EVADING DEEP INSPECTION FOR FUN AND SHELL

Who we are

- Olli-Pekka Niemi
  - Chief Research Officer, Stonesoft
- Antti Levomäki
  - Senior Vulnerability Analyst, Stonesoft

Agenda

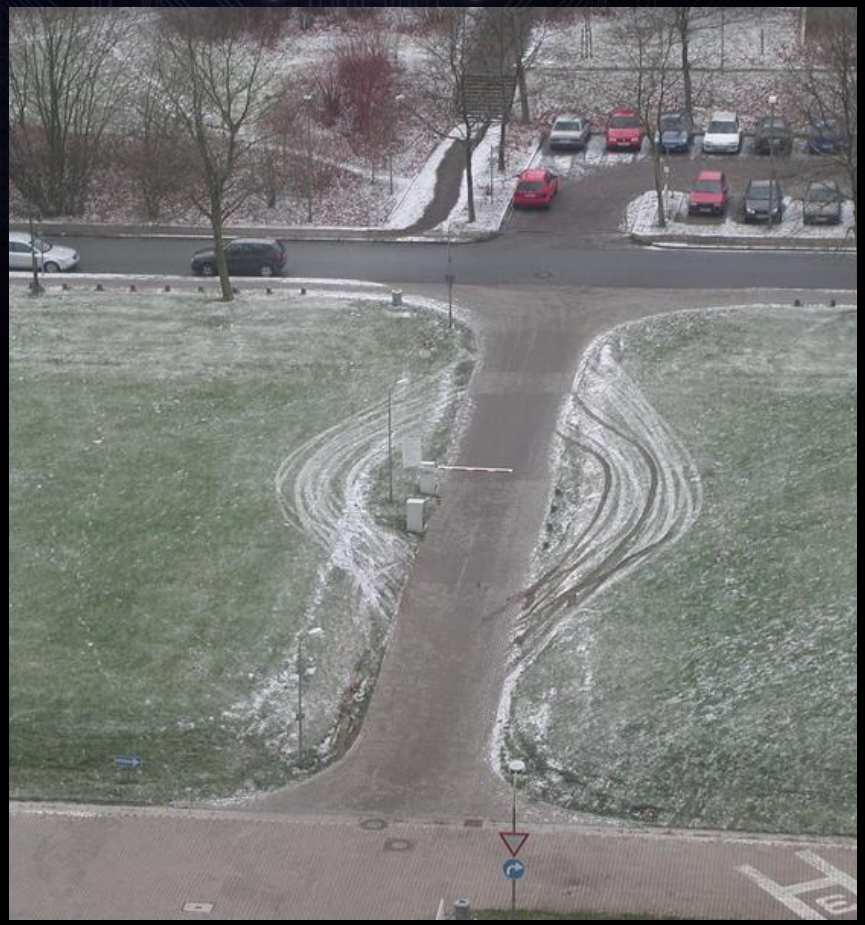
- Introduction to evasions
- Previous research
- Evasions explained
- Evasion testing methodology
- Results

IPS, NGFW, what?

- Network intrusion prevention systems (IPS)
  - middleboxes used to protect hosts and services
  - analyze network traffic and attempt to alert and terminate connections that are deemed harmful.
- Next Generation Firewalls (NGFW)
  - Firewalls with built in IPS functionalities
- We treat NGFW as IPS in this presentation

- Intrusion Prevention Systems should protect vulnerable hosts from remote exploits
- Exploits can apply multiple evasion methods to bypass the detection capabilities of the IPS and break into the remote protected host

What?



Should vs Must

- Successful traffic analysis requires that the IPS device interprets traffic in the same way as the host it is protecting
  - TCP/IP protocols and application protocols on top of TCP/IP are rich in features.
  - there is a large gap between how protocols should be used and how they can be used

Why

- The reason that evasions work is the old robustness principle stated by Jon Postel in RFC793

> "be conservative in what you do, be liberal in what you accept from others".

- We call deliberately sending traffic in a way that is difficult to analyze by a middlebox an evasion technique

- Aren’t evasions just some protocol anomalies or malicious packets…
- …that can be dropped by the IPS?

- No. Some evasions can be classified as an attack, but most evasions are simply alternative ways of encoding data.

