OWASP Atlanta Chapter Meeting

Filter Evasion Techniques
04.25.09

OWASP

APR 2009

The OWASP Foundation

http://www.owasp.org

Roadmap

- Announcements & Acknowledgements (Tony UV)
- Filter Evasion Presentation (Rob Ragan)
- Hands On Workshop
- Meeting Wrap Up (Tony UV)
  - Upcoming events…

Announcements & Acknowledgements

- OWASP Atlanta Case Study Team
- International/ National Chapter News
- OWASP Projects
- OWASP Atlanta Logo Request
- Meeting Locations
- OWASP Membership
- Sponsor Acknowledgements

OWASP Workshop

FILTER EVASION

Filter Evasion

- Why?
  - Cybercriminals are using evasion techniques
  - Targets are relying on IPS/WAF/Firewalls
  - Filter shortcomings need to be identified
- What?
  - Value comes from building evasion techniques into the testing process
  - Developers & QA need to test the strength of their sanitizers and validators.

Filters are a road block

Filters are a road block

Unfortunately sometimes they're poorly designed

Whisker's anti-IDS tactics · 1999

- Method matching
  - GET → HEAD
- Url encoding
  - HEX %xx notation
- Double slashes
  - '/' → '//'
- Reverse traversal
  - /dir/blahblah/../
- Self-reference directories
  - /dir/././././ == /dir/
- Premature request ending
  - Stop at the first HTTP/1.?\r\n
- Parameter hiding
  - %3f → ?
- HTTP mis-formatting
  - %20 → %09 (TAB)
- Long Urls
  - GET /<random>/../dir/a.cgi
- DOS/Win directory syntax
  - '/' → '\'
- NULL method processing
  - GET\0
- Case sensitivity
  - 'abc' → 'ABC'

Details @ http://www.wiretrip.net/rfp/txt/whiskerids.html

Whisker's Session Splicing

- Network level attack
- Not the same as IP fragmentation
- Send parts of the request in different packets
  - "GET / HTTP/1.0" may be split across multiple packets to be
  - "GE", "T ", "/", " H", "T", "TP", "/1", ".0"

IP Fragmentation vs Session Splicing

- IP Fragmentations
  - Packet is too large for the link layer a router can split it into multiple fragments
- Session Splicing
  - Purposefully delivering the payload over multiple packets to evade detection. Smaller than it needs to be.
- Defense
  - Fragment reassembly
  - Session reassembly
  - Send a reset [RST]

Session Splicing 1999 vs 2009

- The current implementation in whisker will result in 1-3 characters in each packet, **depending on your system and network speed**

1999

2009

Evade Passive Filters

- Pragmatic Session Splicing + Timing Attack
  - Use the filter's signatures to split the payload
  - Vulnerable if the IDS stateful inspection timeout is less than session reassembly of the hosts it protects
  - Similar to fragmentation attack but instead of at the IP level we move up to the TCP level

Time Splicer

- The attack is practical if we split the session on the matches found by the signature we're trying to evade

Attack:

```
GET /index.php?param=<script>alert(123)</script>  HTTP/1.1
Host:www.target.com
```

- Signature: Matches on <script>|</script> tags
- Know the stateful inspection timeout for the IDS
- Recursively find matches and split the attack string, then send each splice in a new packet with time delay between each packet

