Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 1
BEING A HACKER
HACKER တစ်ဦးဖြစ်တည်မှု

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 2012, ISECOM
WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

ဤ Hacker Highschool စီမံကိန်း သည်၊ လေ့လာသင်ယူရေး ကရိယာ တစ်ခုဖြစ်ပြီး လေ့လာရေး အချက်များပါဝင်သည့်အလျောက် အနာဃတရာယ်ရှိပါသည်။ အကယ်၍ အချို့သောသင်ခန်းစာများအား၊ တလွဲအသုံး ချခြင်း၊ အဖျက်အမှောင့်ရည်ရွယ်ချက်ဖြင့်သုံးခြင်းသည်၊ ကိုယ်တိုင်နစ်နာမှုများဖြစ်စေနိုင်ပါသည်။ နည်းပညာ ၁ အချက်အလက်များမှ ဖြစ်နိုင်ချေရှိသောရလာဒ်များကို သေချာစွာလေ့လာမထားပါက၊ ဘေးထွက်ဆိုးကျိုးများ ဖြစ်ပေါ်လာနိုင်ပါသည်။ ဤသင်ခန်းစာများကိုအသုံးပြုသော ကျောင်းသား၊ သူများသည်၊ လေ့လာခြင်း၊ကြိုးစား အားထုတ်ခြင်းနှင့် လက်တွေ့အသုံးချခြင်းများ ပြုလုပ်ရာတွင် ကောင်းစွာသင်ကြားခြင်းများကို သင်ယူခြင်း အပြင်၊ စနစ်တကျ ကြီးကြပ်ခြင်းကို ခံယူသင့်ပါသည်။ မည်သို့ဖြစ်စေ ISECOM အဖွဲ့အစည်းမှ ဤသင်ခန်းစာများ တွင်ပါဝင်သော မည်သည့်သတင်းအချက်အလက်များကိုမဆို လွဲမှားစွာအသုံးပြုခြင်းအတွက် တာဝန်ယူနိုင်မည် မဟုတ်ပါ။

အောက်ပါသင်ခန်းစာများ၊ လေ့ကျင့်ခန်း စာအုပ်များကို မည်သူမဆို ISECOM ၏စည်းကမ်းချက်များ အား လိုက်နာ၍ ဖတ်ရှုလေ့လာနိုင်ပါသည်။ ပုဂ္ဂလိကနည်းပညာကျောင်း၊ နိုင်ငံတော် နည်းပညာကျောင်းများ၊ အခြေခံအလယ်တန်း၊အထက်တန်းများတွင် Hacker Highschool စီမံကိန်းမှ ဆောင်ရွက်မှုများ အားလုံးကို စီးပွားဖြစ်အသုံးပြုခြင်းများအား တားမြစ်ပါသည်။ ဤစာအုပ်ပါ အချက်အလက်များအား ကူးယူ၍၊ မည်သည့် ပုံစံဖြင့်ဖြစ်စေ ပြန်လည်ထုတ်လုပ်ရောင်းချခြင်းများအား တားမြစ်ပါသည်။

ဤစာအုပ်ပါအချက်အလက်များမှမည်သည့်အမျိုးအစားဖြစ်စေ၊သင်ခန်းစာဖြစ်စေ (သို့)လေ့ကျင့်ခန်း များဖြစ်စေ ပါဝင်မှုများအား ခွင့်ပြုချက်လိုင်စင် မရှိပဲ တန်ဖိုးတစ်ခုခုဖြင့်ရောင်းချခြင်းကို ပြင်းထန်စွာတားမြစ်ထားပါသည်။

လိုင်စင်ဂယ်ယူရန် http://www.hackerhighschool.org/licensing.html HHS website တွင်ဂယ်ယူနိုင်ပါသည်။ ဤ HHS စီမံကိန်းတွင် အဖိုးတန်မှု၊အကျိုးရှိမှုများ ရှိမည်ဆိုလျင်၊ HHS အား License ဂယ်ယူခြင်း၊ လူဒါန်းခြင်း၊အထောက်အပံ့ပေးခြင်းများ ဖြင့် ကူညီပေးပါရန် တောင်းဆိုပါသည်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Table of Contents

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Contributors - ထောက်ပံ့ပေးသူများ

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Shaun Copplestone, ISECOM
Greg Playle, ISECOM
Jeff Cleveland, ISECOM
Simone Onofri, ISECOM
Tom Thomas, ISECOM

Translators

Htet Aung @Starry Sky, Myanmar

ISECOM

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

HACKING ၏စေတနာများ

Pete Herzog ၏မိတ်ဆက်စကား

မည်သို့ဖြစ်စေ၊ Hacker များအကြောင်း ခင်ဗျားကြားဖူးပါလိမ့်မည်၊ ၎င်းတို့ကရှာဖွေတွေ့ရှိခြင်းကိုအကောင်းဆုံးလုပ်နိုင်သူတွေဖြစ်ကြပါတယ်။ Hacker များကစိတ်အားထက်သန်သူများ၊ စွမ်းဆောင်ရည်ပြည့်ဝသူများ၊ ထိုးထွင်းတီထွင်နိုင်စွမ်းရှိသူများဖြစ်ကြသည်။ Hacker များကအရာဝတ္ထုတွေမည်သို့အလုပ်လုပ်သည်မှစ၍ မည် သို့ထိမ်းချုပ်ရမည်၊ ၎င်းတို့ကိုမည်သို့ပြောင်းလဲအသုံးပြုနိုင်သည်အထိ နက်နက်ရှိုင်းရှိုင်းလေ့လာလုပ်ဆောင်ကြသည်။ ထိုသို့ပြုလုပ်ခြင်းသည် Hacker များအတွက်ကျယ်ပြန့်သောစိတ်ကူးများကိုပင်လျင် ပြန်လည်ပုံပေါ်နိုင်စေတယ်။ ထို့အပြင်သိပ္ပံနည်းကျသိုလိုစိတ်ပြင်းပြမှုအမှားတစ်ခုထဲကို ရလာဒ်တစ်ခုထဲဖြစ်ခြင်းအား၊ အတိအက ျ သိနိုင်ရန်ထပ်တူအမှားမျိုးအကြိမ်ကြိမ်လုပ်ရန ် ၎နေးကြသူများမဟုတ်ပါ။ ဤကဲ့သို့ကျရှုံးခြင်းများသည်လေ့လ ာ သင်ယူရန်နည်းသစ်တွေ့ရှိချက်များဖြစ်သောကြောင့် Hacker များက ကျရှုံးခြင်းကိုအချိန်ဖြုန်းခြင်းအမှားဟုမယူဆ ကြပါဘူး။ ဤအယူအဆသည် မည်သည့်အသင်းအဖွဲ့တွင်မဆို ရှိသင့်ပါတယ်။

> *Hacking လုပ်ခြင်းကြောင့် ဒုက္ခသဓေတွေ့နေသူတွေ၊ အထူးသဖြင့် Media တွေက Hacker လို့ သတ်မှတ်ခြင်း ခံနေရတဲ့ သူတွေကအမှန်တကယ် Hacker မဟုတ်ကြပါဘူး။*

Hacker တစ်ယောက်က တက်ကြွဖျတ်လတ်သောပုံစံ၊ လက်တွေ့ဆန်သော သိပ္ပံသဘောပညာရှင်ပုံစံ၊ တစ်ခါတစ်ရံ ရူးနှမ်းနေတဲ့သိပ္ပံသဘောပညာရှင်ပုံစံဖြစ်ပေမယ့်၊ တကယ့်သိပ္ပံသဘောပညာရှင်တွေမဟုတ်တာကြောင့် စိတ်ခံစားချက်နောက်ပို့၍ လိုက်တတ်ကြပါတယ်။ ဤအချက်ကအမှန်တကယ်ဆိုးဝါးတဲ့အချက်မဟုတ်ပါဘူး။ အချိန်အခါတစ်ခုမှာအမှန ် တရားလို့ယူဆထားမှု၊ ယုံကြည်ထားမှုအစဉ်အလာနောက်ကို မလိုက်ကြတဲ့လူတွေကများစွာသောစိတ်ဝင်စား ဖွယ်အရာများကိုတီထွင်ကြံဆခဲ့ကြပါတယ်။ သချာသဘောပညာရှင် George Cantor ဆိုသူက ၎င်း၏အတွေးအခေါ် အသစ ် (infinity) ကိုအဆိုပြုတင်ပြခဲ့ပြီး များစွာသောပညာရှင်များကြားတွင်ဦးတည်ချက် ပြတ်စေသောကာလကို ဖြစ်ပေါ်စေခဲ့သည့်သီအိုရီကိုဖြစ်စေခဲ့ပြီး ထိုအချက်ကြောင့်၎င်း၏ စိတ်ကူးသစ်ကို သချာသဘောပညာအားကူးဆက ် နေသော စိုးရိမ်ဖွယ်ရောဂါဟုခေါ်ဆိုခဲ့ကြသည်။

အရူးသိပ္ပံသဘောပညာရှင်လို ခေါ်ကြတဲ့ Nikola Tesla ကတော့ ၊ လျှပ်စစ်တွေ ဘယ်လိုသဘာဝရှိတယ်ဆိုတာကို တပါးသူတွေထက် ပိုသိတဲ့လူတစ်ယောက်ပါ။ သူကတော ့ AC လျှပ်စစ်သုံး ပထမဆုံးဘီးမပါတဲ့မော်တာကို တီထွင်ခဲ့ပြီး အများကတော့ Tesla ကွိုင်လို့ပဲသိကြပါတယ်။

Ignaz Philipp Semmelweis ဆိုသူက လူနာတွေကြားမှာရောဂါပြန့်ပွားမှုကိုထိမ်းသိမ်းရန် ဆရာဝန်တွေက လူနာများကိုပြုစုစောင့်ရှောက်မှုလုပ်နေစဉ်မှာသူတို့လက်တွေကိုဆေးကြောသန့်စင်ရန်လိုအပ်တယ်လို့ယူဆခဲ့တဲ့ဆရာဝန်တစ်ဦးပါ။ လူနာတွေကြားမှာရောဂါပြန့်နှံ့မှုတိုးပွားနေတာသူ၏အမှားဟုယူဆပြီးလူနာတွေကို ကြည့်ရှုနေချိန်အတွင်းဂရုတစိုက်လက်ဆေးခြင်းပြုလုပ်၍လက်တွေ့စမ်းသပ်ခဲ့ပြီး၊ ရောဂါပြန့်နှံ့မှုသေချာပေါက်ပျောက်ကွယ်သွားသည်ကိုတွေ့ရှိခဲ့ပါတယ်။ သူအတွေးအခေါ်က ခဏခဏ လက်ဆေးနေရတာ ကသီတယ်လို့ခံစားနေရတဲ့ ဆရာဝန်များကို အဆင်ပြေစေသည့်အပြင်၊ ထိုအချိန်ကလက်ခံထားခဲ့သည့် ရောဂါပိုးမွှားဆိုင်ရာသိပ္ပံသဘောပညာနည်းကျ အစဉ်အလာများကိုလည်း ဆန့်ကျင်ပြီးသက်သေပြခဲ့ပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Hacker တစ်ယောက်ကကွန်ပြူတာထဲချိုးဖောက်ဝင်ရောက်ပြီးအခြားသူများရဲ့အချက်အလက်တွေကိုလွှဲယူနိုင် တယ်၊ ခင်ဗျားမသိလိုက် ပဲ email တွေကိုဖတ်နိုင်တယ်၊ခင် ဗျာ း webcam ကိုကြည့်နိုင်တယ်ခင်ဗျားကိုမြင်နိုင်တယ်၊ ခင်ဗျားပြောတာတွေကြားနိုင်တယ်လို့ ခင်ဗျားထင်နေမှာပါ၊ ဤအချက်တွေက မမှန်တာတော့မဟုတ်ပါဘူး။ တချို့ Hackerတွေက ကွန်ယက်လုံခြုံရေးကို၊ စိန်ခေါ်မှုတစ်ခုလို့ မြင်တတ်တာကြောင့်၊ စနစ်တွေကို အရှုံးလုပ်ရန် လေ့လာကြတယ်၊ ဒါပေမယ့် သူတို့တကယ်လုပ်ဖို့ကြိုးစားနေတာက ကွန်ယက်ပုံစံချသူ၊ ကွန်ယက်စနစ် တည်ဆောက်သူတွေ မတွေးမိတဲ့အချက်တွေကိုစဉ်းစားတွေ့ရှိဖို့ပဲဖြစ်ပါတယ်။ သူတို့တတ်နိုင်သမျှ ကွန်ယက် စနစ်နဲ့ပက်သက်ပြီး- ကွန်ယက်စနစ်ကညွှန်ကြားမှုကိုဘယ်ကရတာလဲ၊ဘယ်လိုပေါ်လစီတွေသုံးထားလဲ၊ OS တွေ နဲ့ဘယ်လိုဆက်သွယ်လဲ၊ ထိုပတ်ဝန်းကျင်မှာရှိတဲ့ အခြားစနစ်တွေ၊ ပြီးတော့ကွန်ယက်တွေကို အသုံးပြုနေတဲ့ လူတွေနဲ့စီမံကွပ်ကဲနေတဲ့ကွန်ယက်အုပ်ချုပ်ရေးမူးတွေစသဖြင့်ရှာဖွေမှတ်သားကြတယ်။ ထို့နောက်သူတို့ရရှိထား တဲ့အချက်အလက်တွေကိုသုံးပြုပြီး၊ ကွဲပြားတဲ့လမ်းကြောင်းတွေကနေ သူတို့လိုချင်တာကိုရယူကြတယ်။ ဤနည်းအားဖြင့် Hacking လုပ်ခြင်းက စနစ်ရဲ့နည်းပညာကိုပိုမိုလုံခြုံကောင်းမွန်အောင် မည်သို့လုပ်ဆောင် ရမည်ကိုနားလည်စေနိုင်ခြင်းဖြင့် ကောင်းကျိုးဖြစ်ထွန်းစေပါတယ်။ ကံမကောင်းစွာအချို့ Hacking ပြုလုပ်ခြင်းကို ဒုစရိုက်သမားများက၊ တရားမဝင်ရည်ရွယ်ချက်၊ ဖျက်ဆီးနှောက်ယှက်ရန် ရည်ရွယ်ချက်တွေနဲ့ တလွဲအသုံးပြု ကြပြီး အဲဒီဒုစရိုက်သမားတွေက ခင်ဗျားဖတ်ရတဲ့ Media တွေကဖော်ပြတဲ့ hacker ဆိုသူတွေပါပဲ။ Hacker တစ်ယောက်ဆိုတာ လူမှုကွန်ယက်စာမျက်နှာတစ်ခုကို တစ်စုံတစ်ယောက်ကဖွင့်ထားခဲ့လို့ ၎င်းအကောင့် မှာ စာတွေတက်ရေးတာ၊ Password ရိုက်နေသူနောက်မှကျော်ကြည့်ခြင်း **(sholder-surfs)** လုပ်ပြီးသူတို့ အကောင့်ကို ယူသုံးတာမျိုးလုပ်သူမဟုတ်ပါဘူး။ script kiddie tools တွေ အင်တာနက်ကရယူပြီး သူများ email ကိုဖျက်လိုဖျက်ဆီး လုပ်သူတွေကလဲ Hacker မဟုတ်ပါဘူး၊ hacking လို့လဲ မခေါ်ထိုက်ပါဘူး၊ ထိုသို့ ပြုမူ သူတွေက အမှန်တကယ် လူရမ်းကားများ၊ သူခိုးများသာ ဖြစ်ပါတယ်။

> Hacking ဆိုတာ စူးစမ်းလေ့လာခြင်းတစ်ခုပါ။ တစ်ခုခုကို မူလပုံမှန်ထက်ခြားနားသောနည်းများသုံးပြီး ခင်ဗျား လိုခြင်တာဖြစ်ဖို့ ထပ်ခါထပ်ခါကြိုးစားဖူးပါသလား? စက်ပစ္စည်းတစ်ခုခုကို ဖွင့်ပြီးဘယ်လိုအလုပ်လုပ်တယ် ဆိုတာကြည့်ဖူးပါသလား? ၎င်းစက်ပစ္စည်းကိုပြောင်းလဲကြည့်ပြီး၊ မူလနှင့်မည်သို့ကွာခြားသွားတယ်ဆိုတာ စမ်းသပ်ဖူးပါသလား? ထိုသို့ပြုလုပ်ခြင်းများကို Hacking လို့ခေါ်ပါတယ်။ ခင်ဗျားလိုချင်တဲ့အရာ တစ်ခုခုရဖို့ အရာတစ်ခုခုကို စူးစူးနစ်နစ် စမ်းသပ်စစ်ဆေးပြီး ပြန်လည်ဆန်းသစ်ခြင်း၊ ထိန်းချုပ်ခြင်းများကို Hacking လို့ခေါ်ပါတယ်။

အင်တာနက်ဆိုတာများစွာသော application များ၊ စနစ်သုံးပစ္စည်းများ၊ ဆောင်ရွက်ပုံအဆင့်များနှင့် ဖွဲ့စည်းတည် ဆောက်ထားပြီး၊ Hacker များကိုတွေ့နိုင်တဲ့နေရာဖြစ်ပါတယ်။ အင်တာနက်ကို Hacker များကတည် ထောင် ခဲ့တာလို့ပြောနိုင်ပါတယ်၊ ၎င်းတို့ရဲ့အကောင်းဆုံးကစားကွင်းတစ်ခုလဲဖြစ်ပါတယ်။ ဒါပေမယ့် အင်တာနက် တစ်ခုပဲမဟုတ်ပါဘူး၊ အခြားနယ်ပယ်များမှာလဲ Hacker တွေကိုတွေ့နိုင်ပါတယ်။ မည်သို့ဖြစ်စေ Hacker များမှာ တူညီတဲ့အချက်တစ်ခုထဲရှိပါတယ်၊ အဲဒါကတော့ အရာဝတ္ထုတွေကိုနည်းလမ်းသစ်တစ်ခုနဲ့ပြန်လည်ဖန်တီးခြင်း ဖြစ်ပါတယ်။ သူတို့က အရာဝတ္ထုတစ်ခုကို မူလပုံစံအတိုင်းမကြည့်ပဲ မူလထက် ပိုကောင်းသော ကြီးကျယ်သော ဖြစ်နိုင်ချေတွေနဲ့ကြည့်မြင်တတ်ပြီး အခြားနည်းလမ်းသစ်တစ်ခုအနေနဲ့ ပြောင်းလဲအသုံးပြုတတ်ပါတယ်။

