ခေတ်မင်းညို့

Wireless Technologies

and

WiFi Hacking

ကျေးဇူးတင်လွှာ

အနန္တော အနန္တ ငါးပါးကို ဦးထိပ်ထားလျက် ကျွန်တော့်ရဲ့ သင်ဆရာ၊ မြင်ဆရာ၊ ကြားဆရာများနှင့်တကွ ဤစာအုပ် ဖြစ်မြောက်ရေးအတွက် အဘက်ဘက်မှ ဝိုင်းဝန်းကူညီ အကြံဉာဏ်များ ပေးခဲ့ကြပါသော မိတ်ဆွေများ၊ အသေးစိတ် ဖတ်ရှုပြီး စာလုံးပေါင်းမှအစ ပြင်ဆင် ပေးခဲ့ပါသော ဆရာ မျိုးမြင့်ထိုက် (mmCERT)၊ Preview များ ရေးပေးကြပါသော UCSY မှ တီချယ်မီ၊ နည်းပညာနယ်ပယ်မှ စိနယာအစ်ကိုတော်များ၊ ထုတ်ဝေဖြန့်ချီရေးအတွက် အကူညီများ ပေးခဲ့ပါသော ဆရာမင်းတခေတ် (Khit Publishing House)၊ ဤစာအုပ်ရေးနေစဉ် ကြုံရသော အခက်အခဲများ စိတ်ဖိစီးမှုများအတွက် ညည်းညူခြင်းအလျဉ်းမရှိဘဲ ကျွန်တော်လုပ်ချင်ရာ လုပ်ခွင့် ရအောင် ပံ့ကူပေးခဲ့ပါသော ကျွန်တော့် ဇနီးသည်၊ ဤသို့သော စာအုပ်များကို ဆက်လက် ရေးသားနိုင်စေရန်အတွက် ထုတ်ခဲ့သမျှ စာအုပ်တိုင်းကို အားပေးခဲ့ကြပါသော နည်းပညာချစ်သူများနှင့် အခြားအခြားသော ကျေးဇူးတင်ထိုက်သူအားလုံးကို အထူးပင် ကျေးဇူးတင်ရှိပါကြောင်း ဦးစွာ ဖော်ပြပါရစေခင်ဗျာ။

စာရေးသူ

Preview

ကလောင်ရှင် မောင်ခေတ်မင်းညီ မြန်မာဘာသာဖြင့် ရေးသားထားသော Wireless Hacking စာအုပ်သည် အခြေခံမှစ၍ လက်တွေ့စမ်းသပ်နိုင်ရန်အထိ ပြည့်စုံစွာ ဖော်ပြထားခြင်း၊ အရေးအသား ရှင်းလင်း ပြေပြစ်မှုရှိခြင်း၊ အချိတ်အဆက်မိခြင်းတို့ကြောင့် Wireless Security နှင့် Hacking အပိုင်း လေ့လာလိုသော ကျောင်းသား၊ ကျောင်းသူများနှင့် စိတ်ဝင်စားသူများ မည်သူမဆို ဝယ်ယူဖတ်ရှုသင့်သော စာအုပ်ကောင်းတစ်အုပ် ဖြစ်ပါသည်။

Prof. Dr. Mie Mie Su Thwin
University of Computer Studies, Yangon (UCSY)

Preview

မြန်မာပြည်မှာ မြန်မာဘာသာနဲ့.ရေးထားတဲ့ IT စာအုပ်တွေက ရှားပါတယ်။
ဒီအထဲမှာ Security အပိုင်းကပိုရှားပါတယ်။
ကိုခေတ်မင်းညီရေးထားတဲ့ ဒီစာအုပ်ဟာ Security အပိုင်းလေ့လာနေသူတွေအဖို့
တစ်ဖက်တလမ်းက အထောက်အကူဖြစ်ပါလိမ့်မယ်။
Wireless Hacking အပိုင်းတခုတည်းကို Theory, Technique, Tool တွေအားလုံး method
အဆင့်အဆင့်နဲ့ သေချာရှင်းပြထားတာဟာ ဖတ်ရသူဖို့ အတော်ကို ကျေနပ်အားရစရာ
ဖြစ်ပါလိမ့်မယ်။

