Kerangka FYP – Diploma (DKM) – I-POP

BUAT RUJUKAN INTENSIF (BUKU/LAMAN WEB/ARTIKEL/TUTORIAL/INDIVIDU):

LATAR BELAKANG (AMALAN BIASA/KEADAAN SEDIA ADA/SENARIO):
Wireless network seperti wifi adalah sangat penting bagi pengguna.Khususnya kepada pengguna yang ingin bergerak 'bebas' dari ethernet cable yang sentiasa mengekang mobiliti user. Namun dalam faedah wireless network, terdapat juga risiko dan bahaya yang akan terjadi bila sesebuah wireless mempunyai sistem keselamatan yang lemah.

PENYATAAN MASALAH (MASALAH/ISU/KELEMAHAN/KEKURANGAN):
Permasalahan itu terjadi apabila adanya individu yang tidak bertanggungjawab cuba untuk menceroboh rangkaian secara wireless.
Access point didapati mudah untuk ditembusi atas sebab kelemahan sistem keselamatan

CADANGAN (IDEA SELESAI/IDEA TAMBAHBAIK/IDEA UBAH):
Membuat MAC Binding Whitelist agar MAC address yang berdaftar sahaja yang boleh connect kepada WLAN

KUMP. SASARAN (PENGGUNA/PENONTON/ KLIEN):
1.Client(user di dalam network)

OBJEKTIF PROJEK (PROJEK MESTI BOLEH?):
1. Membuat *serangan* terhadap *Access point* (AP) dengan menggunakan Aircrack-ng
2. Membangunkan MAC Binding Whitelist untuk meningkatkan keselamatan WLAN

REKABENTUK PROJEK (PRODUK AKHIR):
Sebuah network yang telah siap pasang beserta AP untuk membangun sebuah rangkaian wireless.
Sebuah laptop beserta wifi adapter untuk menguji serangan terhadap wireless network.

SINOPSIS/CIRI-CIRI/FEATURES PROJEK (KONSEP, SKOP, TEKNIKAL):
Pengujian serangan terhadap wireless network akan dilakukan terhadap AP. Selepas itu, langkah – langkah pencegahan bagi mengurangkan risiko serangan akan diambil supaya network akan berada dalam keadaan yang selamat.

TAJUK PROJEK: Wireless Attack on WPA2 Using Aircrack-ng

KRITERIA REKA BENTUK:
1.Sebuah network internet yang mempunyai client
2.Network tersebut disambungkan ke AP bagi membangunkan WLAN
3.Sambungan WLAN kepada client
4.Laptop yang disediakan untuk uji serangan terhadap AP

BAHAN / MATERIAL:
1. Wireless Adapter
2. Laptop
3. PC Client
4. Kali Linux
5.Access Point
6.PC Web Server
7.Cable UTP Straight Cable

KAEDAH/AKTIVITI/TEKNIK:
1.Membuat serangan terhadap WIFI dengan menggunakan kali linux.
2.Mengenalpasti dan mengimbas IP Address beserta port services di dalam LAN
3.Hacker berjaya membuka web server
4.Melakukan konfigurasi semula untuk meningkatkan keselamatan WLAN
5.Menguji serangan semula bagi memastikan ciri keselamatan telah berfungsi dengan baik.

PERKAKASAN/PERISIAN/ PERALATAN:
1.Aircrack-ng
2.Kali Linux
3.XAMPP

PETUNJUK PRESTASI PROJEK:
Network WLAN yang dibangunkan berjaya mengatasi serangan dari penyerang

KAEDAH PENGUJIAN PROJEK:
Pengujian secara simulasi/demo model.
Pengujian secara sebenar di makmal.

KEPENTINGAN / FAEDAH PROJEK (IMPAK PROJEK KEPADA SASARAN):
1. Keselamatan data peribadi dan web server pengguna yang menggunakan network tersebut akan terjamin.