Seeing Red: Improving blue teams through red teaming

Dave Hull

2016-04-01
<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>.net.listdir.txt:1017</td>
<td>pool.xml</td>
<td>pid: 1224</td>
</tr>
<tr>
<td>.net.listdir.txt:1018</td>
<td>Command line: C:\Windows\system32\spoolsv.exe</td>
<td></td>
</tr>
<tr>
<td>.net.listdir.txt:1019</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1020</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1021</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1022</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1023</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1024</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1025</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1026</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1027</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1028</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1029</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1030</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1031</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1032</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1033</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1034</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1035</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1036</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1037</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1038</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1039</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1040</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1041</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1042</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1043</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1044</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1045</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1046</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1047</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1048</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1049</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1050</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1051</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1052</td>
<td>Size</td>
<td>Path</td>
</tr>
<tr>
<td>.net.listdir.txt:1053</td>
<td>Size</td>
<td>Path</td>
</tr>
</tbody>
</table>
Intro

Nimda
From Wikipedia, the free encyclopedia

Zotob
From Wikipedia, the free encyclopedia

Blaster (computer worm)
From Wikipedia, the free encyclopedia

Sasser (computer worm)
From Wikipedia, the free encyclopedia

Sasser is a computer worm that affects computers running vulnerable versions without user intervention, but it is also easily stopped by a properly configured seventeen days earlier.
Next Generation DHCP Deployments

Dave Hull and George F. Willard III

As device mobility has transformed a novelty into a user expectation, the need for managed dynamic network configuration in campus and wireless environments has grown exponentially. User mobility and ease of end-user device network configuration have become key requirements when designing multi-user accessible networks. Additional challenges in this environment include maintaining security access controls, usage tracking, billing, and end-user support.

To support these requirements, the Dynamic Host Configuration Protocol (DHCP) provides the foundation of network auto-configuration, but it must also extend

user system for which you do not have administrative control can quickly generate a large number of end-user support issues.

Operating System Fingerprinting

Increasingly, security and network administrators are relying on device registration systems for access control as well as intrusion detection and prevention systems to maintain network integrity. Additionally, administrators are actively scanning hosts looking for vulnerable systems so they can proactively instruct the owners of those systems to apply the appropriate patches.

Remote OS fingerprinting is
Operating system fingerprinting
US 8458308 B1

ABSTRACT
Determining operating system data is disclosed, including receiving a message associated with a network protocol, extracting a set of one or more features from the message, and determining operating system data at least in part by matching one or more features of the message with one or more features of a fingerprint associated with an operating system. An exact match of the features is not required to determine operating system data.
SANS Computer Forensic Instructors are real-world practitioners who specialize in the subjects they teach. All instructors undergo rigorous training and testing before earning SANS Certified Instructor status. This helps us guarantee that what you learn in class will be up-to-date and relevant to your job.
11 Jan 2012

Metadata distributions in Computer Forensics

0 comments Posted by Dave Hull
Filed under artifact analysis, Computer Forensics, Evidence Analysis

After my previous post, on using uid and gid distributions to spot malicious code on *nix file systems, I took to working on some code to convert *nix "modes" (The Sleuth Kit bodyfile refers to file type and permission information as mode) from its bodyfiles to their octal representations and then to calculate averages and ... Continue reading Metadata distributions in Computer Forensics

24 Dec 2011

Digital Forensics: UID and GID distributions

0 comments Posted by Dave Hull
Intro

Dave Hull
davehull

Various and sundry
I am from enternetz
http://trustedsignal.blogspot.com/
Joined on May 2, 2011

77 Followers 16 Starred 39 Following

Popular repositories

- **Kansa**
  A Powershell incident response framework
  214 stars

- **Mal-Seine**
  Why hunt when you can seine?
  14 stars

- **autorunalyzer**
  A Python script for performing analysis of the output from Microsoft's Sysinternals Autoruns.
  12 stars

- **VirusTotalShell**
  A fork of David B Heise's VirusTotal Powershell Module
  10 stars

- **Get-StakRank**
  A Powershell script for frequency analysis of separated values data files.
  9 stars

68 contributions in the last year

Summary of pull requests, issues opened, and commits. Learn how we count contributions.
Intro

Office 365
Kansa

A modular incident response framework in Powershell. It's been tested in PSv2 / .NET 2 and later and works mostly without issue.

But really, upgrade to PSv3 or later. Be happy.

More info:
http://trustedsignal.blogspot.com/search/label/Kansa
Tanium for Endpoint Security
Detect and RemEDIATE Threats and Issues in Seconds

"Tanium has enhanced our approach to endpoint security, enabling our security team to execute actions and queries efficiently over hundreds of thousands of endpoints firmwide. Tanium’s unique architecture and platform approach provide us with the speed, scale and flexibility we require, with the opportunity to expand our use cases and further enhance its value to us over time."

Rohan Amin, Global Chief Information Security Officer of JPMorgan Chase
Agenda

• Teaser
• Speaker intro
• Why red teaming
• What is red teaming
• Highlights and lessons learned
• Who should be red teaming
• When
• Practicalities of red teaming
• Conclusion
Why red team?