Snort Preprocessors

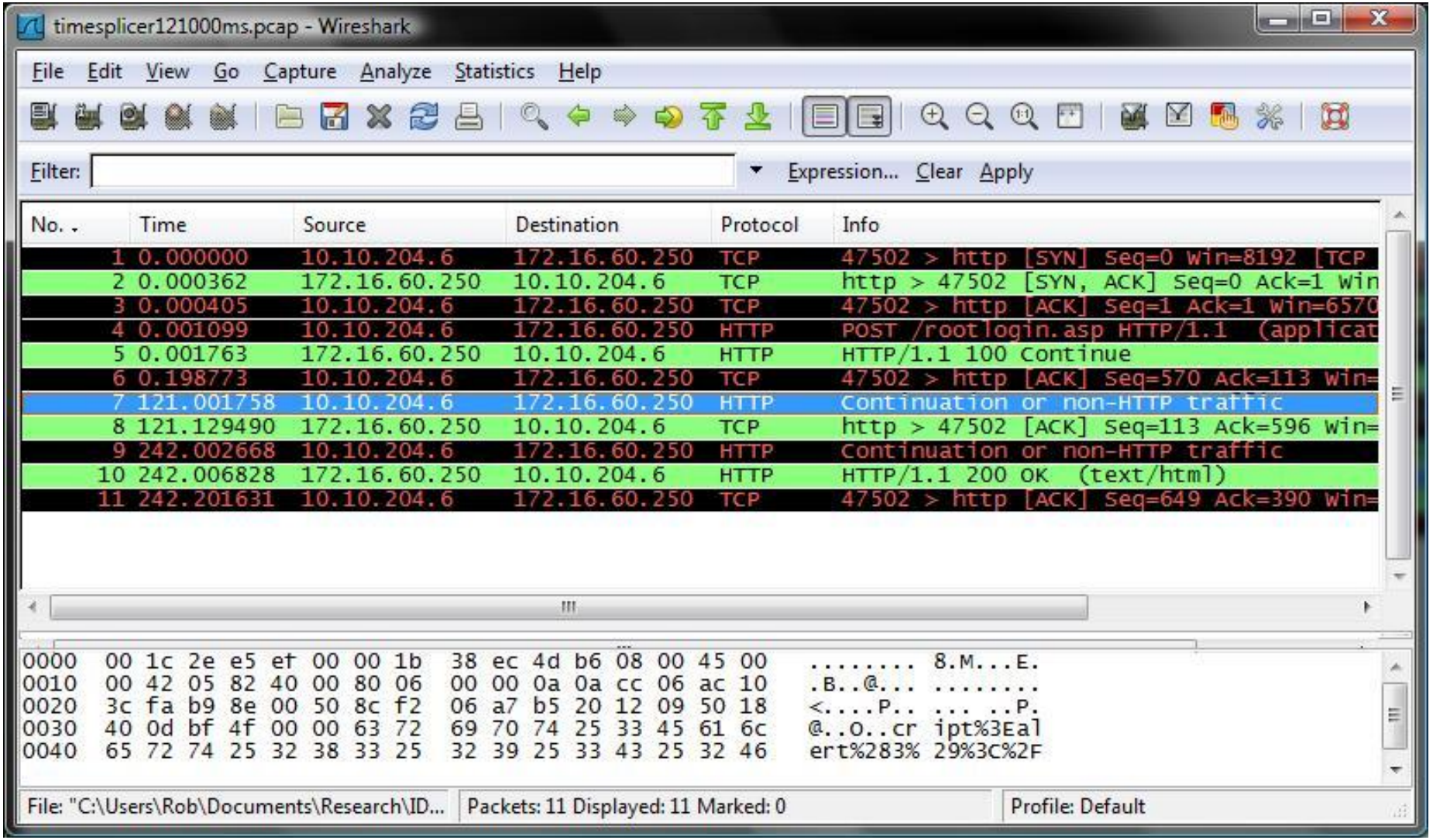
- HTTP Inspect + Stream4
- Stateful inspection
- Default timeout is 30 seconds

```
#  stream4: stateful inspection/stream reassembly for Snort
#--------------------------------------------------- #
   Use in concert with the -z [all|est] command line switch to
   defeat stick/snot against TCP rules. Also performs full TCP
   stream reassembly, stateful inspection of TCP streams, etc. Can
   statefully detect various portscan types, fingerprinting, ECN,
   etc.
# stateful inspection directive
# no arguments loads the defaults (timeout 30, memcap 8388608)
```

```
POST /rootlogin.asp HTTP/1.1
Host: zero.spidynamics.com
Keep-Alive: 300
Content-Type: application/x-www-form-urlencoded
Content-Length: 102

txtPassPhrase=&txtName=%3Cs
…WAIT 30s…
cript%3Ealert%283%29%3C%2F
…WAIT 30s…
script%3E&txtHidden=This+was+hidden+from+the+user
```


