External Network Pen Test 2

- Content Discovery
  - Dictionary based
  - Against ***Web Service*** discovered during scanning
- Password Spraying
  - Against login portals
  - Lockout!
    - Frequency approved by customer
    - And fellow testers on engagement
- Social Engineering involved?
  - Not likely
- ***Does NOT include authenticated Web App Testing***

"Yep... Someone did a web test without checking..."

Internal Network Pen Test

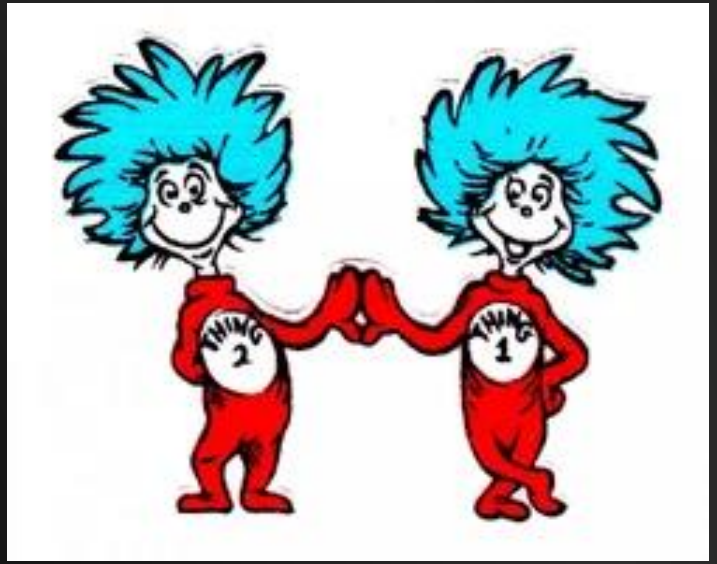
- Similar methodology to the External
- Vulnerability Scanning
- Protocol Abuse
  - LLMNR
  - NBNS, etc.
- Password Spraying
  - Utilizes SMB... Unless there is something better
  - Once again coordinate and approve
  - Please.... coordinate and approve

Internal Network Pen Test 2

- Exploitation
  - ***Demonstrate impact!!!***
  - ***Showcase failures as well***
- No Social Engineering
- If time allows:
  - Pivot/Assumed Compromise attempts
  - Coordinate with other testers and the customer

Assumed Compromise Assessment

- What happens when an attacker gets on a system
- Start with a standard system
  - Standard User
  - Domain Joined system
- A quick note on AV bypass....
  - It is getting expensive
  - Generally not used here
  - Wrong goal
- Generally does not include a vuln scan



Hi! We are in your network!

Assumed Compromise Objectives

- Find unencrypted sensitive data (to be identified by Test)
- Attempt to locate employee PII
- If applicable, privilege escalation from the non-admin user to gain access to privileged shares
- Attempt to "crack" any found password hashes & provide guidance on best practices for password creation and management
- Attempt to gain access as a domain administrator in order to gain access to sensitive data
  - Notice... This is last.

Assumed Compromise Assessment

- Host Configuration Analysis
  - Identify security protocols
  - Unidentified installation files
  - Enumeration of local users and groups
  - Bypassing of security tools
  - Review file systems
  - Review of customer applications

