

Forum:[Hack Forums](#)

Thread: [802.1x peap hacking?](#)

Rainb?w Dash - September 11, 2014, 5:27 am

Hey my school has a locked wifi and it comes up as 802.1x peap on my android. I cant find any tutorials or anything exept really outdated stuff so could someone help with this?

sp3ctrum - September 11, 2014, 10:34 am

Yayyy some Radius excitement. Seems your school is on the right track, but to my knowledge there is no direct way to hack "PEAP". There are ways to break it down but these methods seem to revolve around MITM and client side exploitation. That being said there isn't much to play around with, you will have to luck up and hope that TTLS protocol and certificates are improperly implemented. Improper cert usage would be either the school using a self signed certificate with the radius server, misconfiguration of clients to check for a certificate, & use of cert from a CA that has an improper RA function. A common attack is setting up a fake AP with a backend radius, capturing mschap challenge/response authentication packets with ASLEAP, and using hashcat or JTR to crack the hashes. There are other attacks but this all depends on how the radius is configured, you will have to do some digging around, as there are numerous of write ups and tutorials on EAP-LEAP-PEAP, ASLEAP, Radius, etc all over the wild.

Regards,
-Gator-

Rainb?w Dash - September 11, 2014, 1:31 pm

(Sep 11, 2014 10:34 AM)-Gator- Wrote: [\[CITE\]](#) Yayyy some Radius excitement. Seems your school is on the right track, but to my knowledge there is no direct way to hack "PEAP". There are ways to break it down but these methods seem to revolve around MITM and client side exploitation. That being said there isn't much to play around with, you will have to luck up and hope that TTLS protocol and certificates are improperly implemented. Improper cert usage would be either the school using a self signed certificate with the radius server, misconfiguration of clients to check for a certificate, & use of cert from a CA that has an improper RA function. A common attack is setting up a fake AP with a backend radius, capturing mschap challenge/response authentication packets with ASLEAP, and using hashcat or JTR to crack the hashes. There are other attacks but this all depends on how the radius is configured, you will have to do some digging around, as there are numerous of write ups and tutorials on EAP-LEAP-PEAP, ASLEAP, Radius, etc all over the wild.

Regards,
-Gator-Ok thanks I'm going to look around for some shit about this! :D

sp3ctrum - September 11, 2014, 2:54 pm

(Sep 11, 2014 01:31 PM)Rainb?w Dash Wrote: [\[CITE\]](#) Ok thanks I'm going to look around for some shit about this! :D

Okay, good luck Rainbow Dash! I found a few sources but most of them seem to be really outdated :/ Need any help just shoot me a pm.

ozair123 - March 11, 2020, 6:50 pm

(Sep 11, 2014 02:54 PM)sp3ctrum Wrote: [\[CITE\]](#) Okay, good luck Rainbow Dash! I found a few sources but most of them seem to be really outdated :/ Need any help just shoot me a pm.
Is there anyway to spoof on PEAP?

