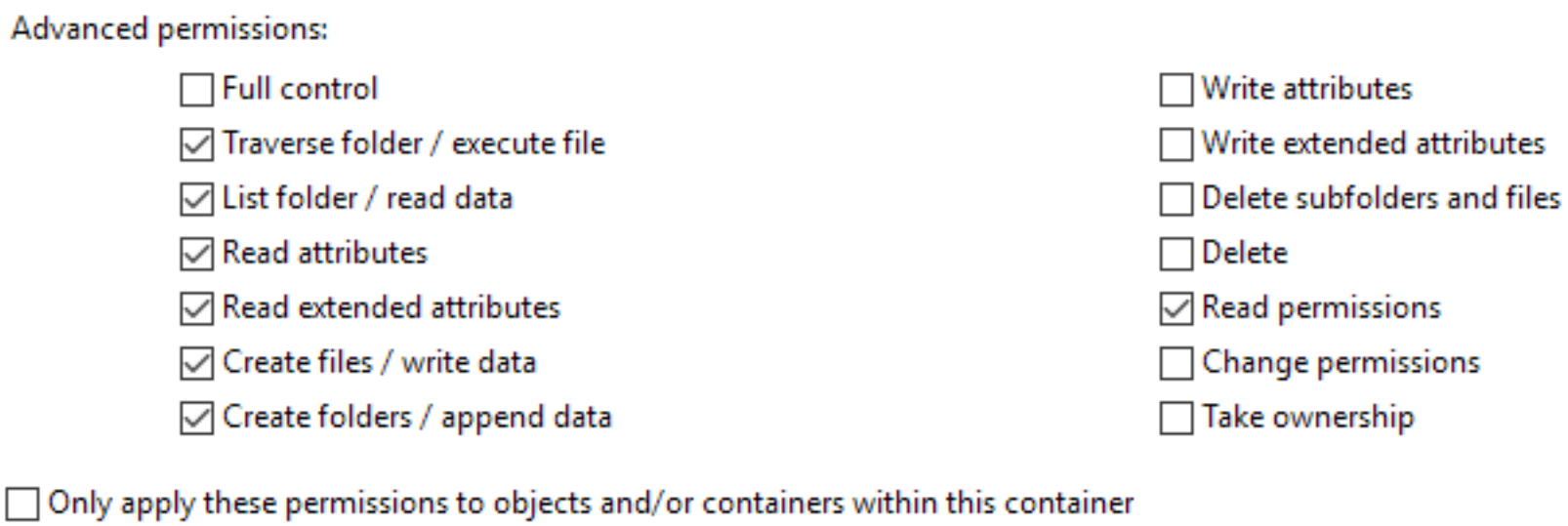
A word on Windows permissions



A word on Windows permissions



A word on Windows permissions



What happens when someone screws up.

More of your opponent's embarrasing past!