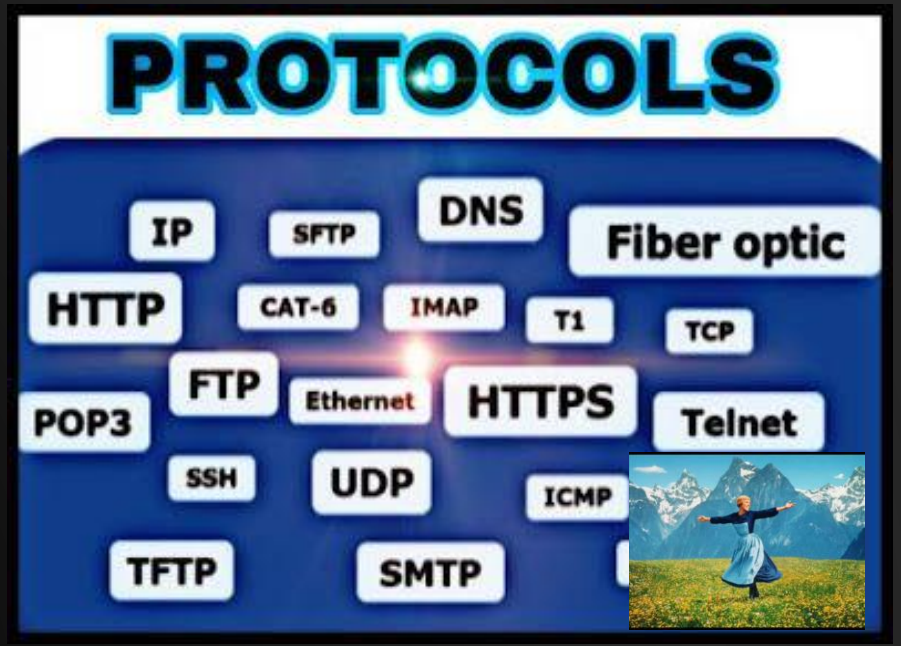
Assumed Compromise Assessment 2

- Local privilege escalation
  - Increase attack opportunities
- Domain SYSVOL Analysis
  - Can house logon scripts
  - Group Policy Definitions
- AD Configuration Analysis
  - Increased attack surface
  - Increased situational Awareness
  - Build an offline representation of AD and session state

On My Way to DA!!!

Assumed Compromise Assessment 3

- Protocol Abuse
  - IPv6
  - Kerberos
  - LLMNR and NBNS
  - Microsoft SQL Server
  - RDP
  - SMB
  - Email



Assumed Compromise Assessment 4

- Credential Harvesting
  - From Protocol Abuse
  - Malicious URLs and LNK files
  - ***Browser Profile analysis***
  - Registry analysis
  - Token stealing
  - Memory analysis
- Password Spraying
  - Similar to Internal Network Pen Test
  - With a goal on demonstrating Weak Password Policies and expand access to environment

C2 Test

- Testing what can be let out of a company
- HTTP, HTTPS, DNS, ICMP, QUIC, etc.
- Testing detective controls for egress
- Usually paired with other testing

More C2 Test

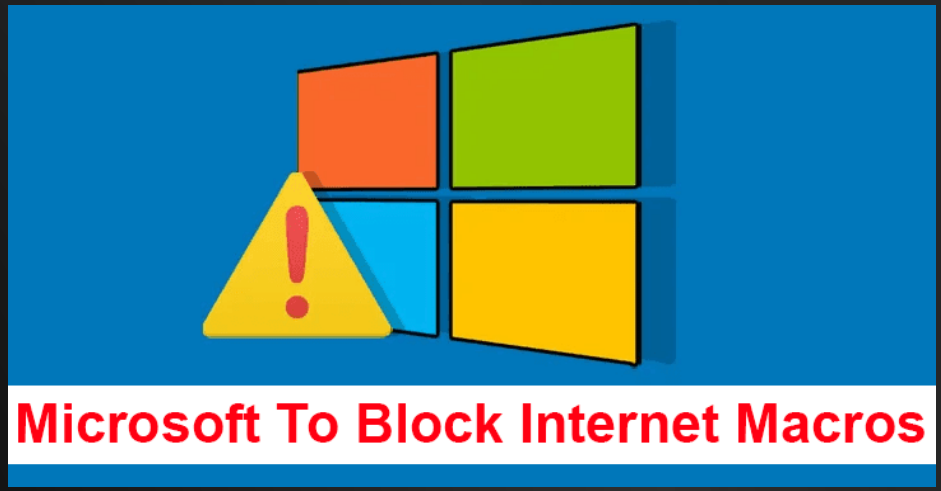
- Host configuration analysis
  - Enumerate installed security products
  - Enumerate local and group memberships
  - Evaluate Administrative utilities
  - Command line a PowerShell logging enabled?
  - Evaluate Installed Applications
  - Does application control exist
  - Office macros execution
  - RDP access to local resource sharing and clipboard

C2 Test Part 2

- Local Privilege Escalation
  - Escalation can allow tool installation and disabling of alerts and tools
  - Also done on an Assumed Compromise test
- Egress Filtering Analysis
  - Can ICMP, TCP or UDP connectivity be achieved?
  - Used to inform payload generation
  - Proxy based firewalls may produce false positives
  - Email

C2 Test Part 3

- Web Content Filtering Analysis
  - Access to?
    - Social Media Sites
    - Personal Email
    - File Transfer sites
  - Prevent access to
    - Scripts
    - Binaries
    - Macro Enables Software
    - Encrypted Office Documents
    - Common Malware file types



Someday....

