All the Cool Kids Are Red Teaming
Should You Be Drinking the Kool-aid Too?

Exploring Different Approaches to Penetration Testing

Cara Marie
NCC Group
ISSA-LA Aug 2017
Obligatory About Me

- NCC Group Principal Security Consultant
  Pentested numerous networks, web applications, mobile applications, etc.
- Hackbright Graduate
- Ticket scalper in a previous life
- @bones_codes | cara.marie@nccgroup.com

Not me, but sometimes I channel her ;)}
Why?

1. What are your most important assets in your company?
2. How would an attacker get access to them?
   Likely not through a single system or application – probably through a combination of things
3. Hence Red Team
Red Team Benefits

- Understand the impact of a security breach
- Identify weaknesses in development and testing processes
- Test incident response capabilities
- Demonstrate security controls – justify security spending
Nobody likes a sad panda...
DANGER
OPEN PIT
PROCEED WITH CAUTION
Security Assessment Flavors

Vulnerability Assessment

Penetration Test

Red Team
Breadth

Vulnerability Assessment

Depth

Penetration Test

Red Team
Threat Model
(environment, system, application, etc.)
Hard Candy Outside, Soft Gooey Center

Guaranteed results from an external-only approach to security
Insider Threats

- Employee
- Third-party Contractor
- Client

- Deliberate / Malicious
- Compromised / Accidental
Trust your employees, but don’t allow unrestricted access across the organization.
Threat Model
(environment, system, application, etc.)

Vulnerability Assessment
Vulnerability Assessment

Goals / Purpose

- Identify as many vulnerabilities as possible
- Prioritize these vulnerabilities for remediation

Exploitation is **NOT** a requirement
BUILD YOUR DEFENSE
We Run [INSERT VULN SCANNER]
We Don’t Need A Pentest

Yes, this is an argument I’ve heard...
Gaps in Automated Vulnerability Scanning

- Ratings lack context
- Risk ratings can be wrong/misleading
- More noise than signal (if misconfigured)
- Encourages “set-and-forget”
Host script results:
 CLOCK-SKEW: mean: -1s, deviation: 0s, median: -1s

Nmap scan report for 18.62.20.52
Host is up, received user-set (0 001s latency).
Not shown: 72 filtered ports
Reason: 72 no-responses

Reason: 72 no-responses
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 126 Microsoft IIS httpd 7.5

http-methods:
| Supported Methods: OPTIONS TRACE GET HEAD POST
| Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/7.5

http-title: IIS7

135/tcp open msrpc?
139/tcp open netbios-ssn?
445/tcp open microsoft-ds?
8081/tcp open tcpwrapped

| mcafee-espo-agent: ePO Agent not found
49153/tcp open unknown
49154/tcp open unknown
49277/tcp open unknown

1 service unrecognized despite returning data. If you know the service/version, please submit it following fingerprint at https://nmap.org/cgi-bin/submit.cgi

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.16.50.50
Host is up, received user-set.
Scanned at 2017-07-31 17:59:36 PDT for 7s

PORT STATE SERVICE REASON
80/tcp filtered http no-response
135/tcp filtered msrpc no-response
139/tcp filtered netbios-ssn no-response
443/tcp filtered https no-response
445/tcp filtered microsoft-ds no-response
7343/tcp filtered swx no-response
8081/tcp filtered blackice-icecap no-response
8443/tcp filtered https-alt no-response
9084/tcp filtered aurora no-response
9443/tcp filtered tungsten https no-response
18443/tcp filtered unknown no-response
49153/tcp open unknown
49154/tcp open unknown
49277/tcp open unknown

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Threat Model (environment, system, application, etc.)