- Evasion is evasion only when applied with attack. Blocking connections based on a potential evasion without normalizing cause false positives

- Most of IPS devices are throughput oriented by design. Evasions work because
  - the IPS devices are lacking proper understanding and analysis of the protocol.
  - TCP/IP reassembly implementation shortcuts to favor packet throughput
  - design flaws or missing features

- Have evasions been researched before?
  - Yes. A lot.

Academic Research

- Ptacek, Newsham: “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”, 1998.
- Raffael Marty, Thor – A tool to test intrusion detection systems by variation of attacks, 2002
- A. Samuel Gorton and Terrence G. Champion, Combining Evasion Techniques to Avoid Network Intrusion Detection Systems, 2004
- Giovanni Vigna William Robertson Davide Balzarotti : Testing Network-based Intrusion Detection Signatures Using Mutant Exploits, 2004
- Shai Rubin, Somesh Jha, and Barton P. Miller: Automatic Generation and Analysis of NIDS Attacks, 2004
- Varghese, et al., Detecting Evasion Attacks at High Speeds without Reassembly, Sigcomm, 2006.

Hacker Research

- Horizon, Defeating Sniffers and Intrusion Detection Systems, Phrack Magazine Issue 54, 1998, article 10 of 12.
- Rain Forest Puppy: A look at whisker's anti-IDS tactics, 1999
- NIDS Evasion Method named "SeolMa", Phrack 57, Phile 0x03, 2001
- Daniel J. Roelker , HTTP IDS Evasions Revisited, 2003
- Brian Caswell, H D Moore, Thermoptic Camouflage:Total IDS Evasion, BlackHat, 2006
- Renaud Bidou: IPS Shortcomings, BlackHat 2006

Tools

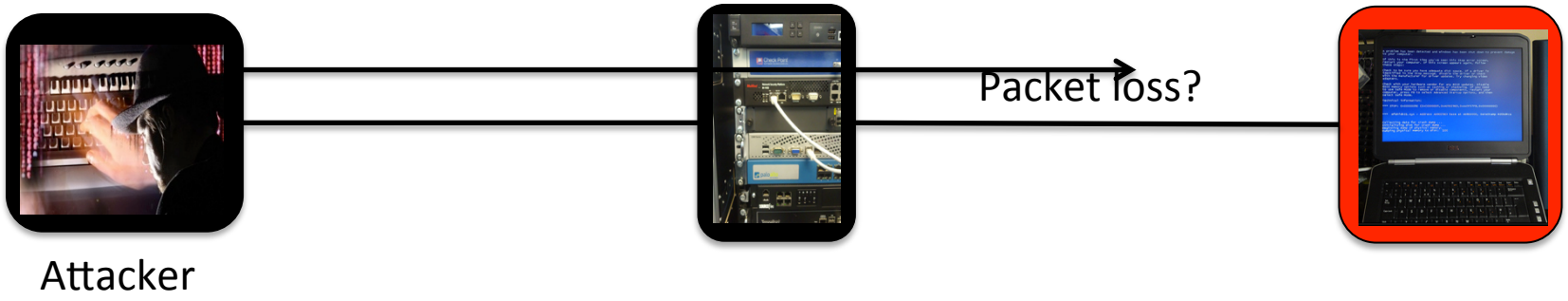
- Fragroute(r) by Dug Song ~1999
- Robert Graham: SideStep, 2000
- Rain Forest Puppy: Whisker, libwhisker
- Raffael Marty: Thor, 2002
- Metasploit Framework
- Immunity Canvas
- Core Impact
- Breaking Point
- Libnet
- Scapy
- Tcpreplay
- Karalon

- So Why do evasions still work?