0wn3d!!!1

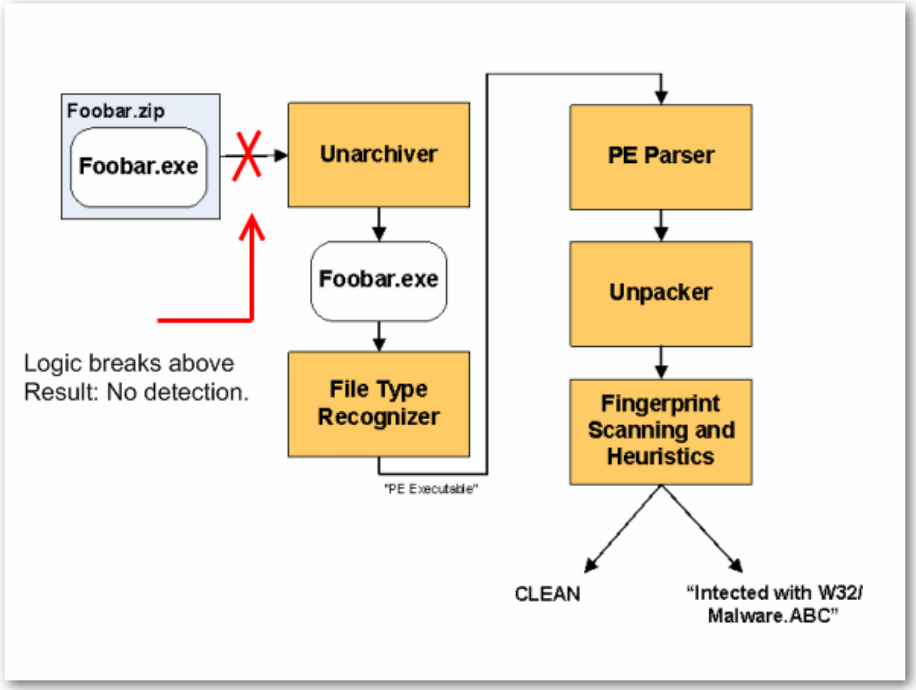

timesplicer121000ms.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.10.204.6 172.16.60.250 TCP 47502 > http [SYN] Seq=0 Win=8192 [TCP
2 0.000362 172.16.60.250 10.10.204.6 TCP http > 47502 [SYN, ACK] Seq=0 Ack=1 Win
3 0.000405 10.10.204.6 172.16.60.250 TCP 47502 > http [ACK] Seq=1 Ack=1 Win=6570
4 0.001099 10.10.204.6 172.16.60.250 HTTP POST /rootlogin.asp HTTP/1.1 (applicat
5 0.001763 172.16.60.250 10.10.204.6 HTTP HTTP/1.1 100 Continue
6 0.198773 10.10.204.6 172.16.60.250 TCP 47502 > http [ACK] Seq=570 Ack=113 Win=
7 121.001758 10.10.204.6 172.16.60.250 HTTP Continuation or non-HTTP traffic
8 121.129490 172.16.60.250 10.10.204.6 TCP http > 47502 [ACK] Seq=113 Ack=596 Win=
9 242.002668 10.10.204.6 172.16.60.250 HTTP Continuation or non-HTTP traffic
10 242.006828 172.16.60.250 10.10.204.6 HTTP HTTP/1.1 200 OK (text/html)
11 242.201631 10.10.204.6 172.16.60.250 TCP 47502 > http [ACK] Seq=649 Ack=390 Win=
0000 00 1c 2e e5 ef 00 00 1b 38 ec 4d b6 08 00 45 00 ..... 8.M...E.
0010 00 42 05 82 40 00 80 06 00 00 0a 0a cc 06 ac 10 .B..@... .....
0020 3c fa b9 8e 00 50 8c f2 06 a7 b5 20 12 09 50 18 <....P.. ... ..P.
0030 40 0d bf 4f 00 00 63 72 69 70 74 25 33 45 61 6c @..O..cr ipt%3Eal
0040 65 72 74 25 32 38 33 25 32 39 25 33 43 25 32 46 ert%283% 29%3C%2F
File: "C:\Users\Rob\Documents\Research\ID... Packets: 11 Displayed: 11 Marked: 0 Profile: Default

Timing Attacks Are Fun

- What else can we do?
  - Fingerprint the Server and Application technology based on timeout
  - Fingerprint an IPS

Generic Archive Evasion

- Bypass scanning engines with archive files
  - Password protect
  - Modify file format
- Effects AV gateway products
  - E-mail
  - WWW
- Get malware to the target
  - Use a custom unpacker to execute



Recent advisories by Thierry Zoller @ http://zoller.lu

Range Header Evasion

- Only examining magic numbers is weak
- FindMimeFromData Function in IE
  - Determines MIMIE type from first 256 bytes
  - Avoid fake content-types used as XSS images
  - Use Range to request only a portion of a file containing an attack

```
Range: bytes=257-2048
```

- Flash used to allow the Range and Range-Request header
- XMLHttpRequest still does!

Reference: http://events.ccc.de/congress/2007/Fahrplan/attachments/1054_unusual_web_bugs.pdf

Questions about filters or evasions?

Hands-on Time

LET. US. HACK.

Meeting Wrap-Up

- Up Coming Meetings/ Workshops
- OWASP Atlanta Board
- Social Events
- Drinks @ Vortex
  - 878 Peachtree St NE # 4, Atlanta, GA
  - (404) 875-1667