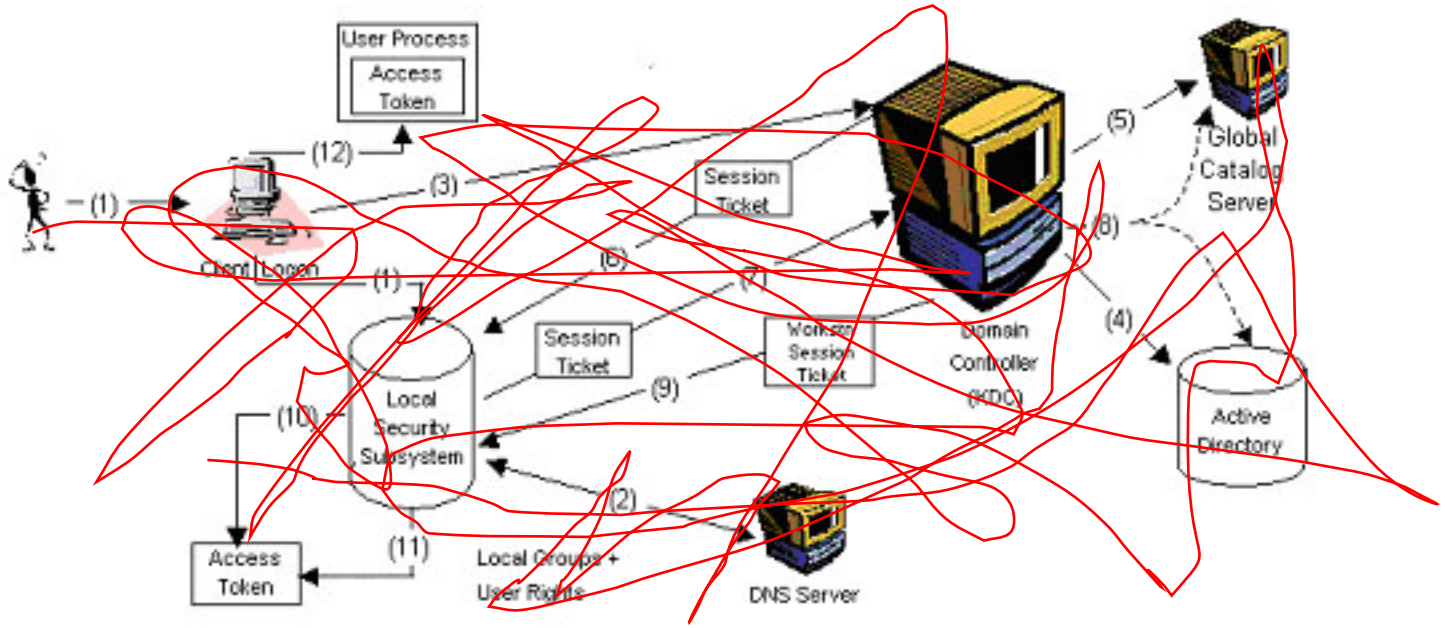
R
E
M
Z
S
C

- Group Policy Preferences Passwords
  - Distributes account credentials to domain computers.
  - Creds are encrypted using a single, global key, that MS publish on TechNet.
  - 'Patched': can't create new policies of this type, but old ones remain.

MORE of your opponent's embarrasing past!

R
E
M
Z
S
C

- Kerberoasting
  - Fuck you, I'm not explaining Kerberos and you can't make me.



tl;dr you ask a domain controller for a thing called a SPN ticket and you crack it offline with john or hashcat.
Mubix's blog has a great writeup on various methods.

Get shady endorsements!

R
E
M
Z
S
C

Gavin Millard @gmillard · 11h
MS14-068 in the real world.
"Welcome Captain. Would you like a coffee before you take off"
#infosec

- MS14-068
  - Only patchable thing I'm covering.
  - Too good not to cover.
  - Only requires that a single DC in the environment not be patched.
  - Equivalent to scrawling 'DOMAIN ADMIN' on your Kerberos ticket in crayon.
- Check for it using responder's FindSMB2UPTime.py script.

Find the IT department's wiki…

R
E
M
Z
S
C

Or raid the company Sharepoint…

- SPartan by Kieran Dennie
- Check out his B-Sides Johannesburg talk
- Securing Sharepoint is HARD.
- Companies that use it often use it for EVERYTHING.

R
E
M
Z
S
C

Use their monitoring systems against them.

- Steal the monitoring account creds, they always have DA.
  - SCOM DB can be decrypted for these.
  - Stand up Responder or Inveigh on an unmonitored machine, add to monitoring, capture authentication.
- Add alert ‘responses’ that run payloads on targets.
- Apply same concepts to backup systems.

R
E
M
Z
S
C

We’re all sick of American politics, let’s have dogs using computers instead.

Workstation and server file systems

R
E
M
Z
S
C

- unattend.xml files
  - Contain base64’d local admin creds
- Cached GPP passwords
  - Like GPP passwords but you don’t even need domain access to steal them!