- Evasion detection and normalization is difficult
- Reduce throughput
- Anomaly based evasion prevention false positives
- Throughput-wise effective packet based pattern matching miss attacks deploying evasions
- Proper TCP/IP reassembly requires a lot of memory

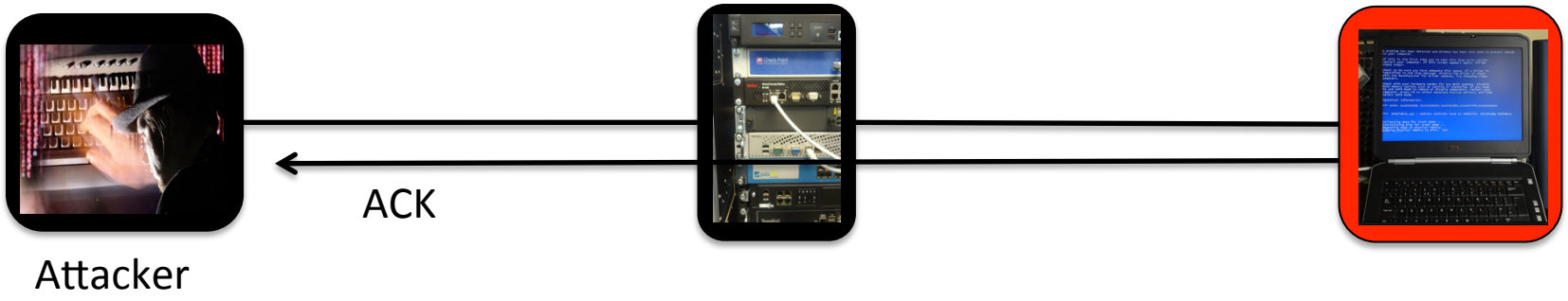
The Problem of Stream Reassembly

- IPS does not know whether a packet seen reaches the destination
  - Packet loss may have occurred
  - Packet will be discarded by the destination



The Problem of Stream Reassembly

- The IPS knows that a packet reached the destination when it receives acknowledgement from the destination



The Problem of Stream Reassembly

- The attacker may craft a packet that will be dropped by the destination, while the IPS is fooled to classify this as normal (packet loss)
- The attacker will then send the malicious packet that the IPS will pass along as a retransmission
  - There are multiple ways of doing this:
    - TTL/IP options/TCP options/checksums

Attacker

Attack Strategy

- At the point of triggering the vulnerability, craft a packet that is not malicious looking and will not exploit the target
- The packet will be dropped by the target
- IPS does not know that
- Send the packet that will compromise the target.
- IPS treat this packet as a resend due to packet loss and passes the packet
- Enjoy shell (IPS does not log anything)

Proper Mitigation

- IPS must keep every unacked packet in memory to avoid being evaded
  - It seems that most do not, or at least the implementation is faulty

EVASIONS EXPLAINED

TCP Segmentation and Reordering

- Payload can be split into segments of arbitrary size
- Segments can be sent in any order
- Too many small TCP segments might lead into anomaly based connection termination. Apply segmentation only when actually triggering the vulnerability and/or to the shellcode
  - Most boxes are still vulnerable to this

