BREACH TO CDE ALL ROADS LEAD TO DOMAIN ADMIN

A SECTOR CONFERENCE PRESENTATION
OCTOBER 2016
Introduction

Yannick Bedard
Security Consultant
Network Penetration Testing
SpiderLabs, Trustwave

email: ybedard.infosec@gmail.com
twitter: @swordgardctf
Disclaimers

- Always test tools in a controlled environment

- Domain admin is not a goal, it is a mean to an end

- Standing on the shoulders of giants: @PythonResponder, @harmj0y, @mubix, @waldo_, @mattifestation, @hashcat, etc…
Presentation motivation

- Corporate networks are Windows based.
- Sysadmins lack:
  - Proper tools
  - Training
  - Time
- Compliance is often required
- Vuln. assessment ≠! pentest
Attack surface overview

1. Traffic Manipulation
2. Password-based protocols
3. Weak security defaults
4. Unsecured protocols
5. Shared passwords
6. Privilege escalation
Initial Reconnaissance

1. Identify domain controllers via DHCP/DNS
2. Arp-scan and NBT-scan for host discovery
3. Check for null session on domain controllers
   1. LDAP Null bind
   2. RPC/SMB Null sessions
Vulnerability scanning

- Last resort:
  - Least successful attack vector
  - Highest noise-ROI
  - Shell-oriented scanner is best
  - See YASUO by @0xaubye
- Remediation:
  - Good patching cycle
  - Change default passwords
Brute forcing attempts

- Dangerous on domain-joined appliances/services
- Domain accounts bruteforcing
  - Standard
  - Vertical (password spraying)
- Remediation:
  - Lock accounts
  - Log/monitor failed attempts
Traffic manipulation

- Multiple layers are vulnerable
- Very stealthy
- A mean to one of two ends:
  - Capturing sensitive traffic
  - Modifying traffic on the fly
# Traffic manipulation

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacker tool</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NBT-NS</td>
<td>Responder, Inveigh, Metasploit, Buttercup</td>
<td>DHCP WINS</td>
</tr>
<tr>
<td>LLMNR</td>
<td>Responder, Inveigh, Metasploit, Bettercap</td>
<td>Disabled via GPO, Registry Fix</td>
</tr>
<tr>
<td>ARP Spoofing</td>
<td>Ettercap, Bettercap, Mitmf</td>
<td>NAC-enabled switch</td>
</tr>
<tr>
<td>DHCP (Inform)</td>
<td>Responder (tool), Bettercap</td>
<td>DHCP snooping</td>
</tr>
<tr>
<td>ICMP Redirect</td>
<td>Responder (tool), Metasploit</td>
<td>Disable via GPO, Registry Fix</td>
</tr>
</tbody>
</table>
Capturing traffic

- Capture existing traffic using Pcredz
- Use Responder to generate authentication attempts
- Cleartext passwords
- Cookies in HTTP traffic
- NetNTLMv1, NetNTLMv2 and Kerberos TGT-REQ
Modifying traffic

- Ask for basic authentication (Responder HTTP server).
- Inject code/shells in HTTP traffic
  - HTA
  - Java applets
  - CHTM
  - MS16-051 + powershell
- Backdoor Excel files with macros on the fly for SMB traffic
- Backdoor exes in HTTP with MITMf or BackdoorFactoryProxy
NetNTLM relay

- Both v1 and v2 can be relayed.
- Same-host-protocol relay not possible.
- Cross-protocol relaying possible.
- Multiple relays possible from a single connection using Snarf.
## Traffic manipulation

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Domain machines</th>
<th>Domain controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Can’t be signed</td>
<td>Can’t be signed</td>
</tr>
<tr>
<td>SMB</td>
<td>Not signed</td>
<td>Signed</td>
</tr>
<tr>
<td></td>
<td>pre-Windows 10</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Not signed</td>
<td>Not signed*</td>
</tr>
<tr>
<td>MSChap (netntlmv1)</td>
<td>Not verified (TLS)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
NetNTLM relay impacts

- Remote Code Execution (SMB Relay)
- Access to services (SMB, webmail, outlook, etc)
- Adding local or domain users (SMB and LDAP)
- Local Privilege Escalation
  - Potato
  - RottenPotato
Traffic manipulation remediation

- Disable NetNTLM
  - Use Kerberos instead
  - Enable signing in netntlm
- Enable TLS where possible
- Use Network Access Controls
- Limit system communications
  - Between workstations
  - Between servers
Password cracking

- Windows authentication protocols are password-based
- Use fast hashing methods or encryption
  - NetNTLMv1/MSChap DES-based
    - Breakable in 14 days and less
  - NetNTLMv2 is MD5-based
    - Weak, but better
  - Kerberos tickets are AES or RC4 based
    - Still weak, but again better
Password cracking

- By default, weak passwords are allowed
- GPUs are faster and cheaper than ever
- “Strong” passwords are still often predictable.
  - Password1!
Password cracking costs

- GTX 1060 (200$): 750 Million hashes/s
- GTX 1070 (450$): 1500 Million hashes/s
- GTX 1080 (800$): 2250 Million hashes/s
- Titan X (1200$): 3000 Million hashes/s

Bar chart showing the cracking rates for NetNTLMv2 and Kerberos RC4 for different GPUs.
Derivative local administrator

- Initial foothold already existing.
- Recover credentials
  - Cached cleartext
  - NTLM
- Look for new system that can be compromised using these.
- Rinse and repeat until Domain Admin
Derivative local administrator

- Oldest method of lateral spread.
- Shortest-path to D.A. can now be found using scripts!
- Remediation:
  - Log off after remote desktop
  - Disable cleartext passwords in memory
  - Segregate privileged accounts
Derivative local administrator
Derivative local administrator
Local administrator password

- If pushed via GPOs:
  - Available to any domain-joined user
  - Easily reversible
- Remediation:
  - Use a randomized password per machine
  - LAPS by Microsoft can be used
Summary

- Limit NetNTLM in favor of Kerberos
- Do frequent password audits
- Principle of least privilege
  - Directly
  - Indirectly
- Invest in:
  - Detection tools (Microsoft ATA)
  - Active Directory security training
Yannick Bedard
Security Consultant
Network Penetration Testing, SpiderLabs
Trustwave

cold:  ybedard.infosec@gmail.com
twitter:  @swordgardctf