> ခင်ဗျားကိုယ်ခင် ဗျာ း ထူးချွန် တဲ့ Hacker ဖြစ်လာနိုင်မယ်လို့ မတွေးပါနဲ့၊ အလွန်နှိမ့်ချ၍လေ့လာခြင်း နဲ့ ထက်မြက် တဲ့ Hacking လုပ်ဆောင်နိုင်မှသာ ဖြစ်လာနိုင်မှာပါ။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Hacking ဆိုတာ တရားမဝင် တဲ့လုပ်ရပ်မဟုတ်ပါဘူး။ တစ်စုံတစ်ယောက်ကို နာကျင်စေရန်ရည်ရွယ်ပြီး ကျောက်ခဲနဲ့ပေါက်ခြင်းကသာ တရားမဝင်လုပ်ရပ်ဖြစ်ပါတယ်။ အကယ်၍ မရည်ရွယ်ဘဲ တစ်စုံတစ်ယောက်ကို နာကျင်စေတယ်ဆိုရင် အဲဒီလုပ်ရပ်ကပြစ်မှုတစ်ခုမဟုတ်သော်လည်း ခင်ဗျားကတာဝန်ယူဖြေရှင်းသင့်သမျှ လျော်ကြေး ပေးဖို့တော့လိုပါတယ်။ လူတွေရဲ့ပိုင်ဆိုင်မှုတွေ့ မတော်တဆ ပျက်ဆီးဆုံးရှုံးမှုတွေက အတွေ့အကြုံနဲသေးသော hacker များကြောင့် အများဆုံးဖြစ်ရတယ်ဆိုတာကို ISECOM ၏ **Hacker Profiling** စီမံကိန်းမှ လေ့လာတွေ့ ရှိထားပါတယ်။ ဤအချက်က လမ်းပေါ်မှာအပျော်သဘောနဲ့ ခဲလုံးနဲ့ပစ်ပေါက်ကစားရာမှ ကားများမှန်ကွဲခြင်း၊ထိခိုက်ပွန်းပဲ့ခြင်းများ၊ မတော်တဆဖြစ်ပွားခြင်းနှင့် တူညီပါတယ်။ အဲဒီပျက်ဆီးမှုက မတော်တဆပါ ဒါပေမယ့် လျော်ကြေးတော့ပေးရမှာပါ။ ထို့ကြောင့် ခင်ဗျားပိုင်ပစ္စည်းကိုဖြစ်စေ၊ တပါးသူပိုင် အရာများကိုဖြစ်စေ၊ Hacking လုပ်တဲ့အခါ အထူးသတိထားပြုလုပ်ရန် လိုအပ်ပါတယ်။

ခင်ဗျားပိုင်အရာကို ခင်ဗျား hacking ပြုလုပ်ခြင်းကလဲ၊တရားမဝင်ဖြစ်နိုင်ပါတယ်။ မိမိပိုင် အရာဝတ္ထုသာထု ကို hacking လုပ်သောကြောင့် အရေးယူခံရတဲ့ hacker များ၊ မိမိဝယ်ယူထားသော သီချင်း၊ ပရိုဂရမ်၊ ရုပ်ရှင်များကို hacking လုပ်ခြင်းကြောင့်အရေးယူခံရတဲ့ hacker များလည်းရှိပါတယ်။ ပုံမှန်အားဖြင့် ခင်ဗျားကိုယ်ပိုင်ဝယ်ယူထားသော ပရိုဂရမ်တစ်ခုကို ခင်ဗျားတစ်ကိုယ်စာသုံးရန် အစမ်းသဘောဖြင့်တောင် hacking ပြုလုပ်ခွင့် မရှိပါဘူး။ အဘယ်ကြောင့်ဆိုသော် ခင်ဗျားတရားဝင်ဝယ် တဲ့ ပစ္စည်းအများစုက၊ ဝယ်ယူသူ လိုင်စင် သဘောတူညီချက်စာချုပ် (ELUA – End user License Agreement) ပါဝင်ပြီး၊ ၎င်းလိုင်စင်တွင် ခင်ဗျားထိုသို့လုပ်ခွင့်မရှိကြောင်း ပါဝင်ပါတယ်။ ခင်ဗျားအဲဒီ ဆော့ဖ်ဝဲ ကို install လုပ်စဉ်ကလဲ လိုင်စင်ကိုခင်ဗျား ဖတ်သည်ဖြစ်စေ မဖတ်သည်ဖြစ်စေသဘောတူထားပြီး ဖြစ်ပါတယ်။ ခင်ဗျားအိမ်မှာ၊ ခင်ဗျားဝယ်ယူထားသော အရာများကို၊ ခင်ဗျား hacking စွမ်းရည်လေ့ကျင့်မှုများပြုလုပ်နေချိန်တွင် အထက်ဖေါ်ပြချက်ကို သိမှတ်ထား ပေးပါ။

Why Be a Hacker? ဘာကြောင့် Hacker ဖြစ်သလဲ?

သိပသိပံပညာရှင်တွေက လူသားမျိုးဗီဇကို ဘယ်လိုပုံဖေါ်ခဲ့ကြလဲဆိုတာ၊ စဉ်းစားကြည့်မယ်ဆိုရင်၊ သူတို့တွေက၊ ဂုဏ်စာဖေါ်ခြင်းနည်းလမ်းကို အသုံးပြုခဲ့တာတွေ့နိုင်ပါတယ်။ Password တွေကိုသတင်းအချက်အလက် (သို့) စာလုံးတွေကို code တွေအဖြစ်ပြောင်းလဲခြင်းစနစ် (Encryption) ပုံစံဖြင့်သိမ်းဆည်းထားလို့ ရယူရန် ခက်ခဲပါတယ်။ Brute-forcing နည်းလမ်းက password များ၏ encrypted ပုံစံကိုဖျက်ပြီး စာလုံးအနည်း ငယ် ကို အချိန်တစ်ခုအတွင်းမှ ၁ ဖြေရှင်းပါတယ်၊ ထို့နောက်ဂင်းအစိတ်အပိုင်းများကိုပြန်လည်သီတန်းထားပါ တယ်။ လူသားမျိုးဗီဇလေ့လာသူများက အခြေခံအချက်၃.၃သန်းရှိတဲ့ မျိုးဗီဇကို ပုံဖေါ်ရန် ထိုနည်းလမ်းကို အသုံးပြုကြပါတယ်။

မီးဖိုခန်းအတွင်း စားဖိုမှူးများကနိုက်ထရိုဂျင်အရည်ကိုအအေးပေးပစ္စည်းအနေဖြင့် ရေခဲမုန့်ကိုကောင်းမွန်စွာအေးခဲ စေရန်အသုံးပြုခြင်း၊ အာလူးချဉ်နှင့်ခရမ်းချဉ်သီးကြော် လုပ်ခြင်းကဲ့သို့ တီထွင်ဆန်းသစ်မှုများဖြင့် Hacking ကို ထုတ်ဖေါ်ပြသနိုင်တယ်။ ဓါတုဗေဒပညာရှင်တွေက ဒြပ်ဆင်တွေဒြပ်ပေါင်းတွေကို ရာစုနှစ်များစွာထဲက Hacking လုပ်နေခဲ့ကြပါတယ်။ ဓါတုဗေဒပညာရှင်တွေကသဘာဝဒြပ်စင်တွေ၊ဒြပ်ပေါင်းတွေကို ရာစုနှစ်များစွာစမ်းသပ် ဖေါ်ထုတ်နေခဲ့ကြတယ်။ သဘာဝမော်လီကျူးများထိခိုက်လွယ်ခြင်းအရ (ပူခြင်း၊အေးခြင်း၊တောင်ကုန်းများပေါ်၊ပင်လယ်ရေအောက်) စသည့်ပတ်ဝန်းကျင် ရာသီဥတုအပြောင်းအလဲများပေါ်တွင်ငင်းတို့မည်သို့တုန့်ပြန်သလ ဆိုတာကို စမ်းသပ်ထုတ်ဖေါ်ကြတဲ့အတွက်၊ ဓါတုဗေဒပညာရှင်များသည် သူတို့မှာရှိတဲ့ဓါတုဗေဒပစ္စည်းများ ပါဝင်ပေါင်းစပ်မှုများ ကိုနက်နက်နဲနဲနားလည်ဖို့ လိုပါတယ်။ ဆေးဝါးသစ် တီထွင်မှုထက် မြင်သာသောနေရာ မရှိပါဘူး။ ထိုဆေးဝါးသစ်ထုတ်လုပ်မှုတွင် ဒေသတစ်ခု၏ ရာချိသော အပင်မျိုးစိပ်တို့ကို အမြစ်မှအဖျား အသီးအပွင့်များ

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

အထိလေ့လာပြီး ခွဲထုတ်ခြင်း တစ်ခုနှင့်တစ်ခု ပေါင်းစပ်ခြင်းများပြုလုပ်၍ စမ်းသပ်ကြပါတယ်။ မှန်ကန်တဲ့ပေါင်းစပ်မှုရဖို့ကြိုးစားထုတ်ဖေါ်ကြပြီး တစ်ခါတစ်ရံ နှစ်များစွာကြာမြင့်တတ်ပါတယ်။

ဖောက်သည်များ၏ တိကျသော ဂယ်ယူမှုပုံစံ (သို့) စျေးကွက်တစ်ခုကိုနားလည်ရန်၊ စီးပွားရေးနယ်ပယ်များတွင် Hacking ပြုလုပ်ကြပါတယ်။ ၎င်းတို့နှင့် ဆက်နွယ်နေသောစီးပွားရေးနယ်ပယ်ကို လွှမ်းမိုးဖို့၊ ပြောင်းလဲဖို့ရည်ရွယ်ပြီး နက်နက်ရှိုင်းရှိုင်းတူးဆွလေ့လာကြပါတယ်။ တစ်ခါတစ်ရံ သူတို့ထုတ်ကုန်တွေအပေါ်မှာ Hacking လုပ်ကြပြီး၊ တစ်ခါတစ်ရံ (ကြော်ငြာများ၊ အဓိကထားမှု social engineering သင်ခန်းစာမှာ လေ့လာရမည့်အပိုင်း) ကိုသုံးပြီး ခင်ဗျားကို Hacking လုပ်ကြပါတယ်။

Hacking သည် စစ်ပွဲတစ်ခု၏ အရေးကြီးသော၊ ကျပ်တည်းသော အပိုင်းတစ်ခုလဲဖြစ်လာပါတယ်။ ကျွမ်းကျင်သော တပ်သားတွေက (ဘယ် Hacker တွေကကုဒ်ဖောက်တဲ့သူတွေ၊ ဉာဏ်ရည်စီစစ်သူတွေ၊ နယ်ပယ်အရာရှိတွေက ဘာတွေသုံးတယ် ဆိုတာတွေ နဲ့ ရန်သူဖက်မှာဘာတွေရှိတယ်၊ ဘာတွေလုပ်နေတယ်၊ သူတို့ အသုံးပြုသော ပစ္စည်းကရိယာများ၏အားနည်းချက်တွေအပေါ် ဘယ်လိုအသာစီးရယူရန် ဘယ်လိုအခြေခံ Hacking စွမ်းရည်တွေ ရှိတယ်ဆိုတာတွေ စတဲ့..) သူတို့ပစ်မှတ်၊ ပန်းတိုင်ရောက်ရန် တီထွင်နိုင်စွမ်းအားပြည့်သူတွေဖြစ်ပါတယ်။ နိုင်ငံ တော်တော်များများ က ကွန်ပြူတာနှင့်ကွန်ပြူတာ ကွန်ယက်အပေါ်မှီခိုနေကြတဲ့အတွက်၊ ဆိုက် ဘာ တိုက်ခိုက်မှု နှင့် ကာကွယ်မှု ဆိုတဲ့အချက် က နိုင်ငံ ကြည်းရေလေ တပ်မတော်နှင့် ရန်သူသတင်းထောက်လှမ်းရေ စစ်ဆင်ရေး များအတွက်တန်ဖိုးကြီးတဲ့ အပိုင်းဖြစ်လာပါတယ်။

> Hacker တစ်ယောက်ဖြစ်လာဖို့ အကြောင်းပြချက်ကတော့ ထိုသို့ဖြစ်ခြင်းကတကယ်စွမ်းအားကြီးမားလို့ပဲဖြစ်ပါတယ်။ အကယ်၍ ခင်ဗျားမှာ တကယ်အားကောင်းတဲ့ Hacking စွမ်းအားရှိတယ်ဆိုရင် တကယ်ကောင်းမွန်တဲ့ အရာတွေခင်ဗျားလုပ်နိုင်ပါလိမ့်မယ်။ လေးနက်တဲ့ဗဟုသုတတိုင်းက ခင်ဗျားကိုကြီးမားတဲ့ စွမ်းအားပေးနိုင်ပါတယ်။ အရာဂတသဃထုတစ ် ခု ဘယ်လိုအလုပ်လုပ်နေတယ်ဆိုတာ ခင်ဗျားသိရင်အဲဒီအရာကိုခင် ဗျ ာ း ထိန်းချုပ်နိုင်မှာသေချာပါတယ်။ ခင်ဗျားလက်ထဲမှာ တကယ်စွမ်းအားရှိနေသလို၊ ခင်ဗျားကိုယ်တိုင် နဲ့ ခင ဗျား အလေးထားတဲ့ အရာတွေကိုကာကွယ်ဖို့ စွမ်းအားတွေ ရလာပါလိမ့်မယ်။

လူတွေက အလုပ်ရှာခြင်း၊ ပိုက်ဆံရှာခြင်း၊ လုပ်ငန်းလုပ်ခြင်းများကိုပြုလုပ်ရန် အင်တာနက်ကိုငင်းတို့ဆွေမျိုး ကဲ့သို့ ဆက်သွယ်ပြီး လူအများစုရဲ့အသက်တမျှအရေးပါနေပါတယ်။ သတင်းအချက်အလက်တွေက အဖိုးတန်သလို၊ ခြိမ်းခြောက်ခံရခြင်းလဲရှိနိုင်ပါတယ်၊ hacker တွေကတော့ ၎င်းတို့၏သတင်းအချက်အလက်တွေကို တခြားသူတွေထက်ပိုကာကွယ်နိုင်ပါတယ်။ သူတို့လိုချင်တဲ့ အချက်ကိုသာရွေးချယ်ဖေါ်ထုတ်ပြီး၊ ပိုမိုလုံခြုံအောင်ထိန်းသိမ်းနိုင်ပါတယ်။ အသေးငယ်ဆုံးအဆိုးမြင်အသိတရားတွေက အဆုံးမှာခင်ဗျားကိုဟန့်တားဆန့်ကျင် နိုင်တာကြောင့် ကျောင်းမှာဖြစ်ဖြစ်၊ ဘဝအတွက်ဖြစ်ဖြစ် ဤအချက်က ကြီးမားတဲ့ ယှဉ်ပြိုင်နိုင်သောအရေးသာမှုတစ်ခုဖြစ်ပါတယ်။

> ***မည်သည့်အရာကိုမဆို Hack ပါ။ နစ်နာထိခိုက်မှုတော့ မရှိပါစေနဲ့။***

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

How to Hack (ဘယ်လို Hack မလဲ)

ခင်ဗျားကိုဘယ်လို Hack ရမယ်ဆိုတာပြောပြရတာ၊ ဘားတန်းပေါ်မှာဘယ်လို နောက်ဂျမ်းပစ်ရမယ်ဆိုတာရှင်းပြ နေရသလိုပါပဲ။ ရှင်းပြချက်တွေဘယ်လောက်အသေးစိတ်ကျတယ်ဆိုတာထက်ပထမဆုံးအကြိမ်မှာတော့ ခင်ဗျား ကိုယ်တိုင်လုပ်နိုင်မှာမဟုတ်ဘူး။ ခင်ဗျားကျွမ်းကျင်မှုခံစားချက်၊ လေ့ကျင့်မှုတွေကြောင့် သိမြင်လာခြင်းစတဲ့ အချက်တွေကို မြှင့်တင်ဖို့လိုပါတယ် သို့မဟုတ်ပါက ခင်ဗျားမျက်နှာနဲ့ မှောက်လျက်လဲကျမှာပဲ။

ပထမဆုံးအနေနဲ့ Hacking တကယ်တမ်းဘယ်လိုအလုပ်လုပ်တယ်ဆိုတဲ့လျှို့ဝှက်ချက်နဲနဲ ခင်ဗျားသိဖို့လိုပါတယ်။ OSSTMM (www.osstmm.org) hacker တွေကတော့ "aw-stem" (ခြော်စတင်း(မ်း)) လို့အသံထွက် တယ်။ အဲဒီကနေလေ့လာကြည့်ကြစို့၊ OSSTMM က Open Source လုံခြုံရေး စမ်းသပ်မှု အညွှန်းပါ၊ ၎င်းကို DvD အသုံးပြုပုံ အညွှန်းကဲ့သို့ မြင်နိုင်တယ်၊ ၎င်းအညွှန်းက ကျွမ်းကျင် hacker တိုင်းလိုလို အစီအစဉ်ချရန်၊ အကောင် အထည်ဖော်ရန်စတဲ့ ရည်ရွယ်ချက်တွေနဲ့ အသုံးပြုတဲ့အဓိက မှတ်တမ်းတစ်ခုပါ။ ထိုအညွှန်း ရဲ့အတွင်းကျတဲ့ အပိုင်းတွေကခင်ဗျားမျက်လုံးတွေကို လင်းလက်စေမယ့် တကယ့်ရတနာတွေပါပဲ။