PAWS

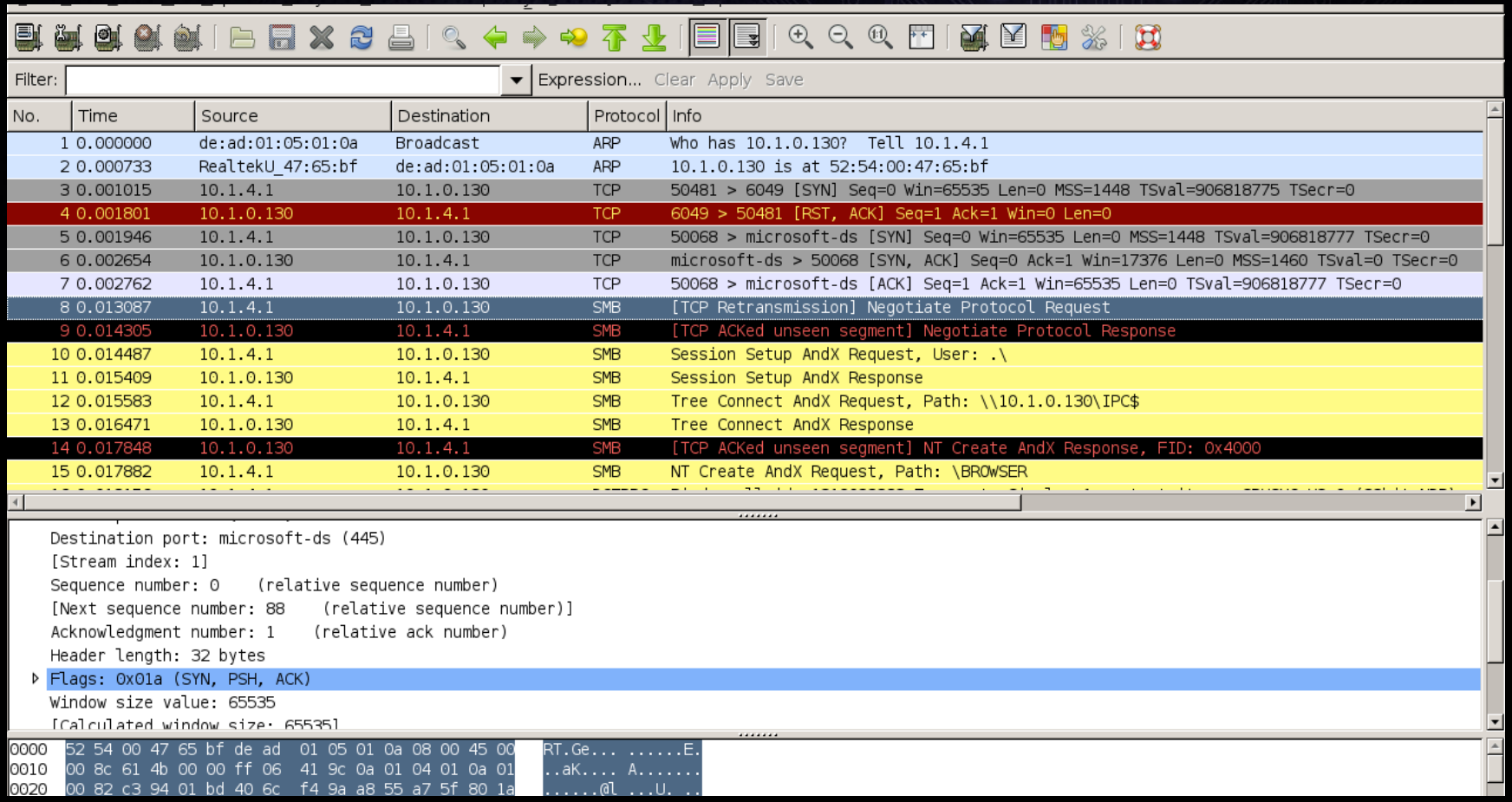
- The PAWS (Protection Against Wrapped Sequence numbers) algorithm is defined in RFC1323
  - uses TCP timestamps to drop segments that contain timestamps older than the last successfully received segment.
- Its use as an evasion was described already by Ptacek and Newsham in 1998
  - Still works against most of today´s IPS devices

PAWS

- PAWS causes problems for TCP reassembly when the IPS does not know which segments the end hosts accept or discard.
- TCP segments designated for PAWS elimination can be created by duplicating a valid TCP header and moving its timestamp value backwards. The actual payload can be arbitrary, e.g., a non-malicious version of a protocol message.

SYN Retransmit

- Retransmit SYN with first segment containing payload
- Most IPS devices have problems with the unexpected combination of a retransmitted SYN flag and new payload in an established connection
  - IPS devices are fooled by the duplicated SYN and pass connection uninspected



IPv4 Options

- IPv4 packet headers can contain options. If any of the options are invalid, the whole IPv4 packet should be discarded by the receiving host. This can cause problems if the inspecting device and the end host discard different packets.

Urgent

- Urgent pointer marks TCP payload as urgent
- TCP socket handle urgent data as either inline or out-of-band.
  - Out-of-band data is not returned via normal recv() calls and gets discarded by applications that do not use urgent data. Most operating systems default to out-of-band urgent data
- The use of TCP urgent data as an evasion was documented in Phrack Magazine 2001.
- Problematic for IPS devices because the choice between handling data as inline or out-of-bound is application specific.
- Urgent pointer evasion is still efficient against many IPS

TCP Receive Window

- TCP receive window is the amount of new data that the sending side is willing to receive. An attacker can advertise a small window size to force the other end of the TCP connection into sending small segments.
- This complements sending small TCP segments by allowing the attacker to control TCP segment sizes in both directions.

