OFFENSIVE DEFENCE
OWASP day, Auckland
Consultant
@ Aura Information Security
www.aurainfosec.com
WE NEED MASS AWARENESS OF THESE COMMON ISSUES
WE NEED **MASS** REMEDIATION OF THESE COMMON ISSUES
30 minutes of your mind
This is My Jam!

RASPBERRY, CHERRY, & DARK CHOCOLATE

Reduced Sugar Jam
Handmade in Bermondsey
Internal Pen Test Recap:

An internal penetration is conducted from the perspective of an unauthenticated internal attacker with physical access to the network, or an external attacker who has achieved a foothold on an internal system.
Defenders

TEAM BLUE

VS

TEAM RED

Attackers
1. Grab a desk
2. Gather Interesting Information
   - User Enumeration, System Information
3. Become a low-level/local admin user
4. Escalate to domain admin
PLAN A: 2017/2018

1. Grab a desk
2. Gather Interesting Information
   - User Enumeration, System Information
3. Become a low-level/local admin user
4. Escalate to domain admin
90% Owned

13 Years

#celebration
ALL THESE NETWORKS HAVE THE SAME PROBLEMS
#1 : NULL Sessions

An anonymous connection to a computer which can be used to gather information about the system.

- Disabled by default on newer versions of Windows.

The Problem

- If allowed, Domain Controllers will return the complete list of domain users, groups, and group membership to aid an attacker.
Group 'Domain Admins' (RID: 512) has member: ACME\research2
Group 'Domain Admins' (RID: 512) has member: ACME\ADM-Charlie
Group 'Domain Admins' (RID: 512) has member: ACME\MeganR
Group 'Domain Admins' (RID: 512) has member: ACME\ADM-Keifer
Group 'Domain Admins' (RID: 512) has member: ACME\A.jordaan
Group 'Domain Admins' (RID: 512) has member: ACME\ADM-Hobson
Group 'Domain Admins' (RID: 512) has member: ACME\BackupAkl
Group 'Domain Admins' (RID: 512) has member: ACME\adm-luke
Group 'Domain Admins' (RID: 512) has member: ACME\QTSupplier
Group 'Domain Admins' (RID: 512) has member: ACME\stevej
Group 'Domain Admins' (RID: 512) has member: ACME\backupexec
Group 'Domain Admins' (RID: 512) has member: ACME\ADM-Neil
Group 'Domain Admins' (RID: 512) has member: ACME\ADM-Tony
Group 'Domain Admins' (RID: 512) has member: ACME\b.furn
Group 'Domain Admins' (RID: 512) has member: ACME\c.philbert
Group 'Domain Admins' (RID: 512) has member: ACME\domainscan
Group 'Domain Admins' (RID: 512) has member: ACME\jkeagan
Group 'Domain Admins' (RID: 512) has member: ACME\fortinet
Group 'Domain Admins' (RID: 512) has member: ACME\mtest

>_enum4linux output sample
Enum4linux
A wrapper around the Samba tools
- smbclient, rpcclient, net nmblookup

https://tools.kali.org/information-gathering/enum4linux
#2 Server Message Block (SMB) Signing

SMB is a file protocol mostly used by windows systems primarily to provide shared access to files, printers, network locations etc.

- Signing is disabled by default on Windows systems (except Domain Controllers)

The Problem

Attacker can perform **SMB Relay** attacks against systems with signing disabled, gaining a foothold.
Relaying credentials for these users:
[ Administrator ]

Retrieving information for: 2...

SMB signing: False
Os version: 'windows 7 Enterprise 7601 Service Pack 1'
Hostname: ' '
Part of the domain

[+] Setting up SMB relay with SMB challenge: 990509b1d6be058a
[+] Received NTLMv2 hash from: 10. False
Nmap scan report for acme1.acme.com (172.16.10.23)
Host is up (0.00043s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode: |
| account_used: guest |
| authentication_level: user |
| challenge_response: supported |
| messageSigning: disabled (dangerous, but default) |
# 3: Link-Local Multicast and NetBIOS Name Resolution

Two components of Microsoft Windows, which helps machines on the same subnet to find each other when DNS fails.

**The Problem**

Attacker can intercept and respond to these requests, to capture password hashes > crack weak passwords.
LLMNR / NBT-NS Poisoning

1. Connect to \pintserver
2. I don’t know that one
3. Anyone know \pintserver ???
4. Yes!! It’s right here!
5. OK! Here are my credentials:

Attacker

Victim

DNS Server

Stern Security LLC
BlueTeam Guidance

Responder
Metasploit

https://github.com/lgandx/Responder
Weak and default passwords are frequently detected. Domain and local account password policies enforce the company password requirements. Password reuse.

The Problem

- The industry requirements are difficult, so users construct passwords following predictable patterns. Captured hashes are more likely to be cracked.
BlueTeam Guidance

Hashcat

https://hashcat.net/hashcat/
#5: Out of Date Software

Software Vendors release new versions to fix bugs. Eventually software becomes deprecated (EOL) and replaced completely.

The Problem

Patches seem to take between 3 months and ‘infinity’ to be installed.
ARE WE PROTECTED FROM THIS NEW ATTACK?
I DON'T KNOW...
BlueTeam Guidance

Nmap (has scripts for several vulns)

OpenVAS (free)

- Community version of Nessus

Metasploit Framework

https://www.openvas.org
[+] 10.7.39.161:445 - Host is likely VULNERABLE to MS17-010!
[+] 10.7.39.171:445 - Host is likely VULNERABLE to MS17-010!
(Windows 7 Enterprise 7601 Service Pack 1)
Service accounts are created by Admins to install, configure and operate software applications. e.g. backup software, anti virus.

The Problem

• Service accounts are often excluded from security policies i.e MFA, password expiration
• Excessive privileges
<UNCSite Type="repository" Name="Christchurch Repository" Order="2"
Server="chrv01" Enabled="1"
Local="0"><ShareName>mcafeeEPO5.1$</ShareName><RelativePath></RelativePath>
<UseLoggedonUserAccount>0</UseLoggedonUserAccount><DomainName>ACME</DomainName><UserName>McafeeEpo_SVC</UserName><Password Encrypted="1">kDTrFXsR/abAFPM9B3Q==</Password></UNCSite><UNCSite Type="repository" Name="Dunedin Repository"
Order="3" Server="dnsrv01" Enabled="1"
Local="0"><ShareName>McafeeEPO5.1$</ShareName><RelativePath></RelativePath>
<UseLoggedonUserAccount>0</UseLoggedonUserAccount><DomainName>ACME</DomainName>
### Password decryption tool for the McAfee SiteList.xml file

<table>
<thead>
<tr>
<th>Branch: master</th>
<th>New pull request</th>
<th>Create new file</th>
<th>Upload files</th>
<th>Find file</th>
<th>Clone or download</th>
</tr>
</thead>
<tbody>
<tr>
<td>funoverip</td>
<td>Cleaning up IV</td>
<td>Latest commit 3665de8 on 12 Feb 2016</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>README.md</td>
<td>Typo fix (French != English)</td>
<td>2 years ago</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mcafee_sitelist_pwd_decrypt.py</td>
<td>Cleaning up IV</td>
<td>2 years ago</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BlueTeam Guidance

Enum4linux, but simpler to just review AD

https://tools.kali.org/information-gathering/enum4linux
There is no acceptable excuse to be at risk to 20 year old vulnerabilities....
Summation

Thank you for your time
No Wait There’s More

(code for: “I went to fast and finished early”)