Two Ways to Get What You Want (အလိုရှိရာကို ရယူနိုင်တဲ့ နည်းနှစ်သွယ်)

ဥပမာအားဖြင့်၊ အရာရာကိုရယူနိုင်တဲ့ တကယ်နည်းလမ်း၂ခုပဲရှိတယ်ဆိုတာ ခင်ဗျားသိထားသင့်တယ်။ ကိုယ်တိုင် ရယူမယ်၊ ခင်ဗျားဆီမှာထိုအရာကိုယူပြီး ခင်ဗျားကိုပေးနိုင်တဲ့ သူတစ်ယောက်ရှိမယ် ဆိုတဲ့နည်းတွေပါပဲ။ အရာရာကိုရယူခြင်းမှာ ရယူမယ့်သူ နှင့် ရယူခံရမယ့်အရာဝတ္ထုကြားမှာ တုံ့ပြန် မှု (Interaction) လိုအပ်တယ် ဆိုတာသိသာပါတယ်။ ဒါပေမယ့်၊ သေချာတွေးကြည့်ရင် အဲဒီအချက်က၊ အာကာအကွယ်လုပ်မယ့်ယန္တရားတွေက ၎င်းတို့ကာကွယ်ထားတဲ့အရာဝတ္ထုနဲ့ တစ်စုံတစ်ယောက်ကြားကတုံ့ပြန်မှုကို တားဆီးဖို့တာဝန်ရှိပါတယ်။ ခင်ဗျားက အရာအားလုံးကိုအခန်းထဲထည့်မပိတ်ထားပဲနဲ့တော့ တုံ့ပြန် မှု (interaction) အားလုံးကို မတားဆီးနိုင်ပါ ဘူး။ စီးပွားရေးလုပ်ငန်းတိုင်းက email server တွေနဲ့ချိတ်ဆက်ထားတဲ့၊ email client တွေကို အသုံးပြုပြီး သတင်း အချက်အလက်တွေ ပေးပို့ဖို့၊ရယူဖို့ လိုအပ်ပါတယ်။ အဲဒါတွေက၊ တုံ့ပြန်မှုတွေကိုဖြစ်စေလျက်ရှိပါတယ်။

ရင်းနှီးပြီးသားလူတွေနဲ့ စနစ်တွေကြားက အချို့တုံ့ပြန်မှုတွေကို ယုံကြည်မှု(Trusts) လို့ခေါ်ပြီး၊ အကျွမ်းတဝင်မရှိ သော လူနဲ့စနစ်ကြားကတုံ့ပြန်မှုတွေကို အသုံးပြုခွင့် (Accesses) လို့ခေါ်ပါတယ်။ ခင်ဗျားလိုချင်တဲ့ အရာကိုရယူဖို့၊ ခင်ဗျားကိုယ်တိုင် Access တစ်နည်းကိုသုံးပြီး ရယူခြင်း (သို့) ပစ်မှတ်နဲ့ Trust ရှိပြီးသားလူတစ်ယောက်ကို ခင်ဗျား အတွက်ယူလာပေးရန် လှည့်စားနိုင်ပါတယ်။ နဲနဲလောက်ထပ်စဉ်းစားကြည့်ရင်၊ လုံခြုံရေးစနစ်ဆိုတာ အရာဝတ္ထုတစ်ခုကို ယုံကြည်ရသူ၊ မယုံကြည်ရသူ နှစ်မျိုးစလုံးဇ၏ရန် မှ ကာကွယ်ဖို့လိုတယ်ဆိုတာ မြင်သာပါတယ်။

Exercises (လေ့ကျင်ခန်းများ)

1.1 search engine တစ်ခုက ဘယ်လို (interaction) တုံ့ပြန်မှုကိုအသုံးပြုပါသလဲ? သေချာစဉ်းစားပါ။ ။ အားလုံးက Access ပေးထားလား ၊ Trust ပေးထားလား?

1.2 စက်ဘီးရပ်နားတန်းမှာ သော့ခတ်ထားတဲ့စက်ဘီးတစ်စီးကိုရယူရန်အတွက် Access နှင့် Trust အသုံးပြု ပုံကို ရိုးရှင်းသော ဥပမာတစ်ခုနဲ့ရှင်းလင်းဖေါ်ပြပါ။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

1.3 အခြားသူတစ်ဦး၏ web-mail အကောင့်ကို ဝင်ရောက်ရန် Access နှင့် Trust ကိုမည်သို့အသုံးပြုနိုင်တယ်ဆိုတာ ရိုးရှင်းသောဥပမာတစ်ခုပေးသဿ၍ ရှင်းလင်းဖော်ပြပါ။

Feed Your Head: Espionage (သူလျှိုလုပ်ခြင်း)

ပြည်ပအစိုးရကိုယှဉ်၍ စစ်ရေးစစ်ရာ (သို့) နိုင်ငံရေးအရေးသာမှုရရန် ကျူးကျော်ဝင်ရောက်ခြင်း၊ခိုးဝှက်ခြင်း၊ ဖျက်စီးတိုက်ခိုက်ခြင်း စတဲ့ဒုစရိုက်အပြုအမူတွေပြုလုပ်ခြင်းမျ ာ Hacking ကိုအသုံးပြုတယ်ဆိုရင် **သူလျှိုလုပ်ခြင်း (espionage)** လို့ခေါ်ပါတယ်။ မတူညီသော နိုင်ငံများကြားမှာစီးပွားရေး အရေးသာမှုရရန်အသုံးပြုခြင်းကို **စီးပွားရေးသူလျှိုလုပ်ခြင်း(economic espionage)** လို့ခေါ်ပါတယ်။

လူတစ်ဦးတစ်ယောက်၏ အတွင်းရေး၊ ကိုယ်ရေးကိုယ်တာကို လူသိရှင်ကြားအရှက်ရစေရန် ရည်ရွယ်ရယူခြင်းတွင် Hacking ကိုအသုံးပြုခြင်းကို **Doxing** လို့ခေါ်ပါတယ်။ အကယ်၍ ဒုစရိုက်ပြုခြင်းတွေမပြုလုပ်ပဲ လူတစ်ဦး၊ ကုမ္ပဏီတစ်ခုအ ာ း တိုက်ခိုက်ရန်အများသိသတင်းအချက်အလက်များကိုသာအသုံးပြုခြင်းကို **Document Grinding** (သို့) **OSInt (Open Source Intelligence)** ဟုခေါ်ပါတယ်။

ကုမ္ပဏီတစ်ခု၏ ကွန်ယက်စနစ်၊အသုံးပြုသောဆော့ဖ်ဝဲ၊စက်ပစ္စည်း များကို သိရှိနားလည်ရန်လက်တွေ့ ကျူးကျော်ခြင်းမပြုလုပ်ပဲ Hacking လုပ်ခြင်းကို **(network surveying)** ဟုခေါ်ပါတယ်။

ရိုင်းပြေသော်လည်း ဥပဒေဘောင်အတွင်းမှနေ၍ ပြိုင်ဖက်များ၏ အခြေအနေကို သိရှိနိုင်ရန် Hacking လုပ်ခြင်းကို **(Competitive Intelligence)** ဟုခေါ်ပါတယ်။

ဘယ်လိုရိုင်းစိုင်းယုတ်မာမှုတွေကများတရားဝင်နေတာလဲလို့ ခင်ဗျားသေလောက်အောင် သိချင်နေပါလိမ့်မယ်။ သတင်းအချက်အလက်တွေရဖို့တစ်စုံတစ်ယောက်ကိုစိတ်ဖိစီးမှုပေးခြင်းကဲ့သို့ ဥပမာတစ်ခုလောက်စဉ်းစားကြည့်ပါ၊ ခင်ဗျားကတစ်ယောက်ယောက်ကို မသတ်မိသ၍ ခင်ဗျားလိမ်လည်ပြောနေတာတွေကတရားဝင်နေတုန်းပါပဲ (ရုပ်ရှင်ရုံနဲ့ လူများတဲ့နေရာတွေမှာ၊ "မီးပျို" လို့လိမ်ပြီးတော့ မအော်မိစေနဲ့ပေါ့)။

ကုမ္ပဏီတစ်ခုရဲ့စက်ရုံသစ်ကို ဘယ်မှာတည်ဖို့ စီစဉ်နေလဲဆိုတ ာ Hacker ကသိချင်နေတယ်လို့ဆိုပါစို့။ Hacker က document grinding ကိုသုံးပြီး ဘယ်သူကအဲဒီဆုံးဖြတ်ချက်ကိုချလဲ ဆိုတာရှာဖွေမှာပါ။ ထို့နောက် Hacker ကသူတို့ရုံးကိုဆက်သွယ်ပြီး သူတို့သွားခဲ့တဲ့နေရာတွေ၊ရောက်ခဲ့တဲ့မြို့တွေကို စုံစမ်း မေးမြန်းပါလိမ့်မယ်။ သူတို့ရဲ့ ပုဂ္ဂိုလ်ရေးရာဇဝင်ရာအကြောင်းတွေကိုတိုက်ရိုက်သွားမေးလို့တော့မရနိုင်ပါဘူ း ဒါကြောင့် Hacker က အနည်းငယ်လှည့်စားပြီးမေးမြန်းဖို့တော့လိုပါလိမ့်မယ်။ သိပ်ခက်တဲ့အရာတော့ မဟုတ်ပါဘူး။ ဥပမာလေးဖတ်ကြည့်ပါ။ ။

> Hacker: ဟိုင်း၊ ကျွန်တော်က ဒေါက်တာ Jones ပါ၊ ခင်ဗျားသမီး Nancy အကြောင်းပြောချင်လို့ ကျောင်းကနေဆက်နေတာပါ။
>
> Target: ဟုတ်ကဲ့၊ ကျွန်တော့်သမီးဘာများဖြစ်လို့ပါသလဲခင်ဗျာ?
>
> Hacker: ကောင်းပြီ၊ သူမက အခုနာခေါင်းသွေးယိုတာ ဆက်တိုက်ဖြစ်နေတယ်၊ ကျွန်တော်တို့ရပ်လို့မရဘူးဖြစ်နေတယ်။ ကျွန်တော်သိချင်တာက သူမက ဓါတုဗေဒဆေးဝါးတွေနဲ့ထိတွေ့ဖူးသလား၊ ဒါမှမဟုတ် အဲဒီလိုစက်ရုံတစ်ခုခုကိုသွားခဲ့ဖူးသလား? အခုဖြစ်နေတဲ့ရောဂါလကဏာက ဓါတုဗေဒဆေးဝါးတွေနဲ့ထိတွေဖူးတဲ့သူတွေက လွဲရင် အဖြစ်နည်းတဲ့လကဏာဖြစ်နေတယ်။ ခင်ဗျားတစ်ခုခု ပြောပြနိုင်မလား?
>
> Target: (လျှို့ဝှက်ချက်တွေ ပွင့်ထွက်လာပါတယ်။)

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

> တရားမဝင်လုပ်ရပ်တော့မဟုတ်ပါဘူးဒါပေမယ့်မလိုအပ်တဲ့စိတ်ဖိစီးမှုတွေကိုဖြစ်ပေါ်စေပါတယ်။ မိဘတစ်ယောက်ကို ထိသိုစိတ်ပူအောင်လုပ်ဖို့မဆိုလိုပါဘူး။

Hacking to Take Over Your World (ခင်ဗျားကမဿဘာကိုရယူဖို့ Hacking လုပ်ခြင်း)

Hacking ဆိုတာကပဲ တုံ့ပြန်မှုကိစ္စသစ်ရပ်မဟုတ်ပါဘူး၊ တချို့လူတွေကတော့ နိုင်ငံရေးကတုံ့ပြန်မှုကိစ္စသစ်ရပ်ပါလို့ပြော ကြပါတယ်။ ဒါပေမယ့် တစ်ခါတစ်ရံမှာတော့ Hacking ဆိုတာ လုံခြုံရေးကိုချိုးဖျက်ဝင်ရောက်ခြင်းလို့ ခင်ဗျားထင် နေလိမ့်မယ်၊ တကယ်တမ်းမ ာ Hacking ဆိုတာတစ်ခုခုကို ထိမ်းချုပ်ခြင်းသာမက၊ ပြောင်းလဲခြင်းဖြစ်ပါတယ်။ ကျွန်တော်တို့ အခြေခံဆွေးနွေးခဲ့တဲ့ တုံ့ပြန်မှု (interaction) က ထိုးဖောက်ဝင်ရောက်ဖို့၊ စူးစမ်းရှာဖွေဖို့၊ (သို့) တီထွင်ဖို့ အသုံးဝင်ပါတယ်။ လွတ်လပ်မှုရအောင် တစ်စုံတစ်ခုကိုခင်ဗျားပိုင်ဖြစ်အောင် လုပ်မှာလား၊ တချို့တွေက လုံခြုံရေးလို့ခေါ်တ ဲ့ "ခင်ဗျာပိုင်အရ ာ တစ်ခုခုကို ၊ တစ်ယောက်ယောက်ကပြောင်းလဲခြင်းကိုတားဆီးဖို့လုပ်မှာလား?

> ခင်ဗျားပစ္စည်းတစ်ခုခုက ို ၊ ဝယ်တဲ့အခါ၊ ခင်ဗျားဝယ်တဲ့ကုမ္ပဏီကအဲဒီပစ္စည်းကို ပြင်ဆင်အသုံးပြုလို့မရအောင် တစ်နည်းနည်းနဲ့ထိမ်းချုပ်တားဆီးပါလိမ့်မယ်။ ခင်ဗျားအဲဒီပစ္စည်းကို ချိုးဖျက်မိရင် ကုမ္ပဏီကပြင်ဆင်ပေးခြင်း အသစ်လဲပေးခြင်း မလုပ်ပေးဘူးဆိုတာကိုသဘောတူထားရပါတယ်။ ထို့ကြောင့် ခင်ဗျားပိုင်အရာတစ်ခုကို Hack ခြင်းက အဲဒီအရာကို ယတိပြတ် ခင်ဗျားတကယ်ပိုင်ဆိုင်စေပါတယ်။ ထိုသို့လုပ်ခြင်းက စွန့်စားလွန်းရာ ရောက်နေရင်တောင် အခြားလူတွေကို ခင်ဗျားကိစ္စသစ်ရပ်တွေအား ပါဝင်စွက်ဖက်ခြင်းမှတားဆီးနိုင်ပါတယ်။

လူအားလုံး ကို ကျွန်တော်တို့ဆိုလိုတာကို သိနားလည်စေချင်တာက လုံခြုံရေးဆိုတာ သော့ခလောက် တစ်ခု၊ အချက်ပေ း စနစ်တစ်ခု၊ Firewall ဒါမှမဟုတ် သီအိုရီအရလုံခြုံအောင် လုပ်ပေးနိုင်တဲ့ ထုတ်ကုန်ပစ္စည်းတစ်ခုကို တစ်နေရာရာမ ာ ထားခြင်းဖြစ်တယ်။ ဒါပေမယ့်ငင်းလုံခြုံရေး ပစ္စည်းတွေကိုယ်တိုင်မှာလည်း အားနည်းချက်တွေ ရှိနေနိုင်ပါတယ်။ အဲဒီ အားနည်းချက်တွေကြောင့် Attack Surface (တစ်ခုခု၊တစ်ယောက်ယောက်ကို တိုက် ခိုက် မှု ပြုနိုင်တဲ့နည်းလမ်း၊ တုံ့ပြန်မှုအားလုံး) ကိုတိုးပွားစေနိုင်ပါတယ်။ ဘယ်ဈေးကွက် က ဝယ်တဲ့ပစ္စည်းပဲဖြစ်ဖြစ် ခင်ဗျားနဲ့အတူရှိနေမှာက ကံကောင်းခြင်းပါပဲ၊ ထို့ကြောင့် ၎င်းပစ္စည်းတွေမှာ ဘယ်နေရာကပျက်နေတယ်၊ အားနည်းနေတယ် ဆိုတာသိဖို့ ခင်ဗျားကိုယ်တိုင် Hacking လုပ်ကြည့်ရမှာပါ။ ပြီးတော့အဲဒီပစ္စည်းကို ဝယ်ခဲ့တဲ့ ကုမ္ပဏီကနေ မူလအတိုင်း ပြန်လည်မပြောင်း နိုင်အောင် ထပ် Hack ဖို့လိုနိုင်ပါတယ်။