Thet Khine

Preview

Wireless Hacking နဲ့ပတ်သက်တဲ့ Concept, Knowledge, နှင့် Tools အသုံးပြုပုံတွေကို စာအုပြင် ပုံနဲ့သေချာရှင်းပြထားတဲ့အတွက် လေ့လာရ လွယ်ကူစေပြီး လက်တွေ့ကျတဲ့ သင်ခန်းစာတွေက ပိုပြီး အထောက်အကူဖြစ်စေမှာ အမှန်ပါပဲ။
ပြောရရင် ဒီစာအုပ်နဲ့ပတ်သက်ပြီး မြန်မာလို ပြည့်ပြည့်စုံစုံရှင်းပြပေးထားတဲ့အတွက်ကြောင့် စပြီးလေ့လာတဲ့သူတွေသာမက ပိုပြီး အသေးစိတ်သိချင်တဲ့လူတွေအတွက် လက်မလွတ်ဘဲ ဖတ်သင့်တဲ့စာအုပ်ကောင်းတစ်အုပ်ပါ..

Min Ko Ko
Founder of Creatigon & Myanmar Security Forum

စာရေးသူ၏အမှာစာ

ယနေ့ခေတ်မှာ WiFi network တွေက နေရာတိုင်းလိုလိုမှာ ရှိနေကြပါပြီ။ မြို့ကြီးတွေမှာဆို အိမ်တိုင်းနီးပါးမှာ WiFi တွေကို အသုံးပြုနေကြပါတယ်။ အချို့ဆို WiFi ကို သုံးပြီး မိမိတို့ နေအိမ်ရဲ့ CCTV စနစ်တွေကိုပါ အဝေးကနေ လှမ်းကြည့်ချိတ်ဆက်နိုင်အောင် အထိ အသုံးချလျက် ရှိနေပါတယ်။ ဒါကြောင့်မို့ Wireless Hacking နဲ့ Wireless Security ရဲ့ အရေးပါမှုက မြင့်တက်လာပါတယ်။

Wireless Network ထဲကို Malicious Attacker တစ်ယောက်ယောက် ရောက်ရှိလာတဲ့အခါ ကျွန်တော်တို့ရဲ့ လုံခြုံရေးအတွက် အသုံးပြုထားတဲ့ အဆိုပါ စီစီတီဗီကင်မရာတွေသည် ကျွန်တော်တို့အတွက် မလုံခြုံမှု ပြန်လည်ဖြစ်သွားစေနိုင်သလို၊ အဆိုပါ ကွန်ယက်မှာ အသုံးပြုနေတဲ့ ကျွန်တော်တို့ရဲ့ IOT device တွေရဲ့ လုံခြုံမှုကိုလည်း ကျိုးပေါက်သွားစေနိုင်ပါတယ်။ အခန်း ၁၂ မှာ နမူနာအနေနဲ့ ကျွန်တော်တို့ရဲ့ ကွန်ယက်ထဲက Windows 10 computer တစ်လုံးကို login bypass လုပ်ပြထားပါတယ်။

Wireless Security နဲ့ ပတ်သက်ပြီးတော့တော့ ဒီစာအုပ်ထဲမှာ သီးသန့် ထည့်ရေးမထားပါဘူး။ ဆိုလိုတာက WiFi hacking နဲ့ ပတ်သက်ပြီး ဆွေးနွေးထားပေမယ့် ဘယ်လို လုံခြုံအောင် ထားရမယ်ဆိုတာကိုတော့ မိမိတို့ဘာသာ ဆက်စဉ်းစားနိုင်ဖို့ ချန်လှပ်ထားခဲ့ပါတယ်။ ဘယ်လိုနည်းလမ်းတွေနဲ့ hack လေ့ရှိတယ်ဆိုတာကို သေချာသိသွားပြီ ဆိုရင် ဘယ်လို ပိုလုံခြုံအောင် ထားရမယ်ဆိုတာက တွေးလို့ ရသွားပြီမို့ပါ။