black hat
USA 2013

What is Evader

- A tool to test (NG)?(I[DP]S|FW) protocol analysis and reassembly capabilities by applying evasions to attacks
- Does not simulate, does real attacks against real targets
- Simple Test Scenario: #shell does not lie
  - Send attack, if we got the shell back, evasion was successful and DUT failed

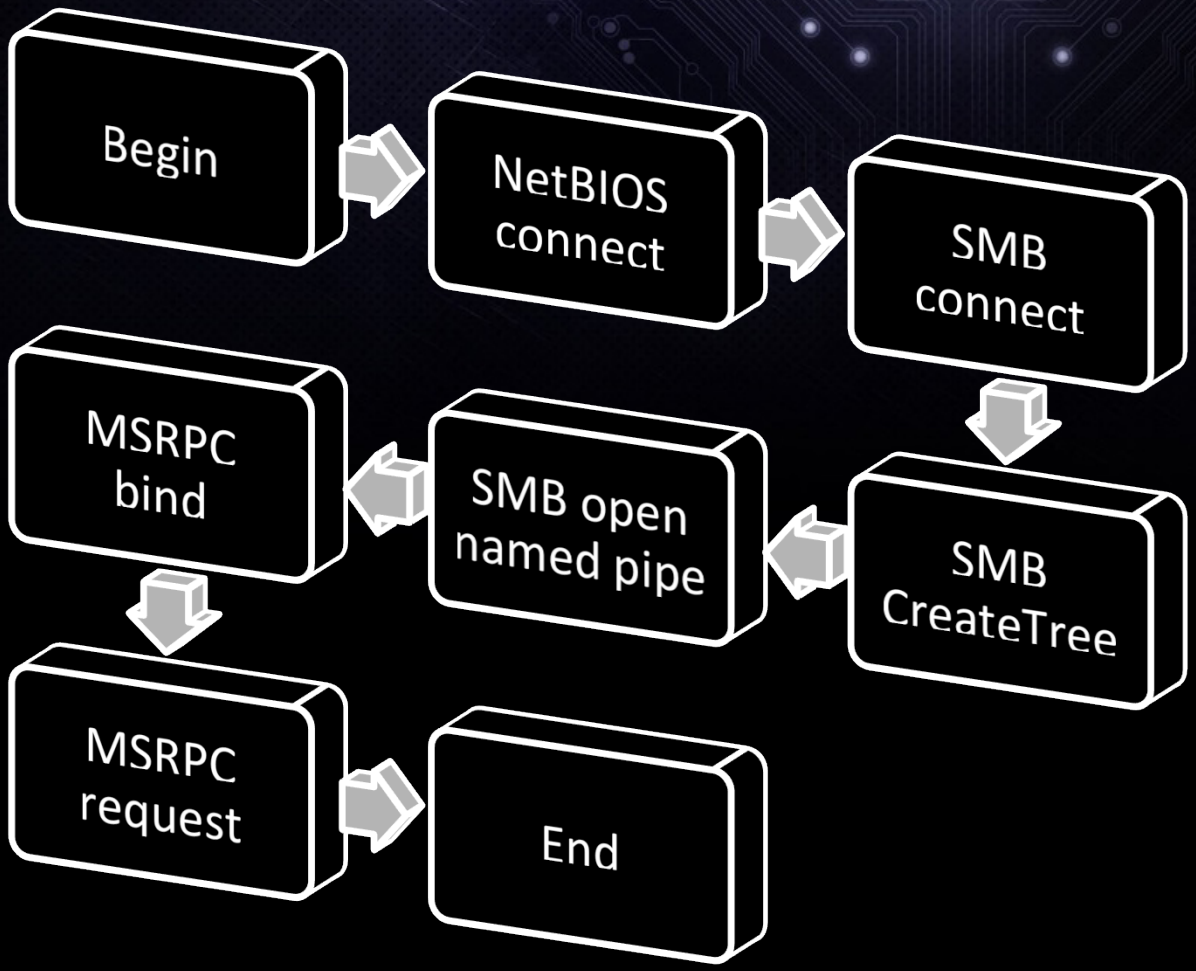
- Built on a proprietary TCP/IP stack.
- Has application clients & servers for higher layer protocols

➢ Complete control over every packet sent.