အဲဒါကြောင့် hacking ဆိုတာလုံခြုံရေးကို ချိုးဖောက်တဲ့အရာလို့တွေးမိတိုင်း ထိုနေရာအတွက် Hacking လုပ်ခြင်းကို အသုံးပြုတယ်ဆိုတာသတိရပါ၊ အဘယ်ကြောင့်ဆိုသော် အဲဒီချိုးဖောက်ခြင်းမလုပ်ရင်ခင်ဗျား နှစ်သက်တဲ့ လွတ်လပ်ခြင်း၊ လုံခြုံစိတ်ချရမှုတွေကို စွန့်လွှတ်ရလိမ့်မယ်။ (ခင်ဗျားအခုချက်ခြင်းတော့ အင်တာနက်ပေါ်မှာ ခင်ဗျား လုပ်တဲ့၊ ပြောတဲ့၊ တင်တဲ့ အရာတွေကိုဂရုပြုမိမှာမဟုတ်ပါဘူး ဒါပေမယ့် အင်တာနက် ကတော့ ခင်ဗျားရဲ့ နောက်ကြောင်းတွေကိုပြန်ခေါ်ပေးနိုင်တဲ့၊ ရှည်လျားကျယ်ပြန့်တဲ့ မှတ်ဉာဏ်တွေရှိပါတယ်။ ကွန်ယက်ပေါ် ရောက်သွားတဲ့အရာတွေက ကွန်ယက်ပေါ်မှာပဲအစဉ်ရှိနေမှာပါ။ ထို့ကြောင့် ဒီနေ့အချိန်က "ခင်ဗျား" က ဂရုမစိုက်ရင်တောင် အနာဂါတ်က "ခင်ဗျား" အတွက် စဉ်းစားချင့်ချိန်ကြည့်ပေးသင့်ပါတယ်။)

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

အခုဆိုရင် ခင်ဗျားက တုံ့ပြန်မှု Interaction အကြောင်းကိုတော်တော်လေးနားလည်နေပါပြီ၊ အနည်းငယ် ထပ်ပြီး အသေးစိတ်လေ့လာကြည့်ရအောင်။ အခြေခံ တုံ့ပြန်မှုနှစ်ခုကတော့ Access နှင့် Trust တွေဆိုတာ ခင်ဗျားသိပြီးဖြစ်ပါတယ်၊ ဒါပေမယ့် တွေ့မြင်နိုင်ခြင်း(Visibility) ဆိုတာကြားဖူးပါသလား? ရှေ့ကနှစ်ခုလိုပဲ စွမ်းအားပြည့်တဲ့ တတိယ တုံ့ပြန်မှု Interaction အမျိုးအစားပါ။ ရဲတွေအတွက်ကတော့ အခွင့်အရေးတစ်ခုလို ရိုးရှင်းပါတယ်။ ဒါပေမယ့် hacking အတွက်တော့ တုံ့ပြန်မှုပြည့်တစ်ခုခု ရှိတယ်၊မရှိဘူး သိနိုင်ခြင်းက ပိုအရေးပါပါတယ်။ အဲဒီ တုံ့ပြန်မှု interaction က လှည့်စားမှု (deception)၊ ပုံရိပ် (illusion)၊ camouflage (ကိုယ်ရောင်ဖျောက်ခြင်း) စတဲ့ လုံခြုံရေးနည်းပညာသစ်တွေယူဆောင်လာခြင်းသာမက၊ အဲဒီ လုံခြုံရေးနည်းပညာသစ်တွေကို ဘယ်လိုရှောင်ကျဉ်ရမယ်၊ ဘယ်လိုလုံခြုံရေးတိုင်းတာမှုတွေရယူရမလဲဆိုတဲ့ Hacking နည်းပညာသစ်တွေကိုပါ ယူဆောင်လာပါတယ်။

နာမည်ကြီးဘဏ်ခါးပြ Jesse Jame ကို "ဘာကြောင့် ဘဏ်ကိုခါးပြတိုက်ရသလဲ?" လို့မေးတဲ့ခါ "ပိုက်ဆံတွေရှိတဲ့နေရာ ဖြစ်နေလို့ပါ" လို့ပြောခဲ့ပါတယ်။ တွေ့မြင်နိုင်မှု (Visibility) ကြောင့်အဲဒီဘဏ်မှာ ပိုက်ဆံတွေရှိနေတယ်ဆိုတာသူသိခဲ့ပါတယ်။ လူတွေက အဲဒီဘဏ်မှာဘာတွေရှိနေလဲဆိုတာသိနိုင်ပါတယ်၊ ဒါပေမယ့် အရာရာမှာတော့ Visibility မရှိနိုင်ပါဘူး၊ visibility မရှိမှုကို privacy (သီးသန့်ရှိမှု)လို့ခေါ်ပါတယ်။ အနာသတရာယ်များတဲ့လမ်းပေါ်မှာ၊ တောထဲမှာ၊ Internet မှာ၊ ဘယ်မှာဖြစ်ဖြစ် ဖေါ်ထုတ်ပြသမှုကို နဲနိုင်သမျှနဲအောင် ထားခြင်း Visibility မဖြစ်ရန် ရှောင်ကျဉ်ခြင်းက ပထမဆုံးတိုက်ခိုက်ခံရမှုမှ ရှောင်ဖယ်နိုင်တဲ့ နည်းလမ်းတစ်ခုဖြစ်ပါတယ်။

Exercises

1.4 အင်တာနက်တွေက ပုံပြင်တွေ၊ ကြာရှည်တည်တံ့နေတဲ့ဇာတ်လမ်း အမှားတွေ ၊ လိမ်စဉ်တွေ လား အမှန်တွေလား ဆိုတာသိဖို့ ခက်ခဲတဲ့အကြောင်းအရာတွေဖန်တီးရန် ခေတ်အစားဆုံးနေရာတစ်ခုပါ။ ထို့ကြောင့် ခင်ဗျားက Hacker ကောင်းတစ်ယောက်ဖြစ်ရန် လေ့လာချင်တယ်ဆိုရင်၊ တကယ့်ဖြစ်ရပ်မှန်တွေကိုဆန်းစစ် လေ့လာတတ်တဲ့အကျင့်ကိုလေ့ကျင့်ပါ။ ထို့ကြောင့်အခု Jasse James ကအဲဒီစကားကိုတကယ်ပြောခဲ့တာလားဆိုတာရှာဖွေကြည့်ပါ။ ပြီးတော့ ပထမဆုံးတွေ့ရ ၁ web စာမျက်နှာကိုကြည့်ပြီးအဖြေကို လွယ်လွယ်မထုတ်ပါနဲ့ သေချာလေ့လာတူးဆွပါ။
အောက်ပါ အကြောင်းအရာတွေကိုဆက်လက်ရှာဖွေကြည့်ပါ။

1.5 Inuit ဘာသာစကားမှ ၁ igloo ဆိုတာဘာအဓိပ္ပာယ်ပါယ်လဲ၊ ဘယ်ကဆင်းသက်လာတာလဲ? အဲဒါကိုရှာဖို့ ခင်ဗျားဘယ် interaction ကိုသုံးခဲ့သလဲ?

1.6 မိဘတွေက သကြားဟာ ကလေးတွေကို တရားလွန်နိုးကြားတက်ကြွစေတယ်လို့ယုံကြည်ကြပါတယ် အဲဒါအမှန်ပဲလား? ကလေးတွေက သကြားနဲ့သကြားလုံးတွေများစွာစားတဲ့အခါ သူတို့ပမ်းဗိုက်ကြွက်သားတွေမှာဘယ်လိုတုံ့ပြန်မှုတွေအမှန်တကယ်ဖြစ်ပေါ်တာလဲ?

1.7 သကြားကြောင့် သွားတွေမှာခေါင်းပေါက်တွေဖြစ်စေတာ ခင်ဗျားကြားဖူးပါလိမ့်မယ် ဒါပေမယ့်ဘယ်လို တုံ့ပြန်မှုကြောင့်ထိုက်ခဲ့သို့ဖြစ်တာပါလဲ? တကယ် သကြားကြောင့်လား? အကယ်၍ သွားတိုက်ခြင်းက တကယ့်အကြောင်းတရားကိုတွန်းလှန်နိုင်တယ်လို့ ခင်ဗျားပြောမယ်ဆိုရင် အနည်းဆုံးဓါတုဆေးပါးတစ်မျိုး ၏ အမည်ကိုဖော်ပြပေးပါ။ (အရိပ်အမြွက်: : ဖလိုရိုက် ဆိုရင်မှားပါတယ်။)

The Four Point Process (ဖြစ်စဉ် လေးချက်)

ခင်ဗျားက တုံ့ပြန်မှု သုံးမျိုးစလုံးကိုအတူတကွ အသုံးပြုလိုက်တဲ့အခါ အခြေခံ Attack Surface ဖြစ်တဲ့ ယိုစိမ့်ပေါက် (porosity) ဖြစ်ပေါ်လာပါတယ်။ porosity ဖြစ်ခြင်းက ခင်ဗျားမှာရှိသင့်တဲ့ ခုခံမှုစနစ်တိုင်းမှာ လိုအပ်တဲ့ တုံ့ပြန်မှု

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

တွေဖြစ်ပေါ်စေတဲ့အပြင် အခြားမလိုအပ်သော တုံ့ပြန်မှုတွေကိုပါ ဖြစ်ပေါ်စေပါတယ်။ ဥပမာအားဖြင့် စတိုးဆိုင်တစ်ခုက ကုန်ပစ္စည်းတွေကို ရောင်းချရန်စင်များပေါ်တွင် တင်ထားဖို့လိုပါတယ် သို့မှသာ ဝယ်သူများက ၎င်းကုန်ပစ္စည်းများကို သူတို့စျေးဝယ်ခြင်းထဲထည့်ပြီး ဝယ်ယူနိုင်မှာဖြစ်ပါတယ်။ ဒါပေမယ့် အဲဒီကုန်ပစ္စည်းတွေကို အ ကျင့်ပျက်ဝန်ထမ်းတော့ (သို့) အပြင်လူတွေမှ ခိုးယူခြင်းကဲ့သို့ မလိုအပ်တဲ့ဖြစ်ရပ်တွေ တုံ့ပြန်မှုတွေ ကိုလည်းဖြစ် ပေါ်စေနိုင်ပါတယ်။

Porosity ဆိုတာ ခင်ဗျားကိုယ်တိုင်ကာကွယ် ဖို့ (သို့) အခြားသူကို တိုက်ခိုက်ဖို့ ခင်ဗျားသိထားသင့်တဲ့ အရာတစ်ခုဖြစ်ပါတယ်။ ဒါပေမယ့် လုံလောက်တဲ့လိုအပ်ချက် မဟုတ်သေးပါဘူး။ Hacking လုပ်ဖို့အတွက် လေ့လာခဲ့တဲ့ တုံ့ပြန်မှု သုံးမျိုးစလုံးကို ပိုပြီးအသေးစိတ်သိဖို့လိုပါတယ်။ ဒါကတော့ OSSTMM ရဲ့ ဖြစ်စဉ်လေးချက် (Four Point Process) [FPP] လို့ခေါ်တဲ့လှျိုဂ်ချက်တွေပါ။ ၎င်းလှျိုဂ်ချက်က အရာတစ်ခုကိုအသေးစိတ်လေ့လာတဲ့အခါ ခင်ဗျားသိထားတဲ့ တုံ့ပြန်မှု (Interaction) တွေကိုအဓိကအသုံးပြုခြင်းနည်းလမ်း လေးသွယ်ကိုဖေါ်ပြထားပါတယ်။

The Echo Process - ပဲ့တင်ဖြစ်စဉ်

ကျွန်တော်တို့က အရာဝတ္ထုတွေကို တိုက်ရိုက်တုံ့ပြန်စေခြင်းပြုလုပ်ပြီး လေ့လာတွေ့ရှိမှုကိုရှာဖွေကြပါတယ်။ ကလေးငယ်တစ်ယောက်က ခြောက်နေတဲ့ရှည်သေတစ်ကောင်ကို တုတ်ချောင်းနဲ့တိုကြည့်ပြီး သေမသေစမ်းသကဲ့သို့ပေါ့၊ ထိုသို့ပြုလုပ်ခြင်းကို ပဲ့တင်ဖြစ်စဉ် Echo Process လို့ခေါ်ပါတယ်။ ထိုသို့စမ်းသပ်ခြင်းက တစ်ကယ့်ကို ကလေးဆန်ပြီး အခြေခံကျတဲ့စမ်းသပ်ခြင်းမျိုးပါ။ လို့ဂ်ဂူတစ်ခုထဲမှာအော်ဟစ်လိုက်ပြီး ပဲ့တင်သံကိုနားထောင်ကြည့်သကဲ့သို့ပါ။ ပဲ့တင်ဖြစ်စဉ် Echo Process ဖြစ်စေဖို့အတွက် ပစ်မှတ်ဆီသို့မတူညီတဲ့တုံ့ပြန်မှုတွေသက်ရောက်ကြည့်ပြီး တန်ပြန်မှုကိုစောင့်ကြည့်ကာ ဘယ်နည်းလမ်းနဲ့ တုံ့ပြန်မှုဖြစ်စေတယ်ဆိုတာပုံဖေါ်ကြည့်ဖို့ လိုပါတယ်။ ပဲ့တင်ဖြစ်စဉ် ဆိုတာ အကြောင်း-အကျိုး (cause-and-effect) ပုံစံ စိစစ်အတည်ပြုခြင်း ဖြစ်ပါတယ်။

ပဲ့တင်ဖြစ်စဉ်က တစ်စုံတစ်ခုကိုစမ်းသပ်ဖို့ မြန်ဆန်တဲ့နည်းလမ်းဖြစ်ပေမယ့် မှန်ကန်မှုတော့ သိပ်မရှိလို့ ကျပန်းနည်းတစ်ခုဖြစ်ပါတယ်။ ဥပမာ- လုံခြုံရေးကိုစမ်းသပ်ဖို့ ပဲ့တင်ဖြစ်စဉ် ကိုသုံးတဲ့အခါ ပစ်မှတ်က တွေ့မြင်နိုင်မှုမရှိလို့ တုံ့ပြန်မှုမပြုလျင် လုံခြုံတယ်လို့ယူဆကြပေမယ့်၊ အရာဝတ္ထုတွေက တစ်ခါတစ် ရံ Interaction တိုင်းကို ပဲ့တင် မ့ု မပြုတတ်ကြတဲ့အတွက် တုံ့ပြန်မှုမရှိဘူး ဆိုတာ ၁ နဲ့ လုံခြုံတယ်လို့မယူဆနိုင်ပါဘူး။ ထိုသို့သာယူနိုင်တယ်ဆိုရင် သားပိုက်ကောင်တွေ သေချင်ဟန်ဆောင်တိုင်း သားရဲတိရိစ္ဆာန်အတွေ့ ရန်ကလွတ်မြောက်နေမယ်၊ လူတိုင်းအကြောက်လွန်သွားတဲ့အခါတိုင်း ဂက်ဝံတွေရဲ့ ဘေးရန်ကလွတ်မြောက်နိုင်နေ ပါလိမ့်မယ်။ တွေ့မြင်နိုင်မှု Visibility မရှိအောင် ရှောင်ကျဉ်နိုင်ခြင်းကသာ ခင်ဗျားကို တုံ့ပြန်စေခြင်းတစ်ချိုကနေ လွတ်မြောက်စေမှာဖြစ်ပေမယ့် တုံ့ပြန်စေမှု အားလုံးရန်မှ ကာကွယ်မှုတော့ မပေးနိုင်ပါဘူး။

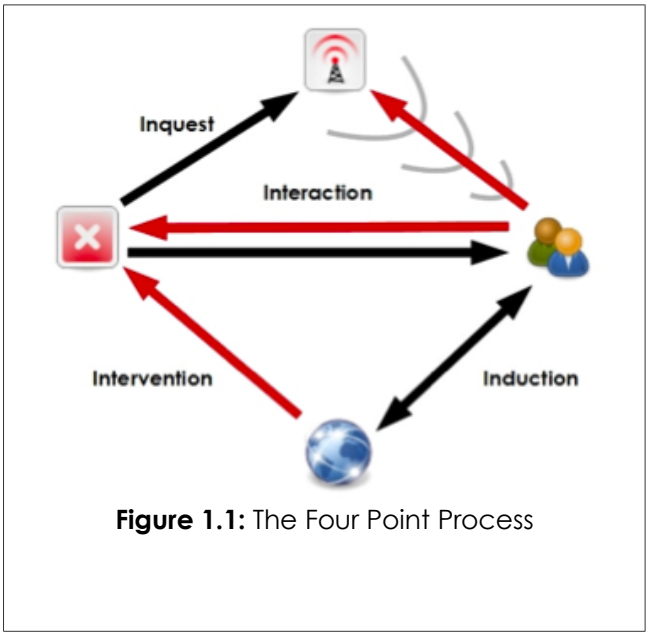

Figure 1.1: The Four Point Process

ကံမကောင်းစွာနဲ့ လူတွေရဲ့နေ့စဉ်ဘဝတွေမှာ စုံစမ်းစစ်ဆေးမှုတွေ ပြုလုပ်နေတဲ့ အဓိကနည်းက ပဲ့တင်ဖြစ်စဉ် တစ်ခုတည်း ဖြစ်နေပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

ထိုသို့တစ်ဖက်မြင်စစ်ဆေးမှုတွေကြောင့် ဆုံးရှုံး ရတဲ့သတင်းအချက်အလက်တွေအများကြီးရှိပါ တယ်။ ကျန်းမာရေးစောင့်ရှောက်မှုအဖွဲ့အစည်း တွေက ဆေးစစ်နည်းလမ်းတစ်ခုဖြစ်တဲ့ "နာကျင်ပါသလား?" "Does it hurt if I do this?" ဆိုတဲ့နည်းလမ်းကို ပြောင်းလဲခဲ့တာကြောင့် ကျွန်တော်တို့ကျေးဇူးတင်သင့်ပါတယ်။ အကယ်၍ ဆေးရုံတစ်ခုက လူတစ်ယောက်ရဲ့ ကျန်းမာရေးစစ်ဆေးရန် အဲဒီလို ပဲ့တင်ဖြစ်စဉ် တစ်ခုတည်းကို သုံးနေမယ်ဆိုရင် လုံးဝလုံလောက်မှာမဟုတ်လို့ ဆရာဝန်တွေ၊ သိပသပံပညာရှင်တွေ အထူးသဖြင့် Hacker တွေက ဖြစ်စဉ်လေးချက် Four Point Process ကိုသေချာ တိကျမှုရှိစေရန် အသုံးပြုလာကြပါတယ်။