ဒီစာအုပ်လေးကို ရေးဖို့ စဉ်းစားတော့ ပထမဆုံးအနေနဲ့ ပြေးမြင်မိတာ WiFu ပါ။ ကျွန်တော်လေ့လာခဲ့ဖူးတဲ့ WiFu ထဲက သင်ခန်းစာတွေက ကျွန်တော့်ကို ဆွဲဆောင်နေပါတယ်။ ဒီခါတော့ WiFu မှာ စီစဉ်ထားတဲ့ အစီအစဉ်ကို မာတိကာအနေနဲ့ ယူမသုံးခဲ့လိုက်ပါဘူး။ လေးစားစွာဖြင့် ဝန်ခံရမယ်ဆိုရင်တော့ ကျွန်တော့်အနေနဲ့ Offensive Security ရဲ့ Public cap ဖိုင်တွေကို packet တွေအကြောင်းရှင်းပြရာမှာ ယူသုံးဖြစ်ခဲ့လိုက်ပါတယ်။

အကြောင်းကတော့ ကျွန်တော်ဘာသာ ဖန်တီးရယူထားတဲ့ captured file တွေကို စိတ်ကျေနပ်မှုမရှိတဲ့အတွက်ပါ။ အချို့ဖိုင်တွေက လိုအပ်ချက်တွေ ရှိနေသလို အချို့မှာ ကျတော့ လိုအပ်တာထက် ပိုပြီး ဖောင်းပွတဲ့ information တွေ ပါနေပြန်ပါတယ်။ ဒါကြောင့် permission မထားဘဲ Download ယူခွင့်ပေးထားတဲ့ Offensive Security ရဲ့ pcap file တွေကို ယူသုံးဖြစ်လိုက်တာပါ။ အကြောင်းအရာပိုင်းဆိုင်ရာ ရှင်းလင်းချက်တွေ အကိုးအကားတွေကတော့ သက်ဆိုင်ရာ Public Sources တွေကနေပဲ ယူသုံးထားပါတယ်။ ယူသုံးထားတဲ့ Link တွေကိုလည်း ထည့်သွင်းပေးထားပါတယ်။

ဒါကြောင့်မို့ ဒီစာအုပ်သည် Offensive Security ရဲ့ WiFu ကို ပြန်ဆိုထားတဲ့ စာအုပ် လုံးဝ မဟုတ်ပါဘူး။ **captured file အချို့ကိုသာ ရှင်းပြရာမှာ sample အဖြစ် ယူသုံးထားခြင်း ဖြစ်ပါတယ်။** အကြောင်းအရာတစ်ခုချင်းစီအလိုက် သက်ဆိုင်ရာ source link တွေကိုပါ ပူးတွဲ ထည့်သွင်းဖော်ပြပေးထားပါတယ်။ နောက်တစ်ခုက အချို့ရဲ့ ထင်မြင်ယူဆချက်လေးတွေနဲ့ ပတ်သက်ပြီး အနည်းငယ် ကြိုတင်ရှင်းပြပါရစေ။

ဘာကိုလဲဆိုတော့ WiFi Hacking နဲ့ ပတ်သက်ပြီး ဒီလောက်ထူတဲ့ စာအုပ်ရေးစရာလိုလို့လား ဆိုတာမျိုး မေးခွန်းတွေ တွေ့ဖူးလို့ဖြစ်ပါတယ်။ သိသင့်တာတွေ ထည့်ရင်း ထည့်ရင်းနဲ့ ဒီစာအုပ်က ထူ သွားပါတယ်။ ဒါပေမယ့်လို့ သိကိုသိထားသင့်တာတွေကို မကျန်ခဲ့ဖို့နဲ့ အခြေခံကျတဲ့ အကြောင်းအရာတွေကို တီးခေါက်မိပြီး ပိုကောင်းတဲ့နည်းလမ်းတွေကို မိမိတို့ဘာသာ ထပ်မံစဉ်းစားတိုးချဲ့နိုင်ဖို့ရာအတွက် လိုအပ်တဲ့ knowledge တွေမို့လို့ ထည့်ခဲ့တာ ဖြစ်ပါတယ်။ ဒါကြောင့်မို့ စာအုပ် စစချင်း ဖော်ပြထားတာတွေကို ဖတ်ရတာ ပျင်းစရာလို့ ထင်ကောင်း ထင်နိုင်ပါတယ်။ သေချာလေ့လာလိုသူတွေအတွက်တော့ ပျော်စရာ ဖြစ်မယ်လို့ ယုံကြည်ပါတယ်။