Workstation and server shares ‘n’ file systems

R
E
M
Z
S
C

- Registry
  - Autologin creds (common on kiosk machines)
  - VNC creds
- Config files with clear text creds
  - Look for file extensions like ini, conf, cfg, config, etc.
  - IIS web.config files are particularly juicy for poaching MS SQL service accounts

Temp Directories

- C:\Temp is a goldmine.

Random “poweruser” file shares

- Use Empire/PowerSploit to find them and scrape them for fun key words like :
  - password
  - config
  - ini
  - Id_rsa
  - *.ppk
  - Etc.
- Often accidentally grant full access to the whole universe.

SYSVOL

R
E
M
Z
S
C

- Special file share synced between DCs
  - All users can read most of it.
- Stores Group Policy stuff, etc.
  - You will find hard-coded creds in these scripts.
- Used by crappy admins as general storage
  - passwords,
  - critical docs,
  - n00dz,
  - etc.

If you already have local admin rights…

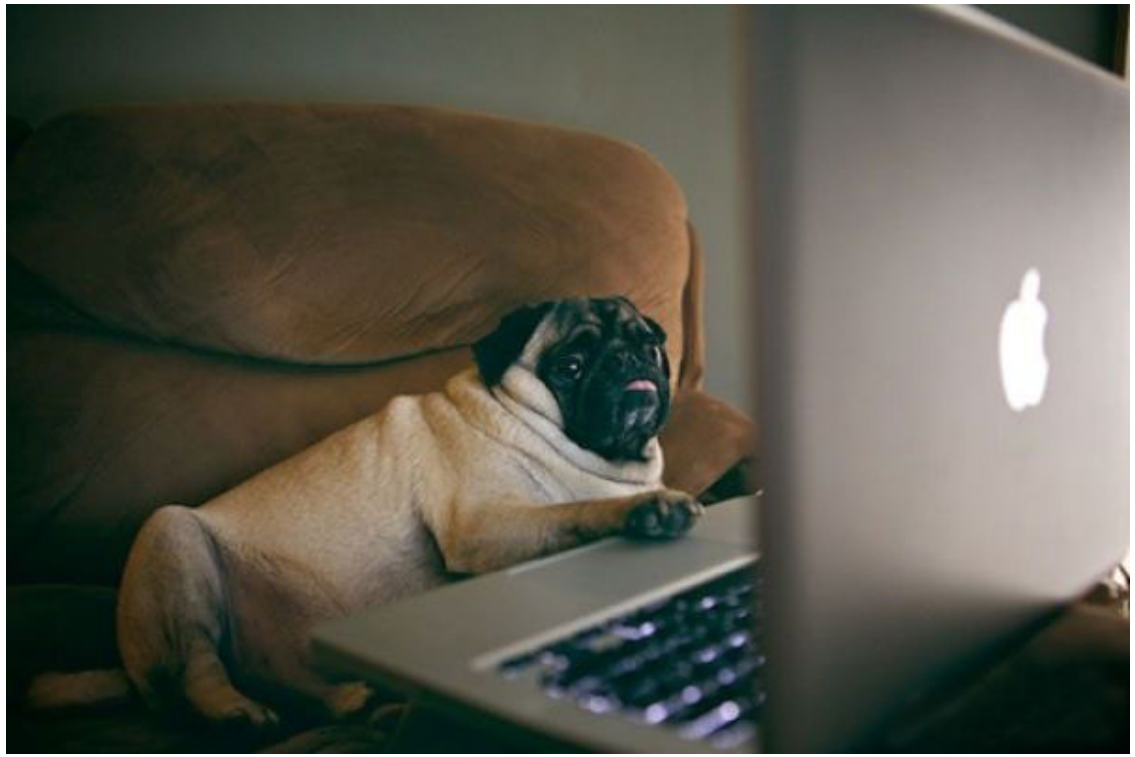
R
E
M
Z
S
C

- Mimikatz – by Benjamin Delpy aka gentilkiwi
  - You know it dumps hashes and passwords.
- If mimikatz only gets you hashes:
  - If LM hash - crack that hash (in about a minute)
  - If MSCachev2 hash - crack that hash (might take a while)
  - If NTLM hash - pass that hash (if you can’t crack it)
- Steal the Kerberos ticket of any active session
  - Impersonate user, do stuff on other machines.