The Four Point Process တွင်အောက်ပါ တုံ့ပြန်မှု တွေကို တွေ့နိုင်ပါတယ်။

1. **Induction ဆင်ခြင်သုံးသပ်ခြင်း** : ပစ်မှတ် ရဲ့ပတ်ဝန်းကျင်အနေအထားအရဘာတွေ့နိုင်သလဲ? ၎င်းက ဘယ်လိုအကျင့်စရိုက်တွေရှိလဲ? အကယ်၍ပစ်မှတ်က ၎င်းပတ်ဝန်းကျင်ရဲ့ လွှမ်းမိုးမှုမရှိရင် စိတ်ဝင်စားစရာပါ။
2. **Inquest စုံစမ်းစစ်ဆေးခြင်း**: ပစ်မှတ်ကဘယ်လိုအချက်ပြမှုတွေ ပေါ်ထွက်တတ်သလဲ? ထွက်ပေါ်လာတဲ့ လမ်းကြောင်းတိုင်း၊ ညွှန်တံ၊ တိုင်းကို စစ်ဆေးပါ။ စနစ် (သို့) ဖြစ်စဉ်တစ်ခုက ယေဘူယျအားဖြင့် ၎င်းပတ်ဝန်း ကျင်မှာ တုံ့ပြန်မှုအမှတ်အသားတွေကျန်စေခဲ့ပါတယ်။
3. **Interaction တုံ့ပြန်မှုပြုခြင်း**: ပစ်မှတ်ကို သက်ရောက်မှုတစ်ခုပြုလိုက်တဲ့အခါ ဘာဖြစ်သွားလဲ? အဲဒီအချက်မှာ မျှော်လင့်လျက်ဖြစ်စေ၊ မမျှော်လင့်ချဖြစ်စေ ပစ်မှတ်ကိုတုံ့ပြန်စေမှုပြုလုပ်တဲ့ စမ်းသပ်ချက် တိုင်းပါဝင်ပါတယ်။
4. **Intervention ကြားဝင်နှောက်ယှက်ခြင်း**: အရာဝတ္ထုတစ်ခုကို မကျိုးပျက်ခင် ၎င်းကိုမည်မျှအထိ ကွေးညွှတ်လို့ရသလဲ? ပစ်မှတ် ကို ၎င်းလိုအပ်သောလျှပ်စစ်ဓါတ်အားကဲ့သို့သောအရင်းအမြစ်တွေသုံးပြီး ကြားဝင်နှောက်ယှက်ခြင်း ပြုလုပ်ပြီး ထိုသို့ နှောက်ယှက်မှုအောက်မှာ မည်သို့အလုပ်ဆက်လုပ်တယ်ဆိုတာ နားလည်ဖို့ကြိုးစား ခြင်းဖြစ်ပါတယ်။

ဆေးရုံဥပမာကိုပြန်ကြည့်ကြစို့ ..... FFP ရဲ့ အဆင့်လေးဆင့်တွေက ...

1. ဆရာဝန်တွေကလူနာရဲ့ ဒူးတတောင်ဆစ်တွေကို "နာကျင်ပါသလား?" "Does it hurt if I do this?" နည်း ကိုသုံးပြီး လူနာတွေရဲ့အမှတ်တမဲ့တုံ့ပြန်မှုကိုစစ်ဆေးစမ်းသပ်တဲ့ **တုံ့ပြန်မှု interaction** က **ပဲ့တင်ဖြစ်စဉ် Echo Process** ဖြစ်ပါတယ်။
2. **စုံစမ်းစစ်ဆေးခြင်း Inquest** ကတော့ လူနာရဲ့သွေးခုန်နှုန်း၊ သွေးဖိအား နဲ့ ဦးနှောက်လိုင်း တိုကဲ့သို့ စစ်တမ်းတွေကို ဖတ်ကြည့်ခြင်းဖြစ်ပါတယ်။
3. **ကြားဝင်နှောက်ယှက်ခြင်း Intervention** ကတော့ လူနာရဲ့ အနေအထိုင်၊ လုပ်ရှားမှု၊ သက်တောင့် သက်သာရှိမှုတွေကို ပြောင်းလဲခြင်း၊ ဖိအားပေးခြင်းများ ပြုလုပ်ပြီး ရလာဒ်ကိုစောင့်ကြည့်ခြင်းဖြစ် ပါတယ်။
4. နောက်ဆုံး **ဆင်ခြင်သုံးသပ်ခြင်း Induction** ကတော့ လူနာ အဖျားမဝင်ခင် သွားခဲ့တဲ့နေရာ၊ ပတ်ဝန်း ကျင်ကိုရှာဖွေစစ်ဆေးခြင်း နဲ့ သူတို့ ထိတွေ့ကိုင်တွယ်ခဲ့တဲ့ အရာတွေ၊ ရူခဲ့တဲ့ လေထုနဲ့၊ စားခဲ့တဲ့ အစားအစာ တွေကြောင့် ဖျားနာရန် မည်မျှအကျိုးသက်ရောက်တယ်ဆိုတာတွေကို ရှာဖွေစစ်ဆေးခြင်းဖြစ်ပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Exercise

1.8 ဖြစ်စဉ်လေးချက် Four Point Process ကိုသုံးပြီး နက်နဲတဲ့ တုံ့ပြန်မှု စုံစမ်းစစ်ဆေးခြင်းတွေ လုပ်နိုင်တယ်ဆိုတာ အခုခင်ဗျားမြင်တွေ့တဲ့အတိုင်းပါပဲ။ အခု ခင်ဗျားကိုယ်တိုင် သုံးကြည့်ပါ။ နာရီတစ်လုံးအလုပ်လုပ်နေသလား၊အကယ်၍ ထိုနာရီကအချိန်မှန်စွာအလုပ်လုပ်မယ်ဆိုရင်ဘယ်လိုသိနိုင်လဲ သိနိုင်ဖို့ ဖြစ်စဉ်လေးချက် ကိုခင်ဗျားဘယ်လို သုံးမယ်ဆိုတာရှင်းလင်းဖေါ်ပြပေးပါ။

What to Hack ဘာတွေကို Hackမလဲ?

မည်သည့်အရာကိုမဆို Hacking လုပ်တော့မယ်ဆိုရင် အခြေခံစည်းမျဉ်းတချို့သတ်မှတ်ဖို့လိုပါလိမ့်မယ်။ ဘာကိုတစ်ကယ် Hack နေတယ်ဆိုတာသိဖို့ အသုံးအနှုန်းနှင့် အတွေးအခေါ်တိုင်းတာမှု လိုပါတယ်။ ထိုတိုင်းတာမှုကခင်ဗျား Hack ချင်တဲ့ အရာမှာရှိတဲ့ ဖြစ်နိုင်ခြေလုပ်ငန်းစဉ် တုံ့ပြန်မှုအားလုံးကိုဖေါ်ပြတဲ့ စကားလုံးပါ။

Feed Your Head: Classes and Channels

ပညာရှင်သုံး နည်းပညာအသုံးအနှုန်း (hacker များအတွက်လည်းအသုံးဝင်ပါတယ်) တွေမှာ၊ ထိုတိုင်းတာမှုကို **Channels** ငါးခုခွဲထားတဲ့ **Classes** သုံးခုဖြင့် ဖွဲ့စည်းတည်ဆောက်ထားပါတယ်။

Class	Channel
Physical Security (PHYSSEC) ရုပ်ပိုင်းဆိုင်ရာလုံခြုံရေး	Human - လူ
	Physical - ရုပ်ဝတ္ထုသဏ္ဌာန
Spectrum Security (SPECSEC) အသံလိုင်းစဉ်လုံခြုံရေး	Wireless - ကြိုးမဲ့စနစ်
Communications Security (COMSEC) ဆက်သွယ်ရေး လုံခြုံမှု	Telecommunications - ကြေးနန်း၊ရေဒီယို
	Data Networks - ကွန်ယက်အချက်အလက်

Classes တွေက အဓိကဂရုပြုရမယ့်အပိုင်းတော့မဟုတ်ပါဘူး။ class တွေကလက်ရှိလုံခြုံရေးနယ်မှာအစိုးရအဖွဲ့အစည်းတွေ၊ စစ်တပ်တွေသုံးကြပြီး လေ့လာဖို့၊ စုံစမ်းဖို့၊ လုပ်ငန်းဆောင်ရွက်ဖို့ အတွက်ကိုယ်စားပြုပါတယ်။

Channels တွေက ပိုင်ဆိုင်ပစ္စည်းတွေကိုတုံ့ပြန်မှုပြုစေခြင်း တွေပြုလုပ်ဖို့သာမန်အသုံးအနှုန်းတွေပါ။ Channel တွေပေါ်မှာ ၁ FFP ကိုသုံးပြီး Hack လုပ်ရန်မဟုတ်ပါဘူး။ ၎င်းတို့ကအလုပ်အများကြီးရှိနေပုံ ဖြစ်နေ ပါတယ် ဒါပေမယ့်ကိရိယာတစ်ခုရဲ့ အညွှန်းမှာမပါတဲ့၊ ထုတ်လုပ်မှုပုံစံကိုတောင် မသိပဲနဲ့ ဘယ်လို လည်ပတ်စေရမယ်ဆိုတာ ၁ ရှာတွေ့တဲ့အခါ ဘယ်လောက်ပျော်စရာကောင်းတယ်ဆိုတာတွေးကြည့်ပါ။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

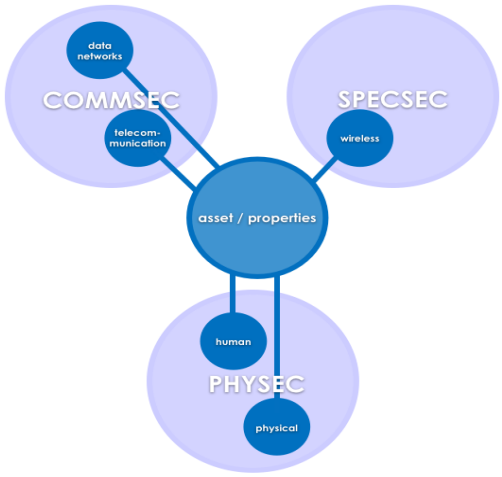

Figure 1.2: Scope

Asset ပိုင်ဆိုင်မှုတစ်ခုဆိုတာ ပိုင်ရှင်အတွက်တန်ဖိုးရှိတဲ့ ရွှေ၊ လူ၊ အသေးစိတ်အစီအစဉ် (blueprints)၊ Laptop၊ ပုံမှန် 900MHzကြိမ်နှုန်းသုံး ဖုန်းတွေ၊ ငွေကြေး စသည်ကဲ့သို့ ရုပ်ပိုင်းဆိုင်ရာ နှင့် ဂန်ထမ်းအချက်အလက်တွေ၊ လူမှုရေးပတ်သက်မှုတွေ၊ ကုန်စည်တံဆိပ်၊ စီးပွားရေး လုပ်ငန်းစဉ်တွေ၊ စကားပုက်၊ ဖုန်းလိုင်းမှာပြောဆိုထားသောစကားမှတ်တမ်းတွေကဲ့သို့ စိတ်ပိုင်းဆိုင်ရာပိုင်ဆိုင်မှုတွေစသည့်အရာအားလုံးဖြစ် နိုင်ပါတယ်။

Dependencies – စပ်ဆက်မှုများက ပိုင်ရှင်ရဲ့ စွမ်းရည်ကို သီးခြားစီအထောက်အပံ့ပေးရန် ပိုင်ဆိုင်မှု နှင့်မတူသောအရာတွေပါ။ ဥပမာ - Computer ပိုင်ရှင်တိုင်း Computer သုံးရန် ကိုယ်ပိုင်လျှပ်စစ်ဓါတ်အားမထုတ်လုပ်ပါဘူး။ ထို့ကြောင့် လျှပ်စစ်ဓါတ်အားက ခင်ဗျားသတိထားရမယ့် ခင်ဗျားရဲ့ စပ်ဆက်မှု နယ်ပယ်တစ်ခုဖြစ်ပါတယ်။

လုံခြုံရေး ရဲ့ အဓိကပန်းတိုင်က ခင်ဗျားရဲ့ပိုင်ဆိုင်မှုတွေ၊စပ်ဆက်မှုတွေ နှင့် ၎င်းတို့ကိုဘေးဖြစ်စေတဲ့ အရာ အားလုံးကြားမှာ **သီးသန့်ခွဲထားခြင်း** (**Separation**) ပဲဖြစ်ပါတယ်။

လုံခြုံရေးဆိုတာ **သီးသန့်ခွဲထားခြင်း** (**Separation**) ဖြစ်ပါတယ်။ သီးသန့်ခွဲထားခြင်း လေးမျိုးကတော့၊

- ပိုင်ဆိုင်မှုတွေ ကိုနေရာချွေထားခြင်း
- ခြိမ်းခြောက်မှုတွေကို အနသတရာယ်မရှိနိုင်တဲ့ အခြေအနေသို့ပြောင်းလဲခြင်း
- ခြိမ်းခြောက်မှုတွေကို ဖျက်ဆီးပစ်ခြင်း
- ပိုင်ဆိုင်မှုကိုဖျက်ဆီးပစ်ခြင်း. (အကြံပြုချက်မဟုတ်ပါ!)

ကျွန်တော်တို့ Hacking လုပ်ကြတဲ့အခါ ပစ်မှတ်ရဲ့ တုံ့ပြန်မှု ရှိနိုင်တဲ့နေရာ၊မရှိနိုင်တဲ့နေရာတွေကိုရှာကြပါတယ်။ အဆောက်အဦးထဲဂင်နိုင်တဲ့တံခါးတွေကိုရှာကြပါတယ်။ အချို့တံခါးတွေက ဂန်ထမ်းတွေ၊ ဂယ်သူတွေ၊ ဧည့်သည်တွေ အတွက်ဂင်ပေါက်၊ အချို့က အရေးပေါ်ထွက်ပေါက်တွေဖြစ်ပြီး အချို့တံခါးတွေကတော့ မလိုအပ်တဲ့ တံခါးပေါက်တွေဖြစ်ပါတယ်။

တံခါးပေါက်တိုင်းက တုံ့ပြန်မှုရှိနိုင်တဲ့နေရာတွေဖြစ်နေပြီး အဲဒီနေရာတွေမှာလိုအပ်တဲ့လုပ်ငန်းတွေလုပ်ဆောင်နိုင်တဲ့အပြင် မလိုလားအပ်တဲ့ သူခိုးကဲ့သို့သောလူတွေလည်း အဂင်အထွက်လုပ်နိုင်နေပါတယ်။ ကျွန်တော့်တို့က အဲဒီတုံ့ပြန်မှုရှိနိုင်တဲ့နေရာတွေကို ဖြစ်စဉ်လေးချက် (FFP) သုံးပြီး Hacker တစ်ယောက်လို ဆန်းစစ်ကြည့်ကြရမှာပါ။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

လျှပ်စီးလက်ခြင်းကိုကြောက်တဲ့လူတစ်ယောက်က (မြေပြင်ပေါ်မှာရှိနေတဲ့အချိန်) လျှပ်စီးလက်ခြင်းကိုပုန်းရှောင်ရန်တန်တစ်ခုတည်းသောနည်းလမ်းက ကျောက်တုံးတွေ၊ ဖုန်မှုန်တွေကို ဖေါက်ပြီးလျှပ်ပြက်ခြင်းမဖြစ်နိုင်တဲ့တောင်ကုန်းတွေထဲကို ဝင်ပုန်းနေခြင်းပဲဖြစ်တယ်။ ဒါပေမယ့် အဲဒီတောင်ကုန်းထဲမှာ အပေါက်တွေဖေါက်မိမယ်ဆိုရင် လျှပ်ပြက်ခြင်းဝင်ရောက်လာနိုင်တဲ့ယိုစိမ့်ပေါက်တွေတိုးလာနိုင်ပါတယ်ဆိုတဲ့အချက်ဖြင့် ယိုစိမ့်ပေါက် porosity များလေလေ hacker တွေက ထိမ်းချုပ်မှုပြုနိုင်လေလေ ဖြစ်တယ်လို့ OSSTMM က နိုင်းယှဉ်ပြထားပါတယ်။

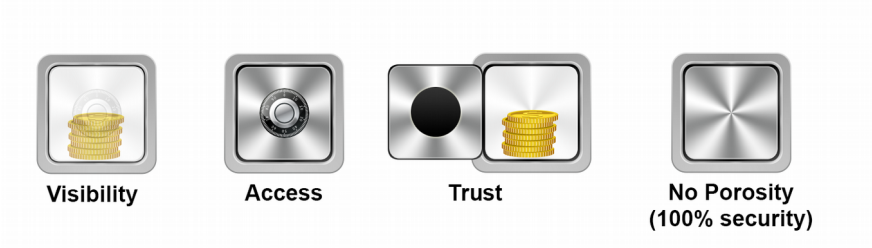

Figure 1.3: Porosity

Feed Your Head: Porosity

ယိုစိမ့်ပေါက် တွေကို မည်သို့ ဖြစ်ပေါ်စေနိုင်လဲ၊ အမျိုးအစားခွဲခြားနိုင်လဲ၊ hacking လုပ်ဆောင်မှုတွေမှာ မည်သို့သတ်မှတ်နိုင်သလဲ ဆိုတဲ့ဥပမာတွေကတော့..