Vulnerability Assessment

Penetration Test
Trust but 

VERIFY
Penetration Test

Goals / Purpose

- Assess the risk of compromise
- Scoped to specific environment, system or application

Does **NOT** provide an accurate demonstration of incident response systems
## Host Details

**Host:** Win2k8SP1 | **IP Address:** 192.168.71.159

### Vulnerabilities

<table>
<thead>
<tr>
<th>Level</th>
<th>ID</th>
<th>Description</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>MS11-058</td>
<td>Vulnerabilities in DNS Server Could Allow Remote Control</td>
<td>Windows</td>
</tr>
<tr>
<td>high</td>
<td>MS08-040</td>
<td>Microsoft SQL Server Multiple Privilege Escalation Flaws</td>
<td>Windows</td>
</tr>
<tr>
<td>high</td>
<td>MS09-004</td>
<td>Vulnerability in Microsoft SQL Server Could Allow Local to Remote Code Execution</td>
<td>Windows</td>
</tr>
<tr>
<td>high</td>
<td>MS12-020</td>
<td>Vulnerabilities in Remote Desktop Could Allow Remote Code Execution</td>
<td>Windows</td>
</tr>
<tr>
<td>high</td>
<td>Multiple Vendor DNS Query ID Field Prediction Cache Poisoning Flaws</td>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>medium</td>
<td>Terminal Services Encryption Level is Medium or Low</td>
<td>Misc.</td>
<td></td>
</tr>
<tr>
<td>medium</td>
<td>Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Attack</td>
<td>Windows</td>
<td></td>
</tr>
</tbody>
</table>
Starting Nmap 7.50 (https://nmap.org) at 2017-08-16 13:56 PDT
Nmap scan report for scan.nmap.org (45.33.49.119)
Host is up (0.036s latency).
Other addresses for scan.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe98:ff4e
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered ports
PORT  STATE      SERVICE     VERSION
22/tcp open  ssh  OpenSSH 6.6.1 (protocol 2.0)
 | ssh-hostkey:
 | 2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:2f:0a:2a:3b:6d (RSA)
25/tcp open  smtp  Postfix smtpd
 | smtp-commands: ack.nmap.org, PIPELINING, SIZE 102400000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp open  http  Apache httpd 2.4.6
 | http-server-header: Apache/2.4.6 (CentOS)
 | http-title: Did not follow redirect to https://nmap.org/
113/tcp closed  ident
443/tcp open  ssl/ssl  Apache httpd (SSL-only mode)
 | http-server-header: Apache/2.4.6 (CentOS)
 | http-title: Did not follow redirect to https://nmap.org/
 | ssl-cert: Subject: commonName=www.nmap.org
 | Subject Alternative Name: DNS:www.nmap.org, DNS:nmap.org
 | Not valid before: 2015-01-17T14:41:49
 | ssl-date: 2017-08-16T20:56:55+00:00; 0s from scanner time.
Service Info: Host: ack.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.83 seconds
root@HPLaserJet:~ #
Last Hackers movie reference – I promise...
A penetration test is, in the simplest of terms...

Systems = Infra + App

PT = Systems (Discovery + Exploitation)

- For the Win!
Default credentials + HTTP PUT method against */*
- excellent configuration ESPECIALLY when exposed to the Internet...
A. Find external entry vulnerabilities

B. Find internal entry vulnerabilities

1. Gain any domain credentials to facilitate intel gathering on the network

2. Gain privileges of Local SYSTEM on Domain Member Servers

3. Traverse to different servers looking for powerful tokens & hashes

4. Steal tokens and hashes for powerful domain users & administrators

5. Use domain admin against Business

- Profit!
Red Team

Goals / Purpose

- Assess end-to-end modeling of real-world threat actor techniques, tactics and procedures
- Identify and emulate attack path(s)

Provides realistic assessment of incident response systems
Threat Model  
(environment, system, application, etc.)

1. Vulnerability Assessment

2. Penetration Test

3. 