If you can own a sysadmin’s workstation…

R
E
M
Z
S
C

- Password vaults
  - more often password spreadsheet
  - or just ’passwords.txt’.
  - There’s always a file.
- Keyloggers and clipboard monitors!



Hypervisors and backup servers

R
E
M
Z
S
C

- Physical access = you own it.
- Virtual physical access = you still own it.
- Got a copy of the backups = you still own it.
- Can modify the backups = you probably own it forever.

Hypervisors and backup servers

R
E
M
Z
S
C

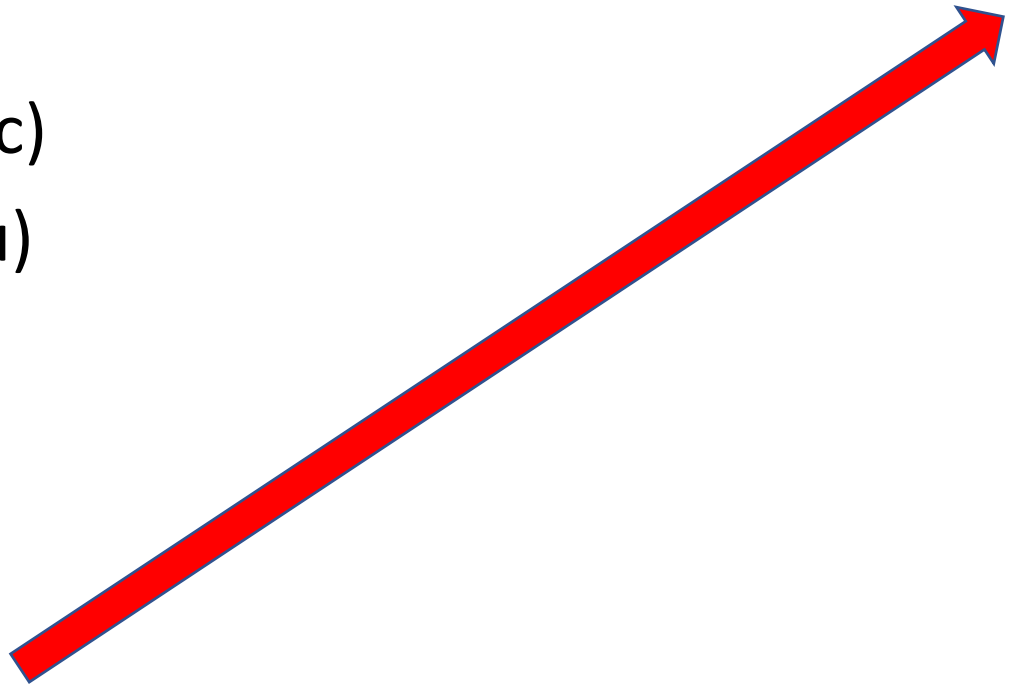
- Copy .vhd or .vmdk files from a hypervisor
- Workstation or member server
  - HKEY_LOCAL_MACHINE\SAM - C:\Windows\system32\config\SAM
  - HKEY_LOCAL_MACHINE\SECURITY - C:\Windows\system32\config\SECURITY
  - HKEY_LOCAL_MACHINE\SYSTEM - C:\Windows\system32\config\system
- Domain Controllers
  - C:\Windows\system32\NTDS.DIT
  - C:\Windows\system32\config\system

Hit me up on twitter for the slides or a chat about breakin stuff.

@mikeloss

ACK

- Asterisk in general (@asteriskinfosec)
- Dave Taylor in particular (@dave_au)
- Andrew Kitis (@nanomebia)
- Uprights everywhere!
- and flats too…
- And the guys who make all of these



R
E
M
Z
S
C