Term	Definition
Visibility မြင်နိုင်ခြင်း	ရဲတွေကရာဇဝတ်မှုတွေကို စုံစမ်းတဲ့အခါ နည်းစနစ်၊ ရည်ရွယ်ချက် နဲ့ အခွင့်အရေးတွေကိုရှာဖွေကြပါတယ်။ အကယ်၍ ပိုင်ဆိုင်မှုတစ်ခုကိုမြင်တွေ့နိုင်နေရင် တိုက်ခိုက်ခံရနိုင်ပြီး မမြင်တွေ့နိုင်ရင်တော့ ပစ်မှတ်ထားခြင်းမခံရနိုင်ပေမယ့်ရှာဖွေလို့ရနိုင်ပါသေးတယ်။ အချို့လုံခြုံရေးပညာရှင်တွေက obfuscation (ဆက်သွယ်ခြင်း၊ သတင်းပေးခြင်း ပြုလုပ်ရာမှာဆိုလိုရင်းကို ဖုံက်ထားပြီး ရှုပ်ထွေးအောင်လုပ်ထားသောစနစ်) သည် မည်သည့်အရာကိုမဆို ဖုံက်ယုံသာဖုံက်ထားနိုင်ပြီးကာကွယ်မှု၊ လုံခြုံမှု မပေးနိုင်ခြင်းကြောင့်အားနည်းသော လုံခြုံရေးစနစ်တစ်ခုလို့ယူဆကြပါတယ်။ သို့သော်လည်း ထိုစနစ်ကဆိုးဝါးတဲ့စနစ်တော့မဟုတ်ပါဘူး၊ အထူးသဖြင့် လုံခြုံရေးစနစ်ဆိုတာ အဆက်မပြတ်တိုးတက်နေရမှာပါ။ ၎င်းရလာဒ်အတွက် OSSTMM မှ *"လုံခြုံရေးက ဘယ်တော့မှဆုံးခန်းမတိုင်ပါဘူး၊ အသစ်ပေါ်ထွက်လာတဲ့ မည်သည့်အရာထက်မဆို ရှေ့ရောက်နေပါတယ်"* လို့ဖေါ်ပြထားပါတယ်။
Access အသုံးပြုနိုင်မှု	Access ကတော့နယ်ပယ်တစ်ခုပြင်ပသို့ တုံ့ပြန်မှုတွေဖြစ်ပေါ်နိုင်တဲ့ မတူညီတဲ့နေရာတွေဖြစ်ပါတယ်။ အဆောက်အဦးတစ်ခုမှာလမ်းပေါ်ရောက်နိုင်တဲ့တံခါးတွေပြုတင်းပေါက်တွေရှိနိုင်ပြီး အင်တာနက်ပေါ်ကဆာဗာတစ်လုံးမှာပွင့်နေတဲ့ကွန်ယက်ဆက်သွယ်မှု portတွေနဲ့ ဆာဗာကွန်ပြူတာမှာ သုံးနိုင်တဲ့ service တွေရှိနေနိုင်ပါတယ်။
Trust	Trust ဆိုတာ တည်ရှိမှုတစ်ခုကအခြားတည်ရှိမှုတစ်ခုရဲ့ တုံ့ပြန်မှုပြုခြင်းကို အဲဒီအတိုင်းအတာအတွင်း လိုလိုလားလားလက်ခံခြင်းဖြစ်ပါတယ်။ ၎င်း Trust ကြောင့် ခင်ဗျားမိခင်က

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

ယုံကြည်မှု	ခင်ဗျားကိုမွေဖက်တဲ့အခါ သူမရဲ့ ID ကို စစ်နေစရာမလိုပါဘူး၊ သူမခင်းကျင်းပေးတဲ့ အစားအစာကိုလည်း သံသယရှင်းရှင်းနဲ့ စားသောက်နိုင်ပါတယ်။ တကယ်လို့ သူမကိုကြိုက်သားတစ်ယောက်က(a la' Invasion of the Body snatchers)စနစ်ဖြင့်အစားထိုးခဲ့ပြီး ခင်ဗျားအစားအစာထဲမှာအဆိပ်ခတ်ခဲ့ရင်လည်း သံသယကင်းကင်းနဲ့ ခင်ဗျားစားနေဦးမှာပါပဲ။ Trust ဆိုတာလူအဖွဲ့အစည်းအတွင်းမှာတန်ဖိုးထားသောလူမှုရေးကျင့်ဝတ်တစ်ခုဖြစ်ပါတယ်။ယုံကြည်မှုမရှိပဲနဲ့ကျွန်တော်တို့တစ်ယာက်နဲ့တစ်ယောက်လွတ်လပ်စွာဆက်ဆံနိုင်မှာမဟုတ်သလို၊ ယုံကြည်မှုကြောင့်ပဲ အရှုံးလုပ်ခြင်း၊ လိမ်လည်ခြင်းများခံရနိုင်ပါတယ်။ OSSTMM က Trust Properties – ယုံကြည်နိုင်မှု ၁၀ ချက်ကိုဖေါ်ပြထားပါတယ်။ အကယ်၍ငင်းသည် ၁၀ချက်စလုံးနှင့်ကိုက်ညီမယ်ဆိုရင်ကျွန်တော်တို့ စိတ်အေးစွာယုံကြည်နိုင်
ပေမယ့်တူညီတဲ့လေ့လာတွေ့ရှိမှုကပဲလူအများစုဟာယုံကြည်နိုင်မှုအချက်တစ်ခုသာ ကိုက်ညီရန်လိုအပ်ပြီး သံသယများသောသူများအတွက်ကတော့ယုံကြည်မှုအကြောင်းပြချက် သုံးချက်သာကိုက်ညီဖို့ လိုပါတယ်လို့ လေ့လာတွေ့ရှိပါတယ်။

Resources - အရင်းမြစ်များ

ထက်မြက်ထိရောက်သော ဆန်းစစ်မှု၊ သုတေသနပြုမှု၊ လေ့လာသင်ယူမှုတွေ နဲ့နိုင်းချိန်တတ်သောအတွေးအခေါ်တွေက Hacker တွေရဲ့အဓိကကျွမ်းကျင်မှုသော့ချက်တွေဖြစ်ပါတယ်။ တကယ်တော့ Hacking ဆိုတာ တီထွင်စမ်းသစ်မှုဖြစ်စဉ်တစ်ခုပါ။ ၎င်းဖြစ်စဉ်က ဘာ၀နေထိုင်မှုပေါ်မှာပို၍အခြေခံပါတယ်။ ကျွန်တော်တို့က ခင်ဗျားသိဖို့လိုအပ်တာတွေအားလုံး မသင်ပြပေးနိုင်ပေမယ့် ခင်ဗျားဘာတွေလေ့လာဖို့လိုတယ်ဆိုတာ နားလည်ဖို့တော့ကူညီပေးနိုင်ပါတယ်။ အဘယ်ကြောင့်ဆိုသော် သိပ္ပံသုတပညာကလျှင်မြန်စွာတိုးတက်ပြောင်းလဲနေပြီး ဒီနေ့ကျွန်တော်တို့ပြောပြတာ အရာတွေကမနက်ဖြန်မှာဆက်စပ်မှုနဲ့ကင်းမှုရှိမနေနိုင်လို့ပဲ ဖြစ်ပါတယ်။ ခင်ဗျားက Hacking မှာမရှိမဖြစ်လိုအပ် တာ hacker တစ်ဦးရဲ့အလေ့အကျင့်တွေကိုလေ့လာဖို့ ယုံကြည်လက်ခံရန်လိုအပ်ပြီး အဲဒီလေ့ကျင့်လေ့လာမှုတွေကပဲ ခင်ဗျားကို *(Script kiddie – hacking tools တွေ ဘယ်လိုအလုပ်လုပ်တယ်ဆိုတာမသိပဲ ထို tools တွေကိုသုံးပြီး hacking လုပ်သူ)* တစ်ဦးမဖြစ်အောင်ကူညီပေးမှာပါ။

အကယ်၍ ခင်ဗျားနားမလည်တဲ့ စကားလုံး (သို့) အယူအဆတစ်ခု တွေ့ခဲ့ရင် ထိုစကားလုံးကိုနားလည်အောင်ရှာဖွေဖို့ တကယ်လိုအပ်ပါတယ်။ စကားလုံးအသစ်တွေကို ကျော်သွားခြင်း၊ ဂရုမပြုခြင်းက ရှေ့လာမယ့်သင်ခန်းစာတွေမှာ အခက်တွေ့စေပါလိမ့်မယ်။ ရှေ့လာမယ့်သင်ခန်းစာတွေမှာ အကြောင်းအရာတစ်ခုကိုစုံစမ်းပြီး အဲဒီအချက်အလက်ကိုသုံးပြီးလေ့ကျင့်ခန်းတွေလုပ်ဖို့ပါလာပါလိမ့်မယ် ဒါပေမယ့် မည်သို့လုပ်ရမယ်ဆိုတာတော့ရှင်းပြထားမှာမဟုတ်ပါဘူး။ ဒါကြောင့် ခင်ဗျားအတွက်အသုံး၀င်တဲ့ ရင်းမြစ်များစွာကိုအသုံးချဖို့ ခင်ဗျားလေ့လာဖို့ လိုသလောက်အချိန်ပေးရန် ပြင်ဆင်ထားပါ။

Books - စာအုပ်များ

ကျွန်တော်တို့က အင်တာနက်မှာရှင်းလင်းစွာညွှန်ပြမထားတဲ့အတွက် ခင်ဗျားထူးဆန်းနေပါလိမ့်မယ် ဒါပေမယ့် စာအုပ်တွေက ခင်ဗျားလေ့လာချင်တဲ့အရာအားလုံးရဲ့ အခြေခံနဲ့လက်တွေ့အဖြစ်မှန်တွေကို လေ့လာဖို့အကောင်းဆုံးနည်းလမ်းတွေပါ။ ခင်ဗျား Personal Computer (PC)ရဲ့ Hardware အသေးစိတ်ပါ၀င်မှုကဲ့သို့ ကွန်ပြူတာသိပ္ပံသဘံဆိုင်ရာအချက်တွေကိုသိချင်နေတယ်ဆိုပါစို့? အဲဒီဘာသာရပ်ဆိုင်ရာ

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

လက်ရှိကာလထွက်တဲ့စာအုပ်ကိုရှာဖတ ် ခြင်းထက်မည်သည့်အရာကမ ့ ခင်ဗျားကိုမကူညီနိုင်ပါဘူး။ ကွန်ပြူတာသိပသံသပံဆိုင်ရာစာအုပ်တွေရဲ့အဓိကပြဿသနာက လျင်မြန်စွာရက်လွန်သွားခြင်းပါပဲ။ အသေးစိတ်အချက်တွေရ ဲ့ ပါးလွှာသောမျက်နှာပြင်အောက်ကအခြေ ံ တည်ဆောက်ပုံကို သိမြင်နိုင်ရန်လေ့လာခြင်းက လျှိုဝှက်ချက်ဖြစ်ပါတယ်။ MS-DOS နှင့် Windows ကသိသိသာသာ ကွဲပြားကြပါတယ် ဒါပေမယ့် ၎င်းစနစ်နှစ်ခုစလုံးက Ada, Countess of Lovelace တို့ ၁၉ရာစုမှာပထမဆုံး ပရိုဂရမ်ကိုရေးခဲ့ချိန်ကတည်းက ကွန်ပြူတာတွေကိုမောင်းနှင်ခဲ့တ ဲ့ Boolean တွက်ချက်မှုစနစ် ပေါ်မှာအခြေခံထားကြပါတယ်။ လုံခြုံရေးနှင့် သီးသန့်တည်ရှိမှုဆိုင်ရာကိစ္စသစရပ်တွေက နှစ်ပေါင်း ၂၅၀၀အတွင်းမှာ ပြောင်းလဲသွားခဲ့နိုင်ပါတယ်။ ဒါပေမယ့် Sun Tzu ရေးသားတဲ့ The Art of War စာအုပ် က ဒီနေ့အထိ အသုံးပြုနေသောအခြေခံ စည်းမျဉ်းတွေကိုဖော်ပြထားပါတယ်။ (စကားမစပ်။ ။ မရင့်ကျက်တဲ့သူ(n00b) တစ်ယောက်လို အထင်ခံရဖို့က Sun Tzu ကို ကိုးကားပြောဆိုပြခြင်းထက်မြန်ဆန်တဲ့နည်းလမ်းမရှိပါဘူး။ တစ်ချို့အရာတွေကို ခင်ဗျားဘယ်လို အသုံးပြုရမယ်ဆိုတာသိပေမယ့် ထုတ်မပြောပါနဲ့။ The Art of War စာအုပ်ကို ကိုးကားပြခြင်းက ခင်ဗျားဒီစာအုပ် ကိုတစ်ကယ်မဖတ်ရသေးကြောင်းပေါ်လွင်နေပါတယ်၊ ဘာကြောင့် လဲဆိုတော့ Sun Tzu (စာရေးသူ) ကိုယ်တိုင်က ခင်ဗျား တကယ်နားလည်ထားတဲ့ အကြောင်းအရာဗဟုသုတကို ခင်ဗျားရဲ့လျှိုဝှက်ချက်အနေနဲ့ထိန်းသိမ်းထားပါလို့ ပြောထားလို့ပဲဖြစ်ပါတယ်။)

စာအုပ်ထဲမှာပါတဲ့အချက်အလက်တွေက အခြားအရင်းမြစ်တွေမှာတွေ့နိုင်တဲ့အချက်အလက်တွေထက် ခေတ်မမှီ နိုင်ဘူးဆိုရင်တောင်စာအုပ်ထဲမှာတွေ့တဲ့အချက်အလက်တွေကအခြားနေရာတွေမှာတွေ့ရတဲ့အချက်အလက်တွေ ထက်ပိုကောင်းမွန်စွာရေးသားထားပါတယ်။ တစ်ခါတစ်ရံစာအုပ်ထဲကအချက်အလက်တွေကပိုမှန်တတ်ပါတယ်။ နှစ်ချီပြီးအချိန်ပေးကာ စာအုပ်တစ်အုပ်ကိုရေးသားထားတဲ့စာရေးဆရာက၊ Blog တစ်ခုကိုတစ်နေ့ ခြောက်ကြိမ် လောက် update လုပ်နေသူတစ်ဦးထက်ပိုပြီးမှန်ကန်နိုင်ပါလိမ့်မယ်။ (Zines နှင့် Blogs အခန်းမှာအသေးစိတ် ဖတ်ပါ။)

ဒါပေမယ့် မှန်ကန်သောအရာတွေကလည်း တစ်ဖက်စောင်းနင်းမဖြစ်နိုင်ဘူးလို့မပြောနိုင်ဘူးဆိုတာ မမေ့ပါနဲ့။ စာရေးသူရဲ့ သတင်းအချက်အလက်တွေရရှိရာရင်းမြစ်ကိုက တစ်ဖက်လိုက်နေတတ်ပါတယ်။ "သမိုင်းကြောင်း စာအုပ်တွေကို အောင်နိုင်ကျန်ရစ်ခဲ့သူတွေကရေးကြတာပါ။" ဆိုတဲ့ကိုးကားချက်ကို ကြည့်ပါ နိုင်ငံရေးအရှုပ်တွေ နဲ့ လူမှုရေးသတ်မှတ်ချက်တွေက ထိုအချိန်ကာလတစ်ခုမှာ ဖော်ပြထုတ်ပြန်ရန် တားမြစ်ခံထားရနိုင်တဲ့ အခြေအနေ မှာ အမှန်တရားတခုတည်းကိုသာဆုတ်ကိုင်ထားပါလိမ့်မယ်။ အများအားဖြင့်ထိုတစ်ဖက်စောင်းနင်းရေးသား မှုတွေ က နိုင်ငံရေးဖြစ်စဉ်တွေနဲ့ လူမှုအဖွဲ့အစည်းအရ သိမြင်ရန်လက်ခံနိုင်သော သုံးသပ်ချက်သတင်းတွေပါဝင်တဲ့ ကျောင်းသုံးဖတ်စာအုပ်တွေမှာအဖြစ်များပါတယ်။ ရွှေရောင်အမှန်တရားကိုသိလိုက်ရပြီလို့ မထင်ပါနဲ့ အဘယ် ကြောင့်ဆိုသော် ခင်ဗျားကစာအုပ်တစ်အုပ်ထဲက အကြောင်းအရာကိုဖတ်နေတာကြောင့်ပါ။ အမှန်တရားဆိုတာ လူတိုင်း စာအုပ်တစ်အုပ်ရေးနိုင်ပြီး စာအုပ်တိုင်းမှာစာရေးသူတွေရဲ့ အမှန်တရားအမြင်အမျိုးမျိုးပါဝင်နိုင်ခြင်းပဲ ဖြစ် ပါတယ်။

အရမ်းထူတဲ့စာအုပ်ကိုကြည့်ပြီး မဖတ်ရသေးခင်စိတ်မလျော့လိုက်ပါနဲ့၊ အဲဒီစာအုပ်ကိုဘယ်သူမှအစကနေအဆုံး မဖတ်ကြပါဘူး။ အဲဒီစာအုပ်တွေကို မှတ်တမ်းမယူမီက web စာမျက်နှာတွေလိုသဘောထားကြည့်ပြီး ကျပန်း စာမျက်နှာတစ်ခုကိုဖွင့်ပြီး စတင်ဖတ်ကြည့်ပါ။ အကယ်၍ ခင်ဗျားတစ်ခုခုကိုနားမလည်တော့ဘူးဆိုရင် နောက်ကို ပြန်သွားပြီးရှင်းလင်းချက်ကိုရှာကြည့်ပါ (သို့မဟုတ် ကျော်ပြီး ခင်ဗျားနားလည်မယ့်အရာကိုရှာဖတ်ပါ)။ web စာ မျက်နှာတွေ ချိတ်ဆက်မှုတစ်ခုကနေတစ်ခု အပြန်အလှန်ဖတ်သလို အဲဒီစာအုပ်ကို အရှေ့အနောက် အပြန်အလှန် ဖတ်ကြည့်ပါ။ ထိုကဲ့သို့အစဉ်အတိုင်းမဟုတ်တဲ့စူးစမ်းခြင်းက စာဖတ်ခြင်းထက် သိလိုမှု၊ စူးစမ်းလိုမှုတွေကို ပြည့်ဝ စေတဲ့ အတွက် Hacker တွေကို စိတ်ဝင်စားခြင်းနှင့်အားရကျေနပ်စေခြင်းတွေ ဖြစ်စေ နိုင်ပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