4. Red Team *

* Depending on the results of previous assessments
Red Team Phases

Attacker Modeled Pentest

- Open Source Intelligence (OSINT)

*Obligatory hacker image*
OSINT (Recon)

“...data collected from publicly available sources to be used in an intelligence context.”
ATT XL MENS SHIRTS **EXCELLENT CONDITION** CASUAL DRESS WORK SHIRTS

Item condition: Pre-owned

Miller Lite AT&T Patron Big O Tires Lanyard Badge Holders

Item condition: New

Brand/Logo: - Select -
Quantity: 1 / 5 available / 4 sold

Price: US $2.75

Buy It Now
Add to cart

3 watching
Add to watch list
Add to collection

New condition
100% positive feedback

Shipping: $1.25 Economy Shipping | See details
<table>
<thead>
<tr>
<th>Location</th>
<th>Address Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlanta, GA</td>
<td>11605 Haynes Bridge Road</td>
</tr>
<tr>
<td></td>
<td>400 Northwinds, Suite 550</td>
</tr>
<tr>
<td></td>
<td>Alpharetta</td>
</tr>
<tr>
<td></td>
<td>GA 30009</td>
</tr>
<tr>
<td></td>
<td>T: +1 (770) 518 2451</td>
</tr>
<tr>
<td>Austin, TX</td>
<td>115 Wild Basin Road</td>
</tr>
<tr>
<td></td>
<td>Suite 110</td>
</tr>
<tr>
<td></td>
<td>Austin</td>
</tr>
<tr>
<td></td>
<td>TX 78746</td>
</tr>
<tr>
<td>Boston, MA</td>
<td>VSR</td>
</tr>
<tr>
<td></td>
<td>76 Summer Street, 4th Floor</td>
</tr>
<tr>
<td></td>
<td>Boston</td>
</tr>
<tr>
<td></td>
<td>MA 02110</td>
</tr>
<tr>
<td></td>
<td>T: 617.933.8919</td>
</tr>
<tr>
<td>Campbell, CA</td>
<td>Payment Software Company Inc.</td>
</tr>
<tr>
<td></td>
<td>591 W. Hamilton Ave.</td>
</tr>
<tr>
<td></td>
<td>Suite 200</td>
</tr>
<tr>
<td></td>
<td>Campbell</td>
</tr>
<tr>
<td></td>
<td>CA 95008</td>
</tr>
<tr>
<td></td>
<td>+1.408.228.0961</td>
</tr>
<tr>
<td>Chicago, IL</td>
<td>11 E Adams St</td>
</tr>
<tr>
<td></td>
<td>Suite 400</td>
</tr>
<tr>
<td></td>
<td>Chicago</td>
</tr>
<tr>
<td></td>
<td>IL 60603</td>
</tr>
<tr>
<td>New York, NY</td>
<td>48 W 25th Street</td>
</tr>
<tr>
<td></td>
<td>4th Floor</td>
</tr>
<tr>
<td></td>
<td>New York</td>
</tr>
<tr>
<td></td>
<td>NY 10010</td>
</tr>
<tr>
<td>San Francisco, CA</td>
<td>123 Mission Street</td>
</tr>
<tr>
<td></td>
<td>Suite 900</td>
</tr>
<tr>
<td></td>
<td>San Francisco</td>
</tr>
<tr>
<td></td>
<td>CA 94105</td>
</tr>
<tr>
<td>Seattle, WA</td>
<td>720 3rd Avenue</td>
</tr>
<tr>
<td></td>
<td>Suite 2101</td>
</tr>
<tr>
<td></td>
<td>Seattle</td>
</tr>
<tr>
<td></td>
<td>WA 98104</td>
</tr>
</tbody>
</table>
Red Team Phases

Attacker Modeled Pentest

- Open Source Intelligence (OSINT)
- Social Engineering, i.e. phishing

* Obligatory hacker image
Social Engineering

The clever manipulation of the natural human tendency to trust.

One of the better (if not the best) social engineering attacks
Hi, I'd like to apply for a-

you're under arrest.

...ok, I should've seen that coming.
Why phishing?