- Exploits are divided into stages
  - Each stage corresponds to a step in the application protocol
- Evasions can be targeted to all or just a range of stages

➢ Targeting to specific stages critical to IPS detection makes anomaly based blocking more difficult

MSRPC exploit stages



- All exploits containing shellcode can be run 'obfuscated'
  - Generates a different shellcode encoder and possible NOP sled for each execution.
  - Makes exploit based detection harder.
- Normal versions attempt to look like commonly found public exploits.

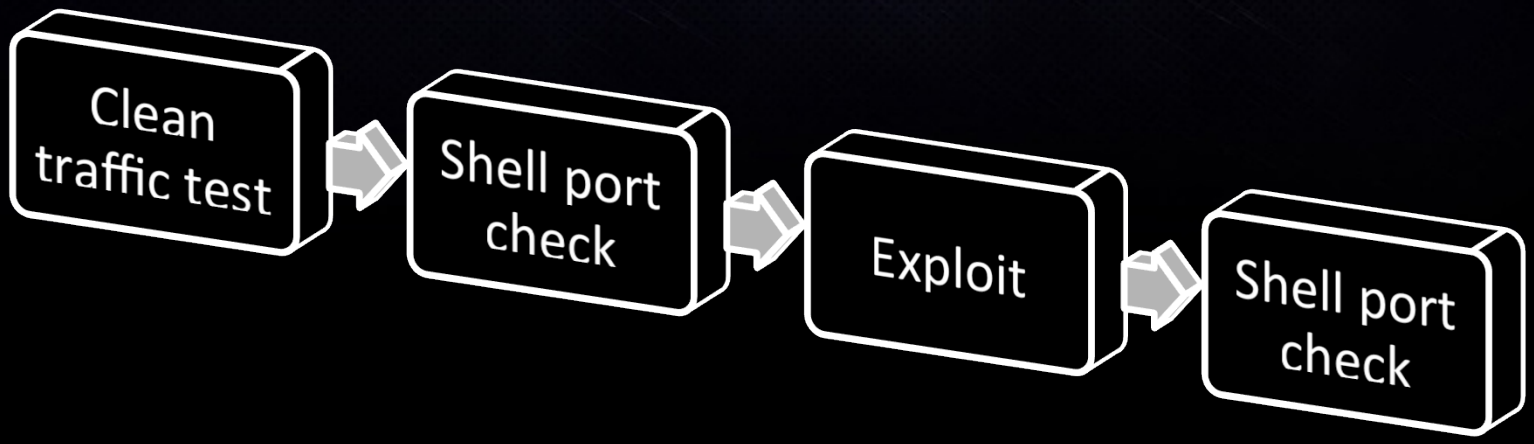
- Evader contains known exploits that every IPS should detect
- CVE-2008-4250, MSRPC Server Service Vulnerability [13].
  - A buffer overflow vulnerability in Microsoft Windows allowing arbitrary code execution. Widely exploited by the Conficker worm.
  - Evader targets a Windows XP SP2 host.
  - Protocols used: IP, TCP, NetBIOS, SMB, MSRPC.
- CVE-2004-1315, HTTP phpBB highlight
  - Input sanitation vulnerability in phpBB allowing arbitrary PHP execution. Exploited by the Santy.A worm in 2004.
  - Protocols used: IP, TCP, HTTP
- CVE-2012-0002, Windows RDP Denial of Service [14].
  - Vulnerability in the Remote Desktop Protocol implementation in Microsoft Windows.
  - Exploit in Evader crashes unpatched Windows 7 hosts.
  - Protocols used: IP, TCP, RDP

- In theory, for the selected exploit, the Evader could produce every possible data stream transmitting the payload, but in practice this cannot be tested since there are virtually endless amount of combinations and stage permutations.