C2 Test Part 4

- Web Content Filtering Analysis part 2
  - Can a user browse or retrieve content from
    - A Raw IP Address
    - Uncategorized Domain
    - A recently categorized domain
    - A CDN Relay
- What are the capabilities of the Content Filtering Solution
  - Is there a client side component?
  - ***Is there a cloud based component?***

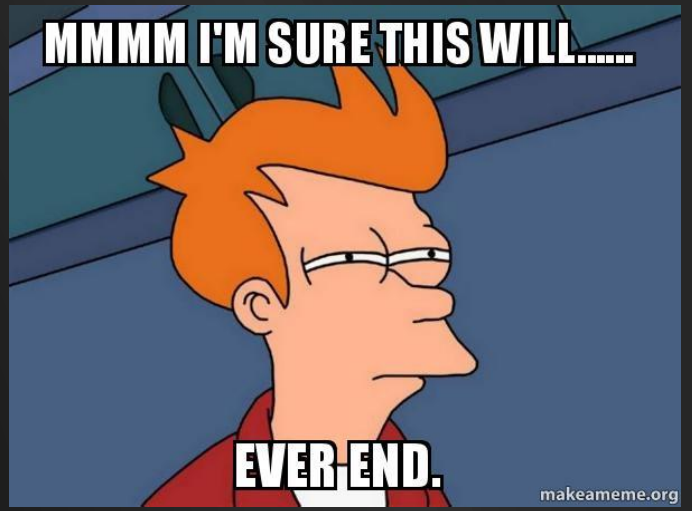
C2 Test Part 5

- Email Filtering Analysis
  - Prevent access to
    - Archive or Encrypted Scripts
    - Archive or Encrypted Binaries
    - Archive or Encrypted Macro enabled documents
    - Encrypted Office Documents
    - Common Malware file types
  - Is URL Rewriting being used
    - Can it be bypassed?
    - Is a sandbox being used for email attachments?

Sup?

C2 Test Part 6

- VPN Client Configuration Analysis
  - Used when clients send you one of their laptops to conduct testing
  - Split tunneling?
  - Host Name checking?
  - Is MFA utilized?
- Commodity Payload Analysis
  - Probably require use of custom malleable C2 profiles
- Covert Channel Analysis
  - Generate payloads that are capable of using covert channels (ICMP, DNS, DNS-over-HTTPS)



Quick question…

- Can we really test all the above in a "stealthy" test?
- Expectation management

Physical

- Description
  - Attempt to bypass controls
  - Social Engineer employees
  - Assessment / Light touch
- Techniques
  - Lockpick, shimming, bypass
  - Lying, cheating, stealing, spoofing employee or vendor
  - Windows, roofs, tunnels, etc.

Physical

- Rules of Engagement
  - Clear boundaries
  - Get out of Jail Free
  - Assessment / Light touch
- Never
  - Break/Damage
  - Get extreme in evasion or resistance
  - People can get hurt and customers will get upset
  - How a Hacker's Mom Broke Into a Prison—and the Warden's Computer | WIRED

Wireless

- Description
  - Assess and compromise wireless client and access point security
  - Focus on authentication and encryption
- Objectives
  - Analyze protocols available
  - Configurations
  - Physical attacks
  - Client attacks

Wireless

- WPA2-Enterprise
  - Requires user interaction to attack
  - Remote access into corporate network
  - RDP access to wireless client using domain creds
  - Wired and wireless access to customer system so wireless connectivity can be manipulated by tester

Wireless

- WPA2-PSK
  - Generally these do not require interaction to test PSK strength
- Open Guest Networks
  - Include WPA2-PSK networks for non-corp access
  - Testers attempt PSK cracking and cred recovery
  - If access not obtained customer provides creds to facilitate segmentation testing
    - Corporate-noncorporate

Web App Pentests

- Very much a grey area
- Absolutely used in pentesting
- But..
- It is also its own full test
- Usually used as a means to an end
  - Access….
- Never proport to be a full assent of a web server
- How to report this?