100% of the time, phishing works everytime

- Gain an idea of risk
- Improve user awareness
- Test internal processes
No-Reply-********@corp-benefits.org>

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this mess:

Sent: Wed 7/26/2017 8:51 PM
To: 

[Redacted]

Your organization [Redacted] has enrolled you within our benefits program. To complete this enrollment please use the link below, and please login with your normal [Redacted] credentials.

https://my.corp-benefits.org/index.html?logon=a7125f38-8cac-43e7-b96c-68155b9a003f

Once completed, you should receive a confirmation email within the next 48 hours with further details.

Kind Regards,

Benefits Enrollment Team

Corporate Benefits, Inc
Username
username

Password
password

Login

Thank you for your enrollment.

You should receive a confirmation email within 48 hours.
Red Team Phases

Attacker Modeled Pentest

- Open Source Intelligence (OSINT)
- Social Engineering, i.e. phishing
- Physical Penetration Test (optional)

* Obligatory hacker image
Physical Security

Who’s watching the watchers?
Getting In

The trick is to look the part, act like you belong – confidence gets you everywhere
Bypassing right to exit heat sensors from the wrong side
Red Team Phases

Attacker Modeled Pentest

- Open Source Intelligence (OSINT)
- Social Engineering, i.e. phishing
- Physical Penetration Test (optional)
- Network Penetration Test (NPT)

* Obligatory hacker image
I googled “Hacker Ninja” and this is what I got :/
Interesting deprecated service...
Define a job and profit!
Red Team Roadmap

OSINT / Recon

Social Engineering / Physical Intrusion

Use Privileges

Escalate Privileges

Profit

```
root@kali:-/Desktop/CrackMapExec-2.3# python crackmapexec.py 192.168.100.100 -u pc -p P@ssw0rd1 -d insecure.com --ntds drsuapi
10-09-2016 16:17:25 SMB 192.168.100.100:445 D1C1 [*] Windows 6.3 Build 9600 (name:DC1) (domain:insecure.com)
10-09-2016 16:17:25 SMB 192.168.100.100:445 D1C1 [*] Login successfully insecure.com:p@ssw0rd1
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] Administrator:500:aab3b435b51404eead3b435b51404ee:eee19cf75e54e06b6a5907af13cef421::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] Guest:501:aab3b435b51404eead3b435b51404ee:333c7e0d016a93e7a5c9c50f0cb89f4b::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] krbtgt:aab3b435b51404eead3b435b51404ee:a83a285d86f94ae117b5d46c7df03ad9::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] insecure.com:pc1:1104:aab3b435b51404eead3b435b51404ee:e97e4786d974abc09b05a9c9be0b16e6846b::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] insecure.com:victimone:1106:aab3b435b51404eead3b435b51404ee:e19cfc75e54e06b6a5907af13cef421::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] insecure.com:victimtwo:1107:aab3b435b51404eead3b435b51404ee:e19cfc75e54e06b6a5907af13cef421::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] insecure.com:victimthree:1108:aab3b435b51404eead3b435b51404ee:e19cfc75e54e06b6a5907af13cef421::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] insecure.com:victimfour:1109:aab3b435b51404eead3b435b51404ee:e19cfc75e54e06b6a5907af13cef421::
10-09-2016 16:17:26 SMB 192.168.100.100:445 D1C1 [*] VICTIM1:1105:aab3b435b51404eead3b435b51404ee:e19cfc75e54e06b6a5907af13cef421::
```

Threat Model (environment, system, application, etc.)

Vulnerability Assessment

Penetration Test

Red Team *

* Depending on the results of previous assessments

Repeat Annually
Conclusion

Drink the koolaid...
but only once the security program is mature enough to handle it.

Benefits Round 2 – The Final Round:

- Understand the impact of a security breach
- Identify weaknesses in development and testing processes
- Test incident response capabilities
- Demonstrate security controls – justify security spending
Questions?

@bones_codes | cara.marie@nccgroup.com