- When evasions are not used, IPS/NGFW devices detect and terminate the attack
- With proper evasions applied, IPS/NGFW start to Fail
  - Does not detect anything
  - Detect something that cannot be terminated due to risk for false positive
  - Detect attack, claims to terminate but fails termination

- Evader can be automated with another tool called Mongbat
- Mongbat runs evader with different evasion combinations and collects results
  - Successful exploits are reported along with a command line for easy repeatability.
  - Takes packet captures
  - Basically Mongbat+Evader=Evader Fuzzer

Mongbat Single Run



- Mongbat randomly selects a number of evasions and their parameters for each Evader execution.
  - No special care is taken to produce only legitimate traffic
    - The victim computer is used to validate working combinations

- Here we present the results of running Mongbat against 9 vendors' commercial IPS devices. The vendors include most Gartner 2012 IPS and 2013 NGFW Magic Quadrant leaders and challengers.
- The devices have up-to-date software and updates installed. We have attempted to configure the devices for maximum detection and blocking while still allowing the Evader clean check to succeed.

- We have defined 12 evasion test cases. The tests are run with Mongbat so that only the listed evasions are used.
- If working evasion is not found in one minute the test case is marked as failed, otherwise as success.

Evasion test cases

#	Atomic Evasions
0	Baseline attack without evasions
1	Paws Elimination Evasion
2	SYN Retransmit Evasion
3	IPv4 Options
4	TCP Urgent Data
5	TCP Receive Window
6	TCP Segmentation and Reordering (TSR)

Evasion test cases

#	Evasion Combinations
7	TCP Paws + TSR
8	SYN Retransmit + TSR
9	IPv4 Options + TSR
10	Urgent Data + TSR
11	TCP Receive Window + TSR
12	All Listed Evasions

Results for MSRPC without stages

Vendor	0	1	2	3	4	5	6	7	8	9	10	11	12
Vendor1													
Vendor2			x		x		x	x		x	x	x	x
Vendor3			x								x		x
Vendor4		x		x			x	x		x	x	x	x
Vendor5		x	x	x				x		x			x
Vendor6						x	x	x		x		x	x
Vendor7		x	x	x	x	x	x	x		x	x	x	x
Vendor8		x	x		x	x	x	x		x	x	x	x
Vendor9								x			x		x

Results for MSRPC with stages

Vendor	0	1	2	3	4	5	6	7	8	9	10	11	12
Vendor1													
Vendor2			x		x		x	x	x	x	x	x	x
Vendor3			x					x	x		x		x
Vendor4		x		x			x	x	x	x	x	x	x
Vendor5		x	x	x				x	x	x			x
Vendor6						x	x	x	x	x	x	x	x
Vendor7		x	x	x	x	x	x	x	x	x	x		x
Vendor8		x	x		x	x	x	x	x	x	x	x	x
Vendor9								x	x		x		x

- All vendors are able to stop the MSRPC exploit with no evasion applied. TCP segmentation and reordering by itself seem to go through most vendors IPS devices. When this is combined with segments destined for PAWS elimination and applied to stages almost all vendors' inspection can be bypassed.

- The MSRPC exploit requires multiple SMB requests and responses before the vulnerability can be exploited. This allows IPS devices to perform protocol validation and possibly terminate evasion attempts during the session setup phase. Evasions using just a small TCP receive window probably cause some devices to lose protocol state due to a failure in parsing server responses.

Results for HTTP

Vendor	0	1	2	3	4	5	6	7	8	9	10	11	12
Vendor1													
Vendor2		x	x	x	x	x	x	x		x	x	x	x
Vendor3	x	x		x	x	x	x	x		x	x	x	x
Vendor4		x	x	x	x	x	x	x		x	x	x	x
Vendor5	x	x	x	x	x	x	x	x		x	x	x	x
Vendor6	x	x	x	x	x	x	x	x		x	x	x	x
Vendor7			x		x						x		x
Vendor8	x	x	x	x	x	x	x	x		x	x	x	x
Vendor9		x	x				x	x			x	x	x

- All vendors were not able to block the obfuscated HTTP exploit without evasions. The complete set of test cases was still run to see if the devices block some evasions as anomalies. TCP segmentation and reordering was again successful also over HTTP, especially when combined with TCP segments containing urgent data.
- In cases when no exploit succeeded Mongbat executed around 500-2000 attempts in the 60 second test period. Most successful evasion combinations were found in 1-10 attempts.

DEMO

Thank You!

- Questions & Comments
  - Olli-Pekka.Niemi@stonesoft.com
  - Antti.Levomaki@stonesoft.com
- Evader tool free download
  - http://evader.stonesoft.com