နောက်ဆုံးအချက်ကတော့ စာဖတ်သူတွေကကောင်းစွာစာရေးနိုင်တဲ့ တန်ဖိုးရှိတဲ့စွမ်းရည်တွေ ရရှိနိုင်ပါတယ်။ နယ်ပယ်အသစ်တစ်ခုမှာ နားလည်ဖို့ ပါဝင်လာတဲ့အခါတိုင်းအတွက် ထိုအချက်ကကြီးမားတဲ့ ကောင်းကျိုးအားသာချက်ဖြစ်ပါတယ်။ ထိုအချက်ကြောင့်ပဲ ခင်ဗျားကိုအခြားစာဖတ်သူတွေ၊ အထူးသဖြင့်ဩဇာရှိသူတွေက ချီးကျူးဂုဏ်ပြုလာပါလိမ့်မယ်။

Magazines and Newspapers – မဂ္ဂဇင်း နှင့် သတင်းစာများ

မဂ္ဂဇင်း နဲ့ သတင်းစာတွေက လိုရင်းတိုရှင်းဖြင့် အချိန်နှင့်အညီ သတင်းများကိုရရှိစေရန် အထောက်အကူပြုပါတယ်။ ထိုကဲ့သို့ ထုတ်ဝေခြင်း နှစ်မျိုးစလုံးက တိကျတိုရှင်းတဲ့ အသေးစိတ်အချက်တွေပါနိုင်ပါတယ်။ သတင်းစာတိုင်း၊ မဂ္ဂဇင်းတိုင်းမှာ မူပိုင်ပရိတ်သတ်၊ မူပိုင်လုပ်ငန်းစဉ်၊ မူပိုင်အသုံးအနှုန်းတွေ၊ "မျှတသောဘက်မလိုက်သော" အဆိုပြုမှုတွေကိုဂရုမပြုခြင်း တွေကိုယ်စီရှိနေတယ်ဆိုတာဂရုပြုပါ။ ထုတ်ဝေမှုပုံစံကိုသိရှိခြင်း - Linux မဂ္ဂဇင်းက Microsoft Windows နဲ့ပတ်သက်တဲ့ရင်းမြစ်ကောင်းတစ်ခုဖြစ်ဖို့ မလိုပါဘူး။ Microsoft က Linux နှင့်မသက်ဆိုင်သောအကြောင်းအရာဖြစ်ပြီး Linux မဂ္ဂဇင်းရဲ့စာဖတ်သူက Linux အထူးပြုအကြောင်းအရာတွေပဲဖတ်ချင်မှာပါ။ အထူးမဂ္ဂဇင်းအများစုက **Cherry Picking** နည်းပညာကိုအသုံးပြုကြပါတယ်။ cherry picking ဆိုတာ မဂ္ဂဇင်းရဲ့ အကြောင်းအရာနဲ့သက်ဆိုင်တဲ့အရာတွေရဲ့ အပြုသဘောဆောင်သော အကြောင်းအရာတွေကို အထူး ပြုဖော်ပြ ခြင်း (သို့) မဂ္ဂဇင်းရဲ့အကြောင်းအရာနဲ့မသက်ဆိုင်တဲ့အရာများရဲ့ အဆိုးမြင်အကြောင်းအရာတွေကို အထူးပြုဖော် ပြခြင်း နည်းစနစ်ဖြစ်ပါတယ်။

သတင်းစာ၊ မဂ္ဂဇင်းတွေရဲ့ ဖြစ်နိုင်ခြေရှိတဲ့ ဘက်လိုက်ရေးသားမှုတွေကိုသတိပြုပါ။ သူတို့က ဖြစ်ရပ်တစ်ခုရဲ့ တကယ့်အဖြစ်မှန်ကို ဖော်ပြခြင်းထက် သူတို့ရဲ့အမြင်တွေကို ဦးစားပေးဖေါ်ပြတာကြောင့် ခင်ဗျားကိုယ်ပိုင် အမြင်ကိုပုံမပေါ်နိုင်ပါဘူး။ ရင်းမြစ်ကိုဆင်ခြင်သုံးသပ်ပါ! "မည်သည့်ဖက်မှမပါသောသူ" ဖြစ်ရင်တောင် အပတ်စဉ် (သို့) လစဉ်ထုတ် မဂ္ဂဇင်း၊ သတင်းစာတွေမှာ ထင်ကြေးတွေ၊ ဘက်လိုက်ရေးသားမှုတွေ ပြည့်နှက်စွာပါဝင်နိုင်ပါတယ်။ ထိုထင်ကြေး၊ ဘက်လိုက်ရေးသားမှုတွေကို "ပညာရှင်နှင့်ယှဉ်ဆချက်"လို့ ဂျာနယ်၊ သတင်းစာ သမားများကခမ်းနား စွာ သုံးနှုန်းရေးသားသော်လည်း ဂျာနယ်သမားများရဲ့ "ထင်ကြေး" တစ်စိတ်တစ်ပိုင်းမျှသာဖြစ်ပါတယ်။

ဆေးဝါးကုမ္ပဏီများက ၎င်းတို့ဆေးဝါးစမ်းသပ်ထုတ်ဝေရန် ကျရှုံးတယ်ဆိုရင်တောင် ဆရာဝန်များက ဘယ်ဆေး၊ ဘယ်လုပ်ထုံးလုပ်နည်း ဆိုတာတွေကို ဩဇာရှိစွာသတ်မှတ်ရွေးချယ်နိုင်တာကြောင့် ၎င်းတို့၏ ဆေးဝါးများအားလုံး ကိုစမ်းသပ်ထုတ်ဝေခွင့်ရရှိနိုင်ရန် ကြီးကျယ်သောလုပ်ရှားမှုတွေ လုပ်ဆောင်လျက်ရှိနေကြပါတယ်။ လက်ရှိ ဆေးဝါး မဂ္ဂဇင်း၊ ဂျာနယ်တွေက စစ်ဆေးခြင်းရလာဒ် အမှန်တရားကိုဖေါ်ပြနေကြစဉ်မှာတောင် အဲဒီအမှန်တရား နောက်ကွယ်က အသေးစိတ်အခြေအနေတွေက ရှုပ်ထွေးမှုန်ဝါးနေဆဲဖြစ်ပါတယ်။ ဤသည် က ၎ း အကြောင်း တရားဖစ်မြစ်ရှိမှုအပေါ်မှာ မှီခိုနေတဲ့အကြောင်းအရာများနှင့်ပတ်သက်ရတဲ့အခါ တကယ့်ကိုအရေးကြီးတဲ့ကိစ္စသစ ဖြစ် ပါတယ်။ အကြောင်းအရာတွေ ဖြစ်ပေါ်ဖို့ ဦးဆုံးဖြစ်တဲ့အကြောင်းနဲ့ အကျိုးရလာဒ် ရဲ့အကြောင်းပြချက်တွေ လိုအပ် ပါတယ်။

သတင်းဂျာနယ်တွေက မရည်ရွယ်ပဲဖြစ်စေ (သို့) ရည်ရွယ်၍ဖြစ်စေ သုံးတတ်တဲ့ အခြားပရိယာယ်တွေကတော့ ပုံပြင်ဆန်ဆန်သက်သေတွေပါ။ အဲဒီပုံပြင်ဆန်ဆန်သက်သေဆိုတာပညာရှင်ဟုတ်သည်ဖြစ်စေမဟုတ်သည်ဖြစ်စေ ဂရုမပြုပဲ သက်သေခံအဖြစ်ထွက်ဆိုသူတိုင်းရဲ့ထွက်ဆိုချက်အမြင်တွေကိုဖော်ပြခြင်း၊ ဒုတိယတစ်ခုက ပြောရေးဆိုခွင့်ရှိသောသက်သေတွေပါ - ဖြစ်ရပ်တစ်ခုဖြစ်ပွားရာဝန်းကျင်မှာရှိတဲ့ကျွမ်းကျင်ဝန်ထမ်းတွေနဲ့၊အခြားနယ်ပယ်တစ်ခုခုက အခွင့်အာဏာရှိသူတွေရဲ့အမြင်တွေကိုဖေါ်ပြခြင်းဖြစ်ပြီး နောက်ဆုံးတစ်ခုကထင်ကြေး ပေးခြင်းတွေပါ -

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

အများကအမှန်ဟုယူဆထားသောအခြေအနေတစ်ခုနှင့် နိုင်းယှဉ်ဖန်တီးပြီးအမှန်တရားအနေနဲ့ဖေါ်ပြခြင်းပဲဖြစ်ပါတယ်။

မှန်ကန်မှု နဲ့ လုပ်ငန်းအစီအစဉ် ကိစ္စသစတွေကိုအကောင်းဆုံးဖြေရှင်းဖို့ နည်းလမ်းကတော့ အမြင်ကျယ်ကျယ်ဖြင့် သေချာဖတ်ခြင်းပဲဖြစ်ပါတယ်။ ခင်ဗျားစိတ်ဝင်စားတဲ့အကြောင်းကို မဂ္ဂဇင်းမှာဖတ်တဲ့အခါ အနာဂါတ်ဖြစ်နိုင်ခြေကို ကြည့်ပါ။ အဲဒီအကြောင်းအရာရဲ့အဖက်ဖက်ကနေဆန်းစစ်အတည်ပြုပြီးအဖြေရှာပါ။ ဤအလေ့အထက တစ်ကယ့် ကို စွမ်းအားပြည့်ဝတဲ့ ဥာဉ်ဖြစ်ပါတယ်။

Exercises

1.9 အင်တာနက်မှာ Hacking မဂ္ဂဇင်း သုံးအုပ်ရှာပါ။ ခင်ဗျားမည်သို့ရှာခဲ့ပါသလဲ ရှင်းပြပါ?

1.10 အဲဒီသုံးအုပ်စလုံးကကွန်ပြူတာHacking အကြောင်းတွေပဲလား?
အခြားစီးပွားရေးလုပ်ငန်းတွေသို့မဟုတ် အခြားနယ်ပယ်တွေ မှာအသုံးဝင်တဲ့ မည်သည့်အရာတွေကိုရောရှာတွေ့ပါသေးလဲ?

Feed Your Head: Speculation - ထင်ကြေးပေးခြင်း

အောက်ပါစာပိုဒ်က သတင်းစာတစ်စောင်ထဲမှာပါတဲ့ ဓါးပြမှုဆောင်းပါးတစ်ပုဒ်ဖြစ်ပါတယ်။ အဲဒီဆောင်းပါးထဲမှာထင်ကြေးပေးခြင်းတွေကို တွေ့ပါသလား? ခင်ဗျားသံသယရှိတဲ့ အပိုင်းတွေကိုမှတ်ထားကြည့်ပါ။

The Lake Meadow ဘဏ် နှင့် Mortgage ငွေချေးဌာန က အဂၤသငါးနေ့ နေလည်ခင်းမှာ ဓါးပြတိုက်ခံခဲ့ရပါတယ်။ ဘဏ်မပိတ်ခင် မှာ မျက်နှာဖုံးတပ်သေနတ် သမားကလမ်းလျောက်ဝင်လာပြီး၊ ဝန်ထမ်းတွေကိုဓါးစာခံအဖြစ်ဖမ်းပြီး၊ ဓါးပြတိုက်ခဲ့ပါတယ်။ ထိုနောက် SUV နောက်ဆုံးပေါ်ကားနဲ့ ထွက်ပြေးလွတ် မြောက်သွားခဲ့ပါတယ်။ ဓါးစာခံတွေ အားလုံးထိခိုက်မှုမရှိခဲ့ပါဘူး။

ဓါးပြတိုက်မှုနောက်ပိုင်းမှာ အဲဒီကားကိုဘဏ်အနောက်ဘက်မှာတွေ့ခဲ့ရပြီး၊ ၎င်းကားက တောင်ဘက် ရှိ Bluegreen တောင်တန်းတွေရဲ့ထူထပ်တဲ့ သစ် တောဆီကိုဦးတည်သွားခဲ့တယ်လို့သိရပြီး၊ ထိုဖြစ်ရပ်နဲ့ ရဲတွေကို ထိုဓါးပြမှုအား ကျွမ်းကျင်လုပ်ငန်းအဖြစ် ယုံကြည်စေခဲ့တဲ့ အဲဒီသေနတ်သမားကို မည်သူတစ်ဦး တစ်ယောက်မှ မဖေါ်ထုတ်နိုင်ခဲ့ပါဘူး။ ရဲတွေကတော့ ထောင်မှတ်တမ်းရှိတဲ့ ကျွမ်းကျင်ဓါးပြတွေ နဲ့ သူတို့ပတ်ဝန်းကျင်ကလူတွေကို စတင်ရှာဖွေ စစ်ဆေးတော့မယ်လို့ ထင်ရပါတယ်။

ပျမ်းမျှ ဘဏ်သူခိုး ၅၇ယောက် ကနေစဉ်တိုင်းကြားခံနေရပြီး ၊ Bluegreen တိုင်းပြည်ရဲ့ လူဦးရေပြောင်းရွှေ့နေထိုင်မှုက လာမည့်နှစ်မှာ ၅၀,၀၀၀ အထက်မှာရှိမှာဖြစ်ပါတယ်၊ အဲဒါကြောင့် ယသသခုဖြစ်ရပ်ကတော့ ဘဏ်ဓါးပြတွေရဲ့ သောင်းကျန်းမှုအစပဲ ရှိပါ သေးတယ်။ "အခုမှ အစပဲရှိသေးတယ် လို့ထင်ရတယ်" လို့ ရဲမင်းကြီး smith ကပြောပါတယ်။

ကျွန်တော်တို့က အချက်အလက်နဲ့ရလဒ်တွေပေါ်မှာ ဘက်လိုက်ရေးသားခြင်းတွေကို သတိမပြုမိခြင်း ထင်ကြေးပေးမှုတွေအပေါ်ခံစားချက်မထားမိခြင်းများရှိသဖြင့် ကျွန်တော်တို့ဖတ်နေတဲ့သတင်းတွေက သတင်း စာဆရာတစ်ယောက်ထဲရဲ့ ထင်ကြေးနဲ့ ဇာတ်လမ်းဆင်ရေးသားမှုတွေဖြစ်နိုင်ပါတယ်။ အထက်ပါသတင်း ဆောင်းပါးမှာ "ဘဏ် က အဂၤသငါးနေ့ နေလည်ခင်းမှာဓါးပြတိုက်ခံရတယ်။" ဆိုတဲ့ သတင်းတစ်ခုပဲအမှန်ဖြစ်ပါတယ်။ ယသသခုအခါ ဂရုပြုမှုရရှိရန် ကျွန်တော်တို့က ထင်ကြေးပေးရေးသားမှုတွေကို ပို၍အဓိပသယပါယ်မဲ့သွားအောင် အောက်ပါအတိုင်း ပြင်ဆင်ရေးသားကြည့်ပါမယ်။

The Righteous ဘဏ် နှင့် Mortgage ငွေချေးဌာန က အဂၤသငါးနေ့ နေလည်ခင်းမှာ ဓါးပြတိုက်ခံခဲ့ရပါတယ်။ ဘဏ်မပိတ်ခင်မှာ မျက်နှာဖုံးစွပ်ပေးထားတဲ့ ကြက်တေ့ လမ်းလျောက်ဝင်လာပြီး၊ ကြက်လျောင်အိမ်ကဲ့သို့ မိုးပျံဘောလုံးပုံစံထဲမှ ၁ ၎င်းတို့ ထွက်ပြေးလွတ်မြောက်မှုရရှိရန်မပြုလုပ်ခင် ဆယ်စုနှစ်တစ်စု ကြာအောင် ဝန်ထမ်းတွေကို ဓါးစာခံအဖြစ်ဖမ်းထားနိုင်ခဲ့ပါတယ်။ မည်သည့် ဓါးစာခံတစ်ဦးတစ်ယောက်မှ ဒုက္ခမွေးများမပေကျံခဲ့ပါဘူး။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

မိုးပြတိုက်မှနောက်ပိုင်းမှာ အဲဒီမိုးပျံဘောလုံးကို ဘက်အပေါ်မှာတွေ့ပြီး ၎င်းဘောလုံးက တောင်ဘက် အနာသတာတိကရဲ့ သနာသတာကျောက်တန်းတွေဆီ ပျံသန်းသွားတာတွေ့ခဲ့ရပြီး၊ ထိုဖြစ်ရပ်ဖြင့် ၎င်းတို့ကကျွမ်းကျင်ရုပ်ဖျက်ပညာရှင်တွေအပြင် ကျွမ်းကျင် သောဘောလုံးပြုလုပ်သူတွေအဖြစ် ရဲတွေကို ယုံစေခဲ့တဲ့ အဲဒီ ကြောက်တွေကို မည်သူမှ မဖေါ်ထုတ်နိုင်ခဲ့ပါဘူး။ ရဲတွေကတော့ ယာယီ အချိန် မှာ ဘောလုံးပြုလုပ်ခြင်းလည်းပါသနာပါတဲ့ ကျွမ်းကျင်မိတ်ကပ် ပညာရှင်တွေကို စတင်စစ်ဆေးတော့မယ်လို့ထင်ရပါတယ်။