Because it delivers a security incident.
Pen testing delivers… a nice report.
Pen testing delivers… a nice report.
Why red team?

Because you will play like you practice.
Why red team?
“We run that play every day — end of every practice,” [Phil] Booth said.

http://www.nytimes.com/2016/04/06/sports/ncaabasketball/villanova-national-championship.html?_r=0
Why red team?

Because you will play like you practice especially under stress.
Agenda

• Teaser
• Speaker intro
• Why red teaming
• What is red teaming
• Highlights and lessons learned
• Who should be red teaming
• When
• Practicalities of red teaming
• Conclusion
What is red teaming?

It is not threat modeling.
What is red teaming?

It is not vulnerability assessment.
What is red teaming?

It is not penetration testing.
What is red teaming?

Red teaming is different.
Pen testing delivers… a nice report.
Red teams:

Have mission objectives.
Red teams:

Have mission objectives.
Enterprise or domain admin.
Red teams:

Have mission objectives.
Customer pivot.
Red teams:

Have mission objectives.
IP theft.
Red teams:

Have mission objectives.
Burn it all down.
Red teams:

- Have mission objectives.
- Test incident response capabilities and procedures.
Agenda

• Teaser
• Speaker intro
• Why red teaming
• What is red teaming
• Highlights and lessons learned
• Who should be red teaming
• When
• Practicalities of red teaming
• Conclusion
Lesson learned

Outliers *may* be leads.
Lesson learned

Automate what you can.
Remediation?
Lesson learned

Lather. Rinse. Repeat.
Lesson learned

Investigate. Remediate. Repeat.
Agenda

• Teaser
• Speaker intro
• Why red teaming
• What is red teaming
• Highlights and lessons learned
• Who should be red teaming
• When
• Practicalities of red teaming
• Conclusion
Who should be red teaming?

Any organization that may have a security incident.
Who should be red teaming?

Any organization with something worth protecting.
Who should be red teaming, practically speaking?

Organizations meeting the previous criteria and having:

- Some monitoring.
- Some defenses.
- Some IR capabilities.
Who should be red teaming?

Probably an internal team, but not just the security team.
Lesson learned

Documentation is wrong.
Code comments are wrong.
Assumptions are wrong.
Agenda

• Teaser
• Speaker intro
• Why red teaming
• What is red teaming
• Highlights and lessons learned
• Who should be red teaming
• When
• Practicalities of red teaming
• Conclusion
When should you red team?

As often as you can.
Lesson learned

Avoid concurrent red team incidents.
Agenda

• Teaser
• Speaker intro
• Why red teaming
• What is red teaming
• Highlights and lessons learned
• Who should be red teaming
• When
• Practicalities of red teaming
• Conclusion
Practicalities

Have Rules of Engagement.
Practicalities

Get approval from management and legal.
Practicalities

No accessing or tampering with customer data.
Practicalities

No accessing or tampering with real customer data.
Practicalities

No outages.
Give the red team access.
Practicalities

Give the red team source code.
Practicalities

Give the red team architecture diagrams.
Practicalities

Keep the blue team in the dark.
Practicalities

Real incidents trump red team incidents.
Practicalities

Red incidents are core hours only.
Red incidents are core hours only, plus a little.
Practice how you want to play.
Practicalities

Cross team collaboration.
Practicalities

Establish a situation room.
Designate incident and investigative leads.
Delegate and PM.
Practicalities

Investigate.
Practicalities

Document.
Practicalities

Report.
Report writing. Not as fun as CLI forensic analysis, but it must be done. Analyze for show, report for dough.
Practicalities

Plan for remediation.
Practicalities

Execute remediation.
Practicalities

Post remediation monitoring.
Practicalities

Postmortems.
Practicalities

Stakeholders, blue team, red team.
Practicalities

No blame games.
Practicalities

But hold yourself accountable.
Practicalities

Blue team goes first.
Practicalities

All cards on the table.
Red team goes second.
Practicalities

All teams get bugs, feature requests.
Agenda

- Teaser
- Speaker intro
- Why red teaming
- What is red teaming
- Highlights and lessons learned
- Who should be red teaming
- When
- Practicalities of red teaming
- Conclusion
Lesson learned

No one runs as admin.
Lesson learned

Just-In-Time admin (JIT).
Lesson learned

Segment the network.
Lesson learned

Segment the accounts.
Lesson learned

Dedicated admin workstations.
Lesson learned

Zero human generated passwords.
Lesson learned

2FA everywhere.
Lesson learned

Don’t trust. Verify.
Agenda

- Teaser
- Speaker intro
- Why red teaming
- What is red teaming
- Highlights and lessons learned
- Who should be red teaming
- When
- Practicalities of red teaming
- Conclusion
Red teaming is hard.
Conclusion

Real incidents may be harder.
Practice how you want to play.
Thank you!
dave.hull@tanium.com