ဒီစာအုပ်လေးနဲ့ပတ်သက်ပြီး မေးမြန်းကြတဲ့အထဲမှာ Windows နဲ့ရော လေ့လာလို့ ရလား။ Kali မှ သုံးလို့ရတာလား။ Android မှာရော ရလား ဆိုတာတွေ ပါဝင်ပါတယ်။ ဒါတွေကို ဒီ အမှာစာလေးထဲမှာ စုစည်းပြီး ပြန်ဖြေပေးပါရစေ။ ဒီစာအုပ်ထဲက အကြောင်းအရာတွေကို Kali, Ubuntu, Parrot, Debian, Fedora, BlackArch အစရှိတဲ့ Linux တွေအားလုံးမှာ လေ့လာနိုင်သလိုပဲ Windows နဲ့ Android system တွေမှာပါ လေ့လာလို့ ရပါတယ်။ Android မှာလည်း လေ့လာလို့ ရတယ်ဆိုပေမယ့်လို့ စာအုပ်ထဲက အကြောင်းအရာတိုင်းကိုတော့ Android မှာ လိုက်လုပ်လို့ ရမှာ မဟုတ်ပါဘူး။ အချို့သော practical တွေကိုသာ လိုက်လုပ်ကြည့်နိုင်မှာ ဖြစ်ပြီး အချို့ကိုတော့ စာတွေ့လောက်ပဲ လေ့လာလို့ ရပါလိမ့်မယ်။

ကျွန်တော့်အနေနဲ့ အကြံပြုရမယ်ဆိုရင်တော့ Kali or Parrot Security OS တို့လို Security/Hacking/PenTesting အတွက် ထုတ်ထားတဲ့ System တွေကို ပိုပြီး အားပေးပါရစေ။ Ubuntu လို Linux တွေမှာလည်း အဆင်ပြေပေမယ့်လို့ လိုအပ်တဲ့ Tool တွေကိုတော့ ထပ်မံ install လုပ်ပြီးမှသာ သုံးလို့ရမှာမို့ပါ။ နောက်တစ်ချက်က Wireless Adapter ပါ။ အချို့သော Wireless Adapter တွေသည် Monitored Mode မှာ ကောင်းကောင်း အလုပ်မလုပ်နိုင်ကြပါဘူး။ ဒါကြောင့်မို့ အချို့သော Laptop တွေမှာ Built-in adapter ပါပေမယ့်လို့ Wireless Adapter တစ်ခု ထပ်လိုအပ်တာမျိုးလည်း ဖြစ်ကောင်းဖြစ်နိုင်ပါတယ်။

Wireless Adapter တွေထဲက ဘာတွေ ရွေးသင့်လဲဆိုတာကိုလည်း စာအုပ်လေးထဲမှာ အခန်း ၅ နဲ့ အခန်း ၁၂ မှာ ဖော်ပြပေးထားပါတယ်။ Desktop Computer တစ်လုံးကို သုံးပြီး လေ့လာချင်တာဆိုရင်တော့ Adapter တစ်ခုကို ကျိန်းသေ လိုအပ်မှာ ဖြစ်ပါတယ်။ နောက်တစ်ချက်က ဒီစာအုပ်လေးနဲ့ ပတ်သက်ပြီး ထပ်သိသင့်တာတွေနဲ့ အချို့ အခက်အခဲတွေ ကြုံတွေ့တဲ့အခါ ဆွေးနွေးနိုင်ဖို့အတွက်ကို Facebook Group လေးတစ်ခု ဖွင့်ထားပေးပါတယ်။ Member Form ပေါ်က ID ကို ဖြည့်ပြီး Group မှာ ဝင် Join နိုင်ပါတယ်။

