

Forum:[Hack Forums](#)

Thread: [Help with packet analysis and specifically, application data.](#)

whiter0x - November 5, 2018, 4:27 pm

Hey all,

I have my setup as follows.

Xbox -- PC -- Router

All are connected via ethernet. My xbox is connected via usb dongle, and latter via built-in ethernet port.

I recorded some data with wireshark. I would like to analyze this data somehow, but I don't know where to start.

The data is being killed 3 times in "Grand Theft Auto V"

I was hoping I could have enough data to maybe make myself die by sending a malicious/malformed packet, or something.

So my question is simple.

Is there a way to unencrypt the data, edit it, and resend it? Or is there a different approach?

Thanks!

(ALL OPINIONS WELCOME :))

VelvetCoding - November 13, 2018, 8:42 pm

This sounds very advanced. I can't imagine any answers being on here

Infamia - November 14, 2018, 7:45 am

if the data is encrypted by tls/tcp, then you would use generic decryption techniques by, say, spoofing the CA or trying a sslstrip attack (would never work, but it's just a filler answer); afterwards, the packet structure is probably quite complex, and it is probably only relevant on the server-side to which it is sent, verified and registered as an actual event.

in all reality, i would give up, unless you have a leak of the actual game protocol then there's pretty much no chance within a reasonable time frame that you could reverse the protocol.

whiter0x - November 14, 2018, 11:54 am

(Nov 14, 2018 08:45 AM)Infamia Wrote: [\[CITE\]](#) if the data is encrypted by tls/tcp, then you would use generic decryption techniques by, say, spoofing the CA or trying a sslstrip attack (would never work, but it's just a filler answer); afterwards, the packet structure is probably quite complex, and it is probably only relevant on the server-side to which it is sent, verified and registered as an actual event.

in all reality, i would give up, unless you have a leak of the actual game protocol then there's pretty much no chance within a reasonable time frame that you could reverse the protocol.

What if I tried capturing data from when I die, and re-send it using packeth (or similar)?

Would kills/deaths be protected by a token or something?

(Nov 14, 2018 08:45 AM)Infamia Wrote: [\[CITE\]](#) unless you have a leak of the actual game protocol What do you mean? How does a protocol get leaked? Do you mean like the backend code?

Infamia - November 14, 2018, 3:00 pm

(Nov 14, 2018 12:54 PM)whiter0x Wrote: [\[CITE\]](#) What if I tried capturing data from when I die, and re-send it using packeth (or similar?)?

Would kills/deaths be protected by a token or something?

i really doubt it, however take a go, you never know nowadays.

most protocols implement order and a certain error-boundary for packets to be sent out of order, else they are dropped.

protocols could also have you send a timestamp, most likely relevant for synchronization but may be used for other anticheat purposes.

as for your other question, yes, game protocols may be leaked because they are (a) recovered from leaked source code or (b) reversed by heuristic analysis of the packets themselves © recovered from binary analysis via RE.

whiter0x - November 15, 2018, 7:08 am

(Nov 14, 2018 04:00 PM)Infamia Wrote: [\[CITE\]](#) i really doubt it, however take a go, you never know nowadays.

most protocols implement order and a certain error-boundary for packets to be sent out of order, else they are dropped.

protocols could also have you send a timestamp, most likely relevant for synchronization but may be used for other anticheat purposes.

as for your other question, yes, game protocols may be leaked because they are (a) recovered from leaked source code or (b) reversed by heuristic analysis of the packets themselves © recovered from binary analysis via RE.

Could deaths/kills be on a different protocol???

when I kill someone, they kinda lag a bit before they actually die. No server connection problems (when lagswitch is off)

Is there anything you can tell me about this? It's a random packet's payload, I will comment 1 more if I find one interesting...

It's UDP

```
.EGDF'.g.D.....T$Z#.DDH.eD..l...s.....H.;W:...B..n.p...N.  
...6..1.....eV.-.....3....(....e.....4f.*.....*-p.=.....y.... QC.q.....u.j..... a.  
..x..... .P...#..",b...g.(...kS..j.
```

Infamia - November 15, 2018, 7:22 am

(Nov 15, 2018 08:08 AM)whiter0x Wrote: [\[CITE\]](#) Could deaths/kills be on a different protocol???

when I kill someone, they kinda lag a bit before they actually die. No server connection problems (when lagswitch is off)

Is there anything you can tell me about this? It's a random packet's payload, I will comment 1 more if I find one interesting...

It's UDP

.EGDF'.g.D.....T\$Z#.DDH.eD..l...s.....H.;W:...B..n.p...N.
...6..1.....eV.-.....3....(....e.....4f.*.....*.....-p.=.....y.... QC.q.....u.j..... a.
..x..... .P...#..",b...g.(...kS..j.

as i said the payload is most likely encrypted either via dtls or some other form of encryption.
if not, then it is definitely a binary protocol.

i really doubt that there are separate protocols for different events, a protocol is supposed to
subtend and categorize these events in a concise and efficient format.

Twistd - November 26, 2018, 11:52 am

(Nov 5, 2018 05:27 PM)whiter0x Wrote: [\[CITE\]](#) Hey all,

I have my setup as follows.

Xbox -- PC -- Router

All are connected via ethernet. My xbox is connected via usb dongle, and latter via built-in ethernet
port.

I recorded some data with wireshark. I would like to analyze this data somehow, but I don't know
where to start.

The data is being killed 3 times in "Grand Theft Auto V"

I was hoping I could have enough data to maybe make myself die by sending a
malicious/malformed packet, or something.

So my question is simple.

Is there a way to unencrypt the data, edit it, and resend it? Or is there a different approach?

Thanks!

(ALL OPINIONS WELCOME :))

In 99% of the games i reverse, they all uses custom encryption. Which means you'd need access to
the memory of the game it self.

You can't just resend encrypted data, decrypt it first and encrypt it yourself by hooking their packet
encryption is normally the easiest alternative.

Time to put on your gloves, root the box and disassemble or debug the game files to see what's up.

whiter0x - November 30, 2018, 5:49 am

Thank's everyone for your replies! I think that answered my questions.