ဆိုခဲ့သမျှကို အကျဉ်းချုပ်ပြီး ပြန်ဆွေးနွေးရရင် ဒီစာအုပ်မှာ သိသင့်သိထိုက်တဲ့ အခြေခံသဘောတရားတွေကိုပါ ထည့်သွင်းထားတာဖြစ်လို့ စာရှူသူတို့အနေနဲ့ စိတ်ဝင်စားမှာ မဟုတ်တဲ့ အကြောင်းအရာအချို့ ပါနေနိုင်ပါတယ်။ ဒါပေမယ့်လို့ သည်းခံဖတ်ရှုပေးပါ။ အနည်းဆုံးတော့ ဗဟုသုတအနေနဲ့ဖြစ်ဖြစ်ပေါ့။ ကျော်မချဘဲ ဖတ်သွားစေချင်ပါတယ်။

အဲသလိုပဲ Captured File တွေကို လက်တွေ့လေ့လာတဲ့အပိုင်းတွေကိုလည်း ပုံကြည့်ရုံနဲ့ ဒါလွယ်ပါတယ်ဆိုပြီး ကျော်ချလိုက်တာထက် ကိုယ်တိုင် သေချာလုပ်ကြည့်ပြီး analyze လုပ်စေချင်ပါတယ်။ နောက်ပြီးတော့ စာအုပ်ထဲမှာ ဒီဘက်ခေတ်မှာ သိပ်မသုံးတော့တဲ့ WEP encryption ကို crack တဲ့အပိုင်းတွေလည်း ပါပါသေးတယ်။ အခန်း ၂ ခန်းတောင်မှ ထည့်ရေးထားတယ်ဆိုပြီး မကျော်ခဲ့စေချင်ပါဘူး။ ဘာကြောင့်လဲဆိုတော့ Deauthentication တို့၊ Fake Authentication တို့ စတဲ့ အကြောင်းအရာတွေကို အဲသည်မှာ အသေးစိတ် ဆွေးနွေးထားလို့ ဖြစ်ပါတယ်။ စာရှူသူများအား အထူးပင် ကျေးဇူးတင်ရှိပါတယ်ခင်ဗျာ။

လေ့လာနေသူအပေါင်း ကိုယ်စိတ်နှစ်ဖြာ ရွှင်လန်းချမ်းမြေ့စွာဖြင့်
မိမိတို့ ဝါသနာပါရာ ပညာရပ်များကို
ထူးချွန်စွာ တတ်မြောက် ကျွမ်းကျင်ကြပါစေကြောင်း
ဆန္ဒပြုလျက်

စာရေးသူ

မာတိကာ

Chapter 1: IEEE စံနှုန်းများအကြောင်း မိတ်ဆက်

Chapter 2: ကြိုးမဲ့ကွန်ယက်များအကြောင်း

Chapter3: Packet များနှင့် Network ၏ တုံ့ပြန်မှုများကို လေ့လာခြင်း

Chapter3: Packet များနှင့် Network ၏ တုံ့ပြန်မှုများကို လေ့လာခြင်း

Chapter 4: ကြိုးမဲ့ကွန်ယက်များ၏ လုံခြုံရေးဆိုင်ရာ နည်းပညာများနှင့် အထွေထွေ

Chapter 5: WiFi hacking ပြုလုပ်ရန်အတွက် ပြင်ဆင်ခြင်း

Chapter 5: WiFi hacking ပြုလုပ်ရန်အတွက် ပြင်ဆင်ခြင်း

Chapter 6: Linux ဖြင့် WiFi hacking ပြုလုပ်ရန်အတွက် သိရန်လိုအပ်သည်များ

Chapter 7: Aircrack Suit ကို လေ့လာခြင်း

Chapter 8: WEP ကို Crack ကြည့်ခြင်း

Chapter 8: WEP ကို Crack ကြည့်ခြင်း

Chapter 9: WEP Password Cracking အပိုင်း ၂

Chapter 10: WPA & WPA2 Cracking

Chapter 11: Other Tools

Chapter 12: Additional

CHAPTER 1
IEEE စံနှုန်းများအကြောင်း မိတ်ဆက်

1. IEEE 802.11 အကြောင်း
1.1. IEEE ဆိုတာ

IEEE ဆိုတာ ကျွမ်းကျင်နည်းပညာရှင်ပေါင်းများစွာ ပါဝင်စုဖွဲ့ထားတဲ့ ကမ္ဘာ့အကြီးဆုံး အဖွဲ့အစည်းကြီးတစ်ခုလို့ ဆိုနိုင်ပါတယ်။ IEEE ဆိုတာ Institute of Electrical and Electronics Engineers ကို အတိုကောက်သုံးထားခြင်းဖြစ်ပါတယ်။ လျှပ်စစ်နှင့် အီလက်ထရောနစ်ဆိုင်ရာ အင်ဂျင်နီယာကျောင်း လို့ ဆိုနိုင်ပါတယ်။ အဲသည်မှာ သိပ္ပံပညာရှင်တွေ၊ အင်ဂျင်နီယာတွေ၊ အာသာသသိပ္ပံလို၊ Telecommunication နဲ့ Biomedical လို၊ EP တွေလို ကမ္ဘာတစ်ဝှမ်းလုံးက တကယ့်ထိပ်တန်း ကျွမ်းကျင်ပညာရှင်တွေ ပါဝင်နေတဲ့အဖွဲ့အစည်းကြီးတစ်ခုလို့ ဆိုနိုင်ပါတယ်။ https://www.ieee.org/about/ieee-history.html မှာ သူ့ရဲ့ သမိုင်းကြောင်းကို အကျယ်တဝင့် သွားရောက် လေ့လာနိုင်ပါတယ်။

IEEE ရယ်လို့ ဖြစ်မလာခင်တုန်းက IEEE ကိုဖြစ်ပေါ်စေတဲ့ ကျောင်းနှစ်ကျောင်း ရှိခဲ့တာပါ။ ကြိုးနဲ့ဆက်သွယ်တဲ့ ဆက်သွယ်ရေးနဲ့ လျှပ်စစ်မာတ်အားဆိုင်ရာ ဘာသာရပ်တွေကို သင်ကြားပေးတဲ့ American Institute of Electrical Engineers ဆိုတဲ့ AIEE ကျောင်းနဲ့ Institute of Radio Engineers (IRE) ဆိုတဲ့ ကြိုးမဲ့ဆက်သွယ်ရေးနည်းပညာပိုင်း သင်ကြားပေးတဲ့ကျောင်းဆိုပြီးတော့ပါ။ 1963 မှာတော့ အဲသည်ကျောင်းတော်ကြီးနှစ်ခုကို ပူးပေါင်းလိုက်ပြီး IEEE ရယ်လို့ ဖြစ်ပေါ်လာစေခဲ့ပါတယ်။

IEEE မှာ ကော်မတီတွေ အများကြီးပါဝင်ပြီး သီးခြားစီ ခွဲခြားထားပေးပါတယ်။ ကျွန်တော်တို့နဲ့ ရင်းနှီးပြီးသားဖြစ်တဲ့ LAN (Local Area Network) နဲ့ MAN (Metropolitan Area Network) တို့အတွက် စံတွေကိုတော့ IEEE ရဲ့ 802 ကော်မတီကနေ develop လုပ်ပေးခဲ့တာဖြစ်ပါတယ်။ အကျော်ကြားဆုံးကတော့ Ethernet, Token Ring, Wireless LAN, Bridging နဲ့ Bridged LAN (for virtual) နည်းပညာတွေပဲ ဖြစ်ပါတယ်။ IEEE specification မှာ Lowest OSI layer နှစ်ခု ပါဝင်ပြီး Physical Layer နဲ့ Link Layer လို့ မှတ်ထားနိုင်ပါတယ်။

Link Layer ကိုတော့ sub-layer နှစ်ခုပြန်ခွဲထားပါတယ်။ ဘာတွေလဲဆိုရင်တော့ Logical Link Control (LLC) နဲ့ ကျွန်တော်တို့ အားလုံးနီးပါး သိကြတဲ့ Media Access Control (MAC) တို့ပဲ ဖြစ်ပါတယ်။ http://www.ieee802.org/ မှာ IEEE 802 အကြောင်း အကျယ်လေ့လာနိုင်ပါတယ်။ အဖွဲ့ဝင်ချင်တယ်ဆိုရင်လည်း https://www.ieee.org/membership/join မှာ အခမဲ့ဝင်ရောက်နိုင်ပါတယ်။