ပျမ်းမျှ ဘက်သူခိုး ၅၇ဦးခန်ဟာ နေ့စဉ်တိုင်ကြားခံနေရပြီး ဘောလုံးထုတ်လုပ်မှုစက်ရုံ တွေကအနာဂါတ်မှာရောင်းအား $၄၇ ဂါဇီလီယံ ရရှိနိုင်ရန်ကြောင့်နေကြပါတယ်၊ ဒါဟာ ဘက်ဓါးပြတွေရဲ့ သောင်းကျန်းမှုအစပဲရှိသေးတာဖြစ်နိုင်ပါတယ်။ "အခုမှ အစပဲရှိသေးတယ် လို့ထင်ရတယ်" လို့ ရဲမင်းကြီး Gordon ကပြောပါတယ်။

အလွန်အကြူးဖွဲ့ဆိုခြင်းကြောင့် ၎င်းဘက်လိုက်သတင်းက လုံခြုံရေးဆိုင်ရာအဆောက်အအုံထဲသို့ လျင် မြန်စွာ ပျံနှံ့လာတာ အဆန်းမဟုတ်ပါဘူး။ ထိုအဆောက်အအုံထဲမှာသာမန်သုံးတဲ့အသုံးအနှုံးကတော့ (Fear, Uncertainty and Doubt) FUD ပဲဖြစ်ပါတယ်။ ၎င်းစကားလုံးက တစ်စုံတစ်ဦးရဲ့ စိတ်ဝင်စား မှုရရှိပြီး လုံခြုံရေး ဆိုင်ရာဝန်ဆောင်မှုတွေကို ရောင်းချရန်အတွက် ထင်ကြေး နှင့် စိတ်ကူးယဉ်ရေးသားခြင်းတွေကို မည်သို့အသုံးချ တယ်ဆိုတာကိုရည်ညွှန်းပါတယ်။ ကံမကောင်းစွာနဲ့ ထိုသို့အသုံးပြုခြင်းက လူတွေ ရဲ့ယုံလွယ်ခြင်းအပေါ်ကောင်း စွာအကျိုးသက်ရောက်မှုရှိနေပါတယ်။ ထိုအချက်များကြောင့် မမှန်ကန်သော လုံခြုံရေးနည်းပညာဖြေရှင်းမှုတွေ ဖြစ်ပေါ်စေခြင်း၊ လုံခြုံရေးကို မှားယွင်းစွာအသုံးပြုခြင်း၊ မှားယွင်းစွာယုံကြည်ပြီး ခွင့်ပြုခြင်းများ ဖြစ်စေနိုင်ပါတယ်။ ထိုသတင်းဖေါ်ပြချက်မှာ လူဦးရေပြောင်းရွှေ့နေထိုင်မှုအပေါ် ဆိုးဝါးစွာထင်မြင်ယူဆထားတဲ့ စီးပွားရေး ကြောက်ခြာ နှင့် ဒုစရိုက်မှု နှစ်ဖက်လုံးကို အထူးပြု၍ဖော်ပြထားမှုက ထင်ရှားစွာပေါ်လွင်နေပါတယ်။

Search Engines - ရှာဖွေရေးစက်များ

Google ကတော့ ကျော်ကြားတဲ့ search engine တစ်ခုပါ ဒါပေမယ့် google တစ်ခုထဲ search engine မဟုတ်ပါဘူး။ Bing ကတော့ ရိုးရှင်းတဲ့မေးခွန်းတွေရှာဖွေတဲ့နေရာမှာပြည့်စုံကောင်းမွန်ပြီ း Yahoo ကတော့ သုတသန လုပ်ငန်းတွေအတွက် ကောင်းမွန်ပါတယ်။ အဲဒီ web ဝန်ဆောင်မှုတွေ ကခင်ဗျားအကြောင်းကို သူတို့ သိသင့်တာထက်ပိုသိနိုင်အောင်စောင့်ကြည့်မှတ်တမ်းယူနေကြတယ် ဆိုတာတော့ အထူးသတိပြုပါခင်ဗျားရှာသမျှ တွေနဲ့ search engine အသုံးပြုပြီး ဘယ် website တွေကိုသွားတယ်ဆိုတာ အားလုံး search engine ဝန် ဆောင်မှုတွေက မှတ်တမ်းယူထားကြပါတယ်။

> AltaVista နဲ့ DuckDuckGo.com search engine တွေကတော့ လျှို့ဝှက်စွာရှာဖွေခြင်းပြုလုပ်တဲ့အခါ မှတ်တမ်းမယူနိုင်အောင် ကာကွယ်ပေးနိုင်တဲ့ search engine တွေပဲဖြစ်ပါတယ်။

Website တွေ online ဖြစ်နေတဲ့အခါနဲ့ online ဖြစ်ခဲ့ပြီးနောက် ကြာရှည်စွာ ၎င်းတို့ကိုရှာဖွေတွေ့နိုင်ပါတယ်။ ပုံမှန် အားဖြင့် ၎င်းတို့ကို cache page form ထဲမှာ ကြာရှည်စွာ သိမ်းဆည်းထားပါတယ်။ အင်တာနက် cache ဆိုတာ website တွေရဲ့ ရှေးဦးပုံစံတွေကိုမှတ်တမ်းတင်ထားခြင်းတစ်ခုဖြစ်ပါတယ်။ search engine များနဲ့ မှတ်တမ်းထား တဲ့နေရာ (archive sites) တွေက အဲဒီသတင်းအချက်အလက်တွေကို အကန့်အသတ်မရှိ ထိန်းသိမ်းထားပါတယ်။ ထိုသို့ထိန်းသိမ်းခြင်းကို အင်တာနက်အခေါ်အဝေါ် "forever" လို့ခေါ်ပါတယ်။ ခင်ဗျားကအင်တာနက်ပေါ် တင်မည့် မည်သည့်အရာမဆို မတင်ခင် "forever" ဆိုတာကိုသတိရဖို့အရေးကြီးပါတယ်။ Webpage တစ်ခုရဲ့ cached copy ချိတ်ဆက်မှုကို ရှာနိုင်ပါတယ် ဥပမာ - Google ကရိုးရှင်းစွာ "Cache" လို့ အမည်ပေးထားတဲ့ လင့်ခ်ကို ပုံမှန် အသုံးပြုပါတယ်။

Search engine များအပြင် အင်တာနက်မှတ်တမ်း (Internet archive) (http://www.archive.org) များက လည်းအသုံးဝင်တဲ့ဝန်ဆောင်မှုတွေ ဖြစ်ပါတယ်။ အဲဒီအင်တာနက်မှတ်တမ်းတွေမှာ website တစ်ခုလုံးရဲ့ cache

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

တွေအားလုံးရှာတွေ့နိုင်လို့ ပျောက်ကွယ်သွားတဲ့သတင်းအချက်အလက်တွေကို ရှာဖွေရန် တကယ့်ကိုအသုံးဝင်ပါတယ်။

website တွေကို search engine မှာရှာဖွေနိုင်တဲ့အတွက် ယုံကြည်နိုင်တယ်လို့ မယူဆပါနဲ့။ Hacker အများစုရဲ့ တိုက်ခိုက်မှုတွေ၊ ကွန်ပြူတာပိုင်းရပ်စ်တွေက website တွေဝင်ကြည့်ခြင်း၊ ပုံမှန်လို့ထင်ရတဲ့ ပရိုဂရမ်တွေကို download လုပ်ယူခြင်းတွေကနေတဆင့် ပျံနှံ့ဖြစ်ပွားတာပါ။ မယုံကြည်နိုင်တဲ့၊ မူမမှန်တဲ့ website တွေကနေ ပရိုဂရမ်ကိုမယူခြင်း၊ ခင်ဗျားရဲ့ browser ကို sandbox (virtual machine) ပေါ်မှာသုံးခြင်းဖြင့် လုံခြုံမှုရှိနိုင်တယ်ဆိုပေမယ့် ထိုကဲ့သို့အသုံးပြုခြင်းများကလည်း မလုံလောက်ပါဘူး။ Browser ဆိုတာ အင်တာနက်ကိုရောက်ဖို့ ပြုတင်းပေါက်တစ်ခုဖြစ်တဲ့အတွက် အခြားပြုတင်းပေါက်များလိုပဲ ဖွင့်လိုက်တာနဲ့ ကောင်းတဲ့အရာတွေရော၊ မကောင်းတာတွေရော ဝင်လာနိုင်ပါတယ်။ တစ်ခါတစ်ရံ အရမ်းနောက်ကျသွားတဲ့အထိခင်ဗျား မသိနိုင်တာတွေ တောင်ရှိနိုင်ပါတယ်။

Exercises

1.11 search engine များစွာရှိပါတယ် တစ်ချို့က တခြား search engine တွေမရှာနိုင်တဲ့ တစ်ဦးပိုင် database တွေကဲ့သို့ **(invisible web)** မခြင်နိုင်တဲ့ web တွေကိုရှာဖွေရန်ကောင်းမွန်ပါတယ်။ တစ်ချို့ကို ထူးချွန်တဲ့သုတေသနပြုသူတွေသုံးကြတယ်၊ တစ်ချို့က search engine တွေကိုခြေရာခံနိုင် ပါတယ်။ ဒါဆို၊ ခင်ဗျာအသုံးမပြုဖူးတဲ့ (သို့) ကြားဖူးတဲ့ search engine ၅ခုကို ရှာဖွေကြည့်ပါ။

1.12 အခြား search engine တွေကိုရှာဖွေနိုင်တဲ့ search engine တွေလည်းရှိပါတယ်။ ၎င်းတို့ကို **meta search engine** လို့ခေါ်ပါတယ်။ meta search engine တစ်ခုလောက် ရှာဖွေကြည့်ပါ။

1.13 "security and hacking" (quotation အမှတ်အသားတွေပါ ပါဝင်ပါတယ်) ကိုရှာဖွေပါ ပြီးတော့ ပထမဆုံးတွေ့ရှိတဲ့ အဖြေ ၃ခုကို မှတ်သားထားပါ။ quotation အမှတ်အသားတွေပါခြင်း၊မပါခြင်းက မည်သို့ကွဲပြားပါသလဲ?

1.14 စကားလုံးတစ်လုံး သို့ စကားစုတစ်ခု ကိုရှာဖွေခြင်းထက် အကြောင်းအရာတစ်ခုကို ရှာဖွေခြင်းကပိုခက်ပါတယ်။ ပြီးခဲ့တဲ့ လေ့ကျင့်ခန်းမှာ စကားစုတစ်ခုကို ရှာဖွေခဲ့ပြီးပြီဆိုတော့ အခု အတွေးအခေါ်တစ်ခုကို ရှာဖွေကြည့်ပါ။

ရှာဖွေရန်၊ **ခင်ဗျားရှာဖွေမယ့်အကြောင်းအရာမှာပါဝင်နိုင်မယ့်စကားစုကို စဉ်းစားကြည့်ပါ။** အကယ်၍ ခင်ဗျားက search engine ကို hacking အကြောင်း online မဂ္ဂဇင်းရှာဖွေစေချင်တယ်ဆိုရင် "a list of online magazines about hacking." ဆိုတဲ့စကားစုနဲ့တော့ အများကြီးမတွေ့နိုင်ပါဘူး။ အဲဒီအစား "ငါသည် hacking မဂ္ဂဇင်းရေးမယ်ဆိုရင် ပုံမှန်စာကြောင်းတွေက ဘာတွေဖြစ်နိုင် မလဲ?" တွေးကြည့်ဖို့လိုပါတယ်။

အောက်ပါစကားလုံးတွေ၊ စကားစုတွေကို search engine တစ်ခုမှာရိုက်ကြည့်ပြီး ဘယ်တစ်ခုက အကောင်းဆုံးရလာဒ်ကို ရှာတွေ့နိုင်တယ်ဆိုတာရှာဖွေကြည့်ပါ။

1. my list of favorite magazines on hacking
2. list of professional hacking magazines
3. resources for hackers
4. hacking magazine
5. magazines hacking security list resources

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

1.15 http://www.archive.org မှာ www.mozilla.org လို့ရိုက်ပြီး Mozilla ရဲ့ ရှေးအကျဆုံး website ကို အင်တာနက်မှတ်တမ်းမှာရှာဖွေကြည့်ပါ။

1.16 ယဿခု လေ့ကျင့်ခန်းအားလုံးစုပြီးလုပ်ကြည့်ပါ။ Netscape web browser version 1 ကို search engine နှင့် Internet Archive များအသုံးပြုပြီး ရှာပါ။ တွေ့လျှင် download လုပ်ပေးပါ။

Websites and Web Applications

de facto (လက်ဆင့်ကမ်း) စံနှုန်းက သတင်းအချက်အလက်တွေမျှပေးရန် web browser များမှာပါဝင်ပါတယ်။ web ပန်ဆောင်မှုတွေကို မျိုးတူစုကြည့်တဲ့အခါ web တိုင်းက website မဟုတ်ပါဘူး web application လည်းပါ ဝင်ပါတယ်။ web browser ကိုသုံးပြီး email တွေစစ်ခြင်း၊ သီချင်းတွေနားထောင်ခြင်း၊ ဗွီဒီယိုကြည့်ခြင်း တွေ ပြုလုပ်တဲ့အခါ "web application" တစ်ခုကို အသုံးပြုနေတာပဲဖြစ်ပါတယ်။

တစ်ခါတစ်ရံ web application တွေသုံးတဲ့အခါ အသုံးပြုခွင့်ရှိမှု (privileges) လိုအပ်ပါတယ်။ ဆိုလိုတာက အသုံးပြုရန် Login နာမည် နှင့် စကားဝှက်လိုအပ်ခြင်းဖြစ်ပါတယ်။ တရားဝင်အသုံးပြုခွင့်(access)ရှိခြင်းကို (privileges) ရှိခြင်းဟုခေါ်ပြီး web စာမျက်နှာတွေပြောင်းလဲပစ်ရန် hacking လုပ်ပြီးဝင်ရောက်သောအခါ access ရှိသော်လည်း တရားဝင်အသုံးပြုခွင့် (privileges) ရှိခြင်းမဟုတ်ပါဘူး။ အဲဒီနည်းနဲ့ ဆက်လက်အသုံးပြုရင်းနဲ့ တရားဝင်အသုံးပြုခွင့်ဖြစ်တဲ့နေရာတွေကို ဝင်ရောက်ခွင့်ပေးနိုင်တဲ့ ချိတ်ဆက်မှုတွေများစွာ မတော်တဆတွေ့ရှိနိုင်ပါလိမ့်မယ်။

ထိုကဲ့သို့ အရာတစ်ခုကိုရှာတွေ့တဲ့အခါ ၎င်းအချက်ကို website အုပ်ချုပ်ရေးမှူးတွေကို အကြောင်းကြားရန်မှာ ကောင်းမွန်တဲ့အလေ့အထ တစ်ခုဖြစ်ပေမယ့် website အုပ်ချုပ်ရေးမှူးတော်တော်များများက သူတို့မတောင်းဆိုပဲ အားနည်းချက်တွေသတင်းပေးခြင်းအပေါ် မနှစ်သက်ခြင်းများရှိတတ်တာကိုတော့ သတိထားပါ။

> အဲဒီweb အုပ်ချုပ်ရေးမှူးတွေကို အားနည်းချက်အကြောင်းကြားစာတွေ ရောင်းချရန်အတွက် ခင်ဗျားကိုယ် ခင်ဗျားကာကွယ်ရင်းနှီးအင်တာနက်ကိုပိုမိုလုံခြုံတဲ့နေရာအဖြစ်အသုံးပြုရန်အတွက်နာမည်ဝှက်ခြင်းပန်ဆောင် မှုအသုံးပြုရန် စဉ်းစားသင့်ပါတယ်။ (ဥပမာ - Tor (သို့) anonymous-remailers များစသည်ဖြင့်...)။ ဒါပေမယ့် အဲဒီ နာမည်ဝှက်အသုံးပြုခြင်းနည်းပညာ များမှာလည်း အားနည်းချက်တွေရှိ နေတတ်တာတော့ သတိပြုပါ။

Exercises

1.17 search engine ကိုအသုံးပြုပြီး လူတိုင်းကိုမှားယွင်းစွာ privilege ပေးထားတဲ့ website တွေကို ရှာဖွေပါ။ ထိုသို့ပြုလုပ်ရန် "directory listing" လို့ခေါ်တဲ့ ပါဝင်မှုတွေကိုစာရင်းလုပ်နိုင်ခြင်းပြုလုပ်ခွင့် ပေးထားတဲ့ folder တွေကို ကျွန်တော်တို့ရှာဖွေမှာပါ။ တကယ်တမ်းတော့ အသုံးပြုခွင့်မပေးထားသင့်တဲ့အရာတွေပါ။ ကျွန်တော်တို့Google command လှည့်ကွက်တွေကို http://www.google.com search box မှာ သုံးပြီးရှာဖွေမှာပါ။

```
allintitle:"index of" .js
```

အဲဒီရလဒ်တွေကို ဖတ်ကြည့်ပါ။ directory listing နှင့်တူတဲ့ရလဒ်တွေ တွေ့နိုင်ပါတယ်။ ယဿခုလို ရှာဖွေခြင်းကို Google Hacking လို့ခေါ်ပါတယ်။

1.18 အခြား document အမျိုးအစားတွေကို ထိုနည်းနှင့် ရှာဖွေနိုင်ပါသလား? .xls, .doc, .avi file များပါဝင်တဲ့ နောက်ထပ် directory listing သုံးမျိုးရှာဖွေပါ။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

1.19 "allintitle:" ကဲ့သို့ အခြား အသုံးပြုနိုင်တဲ့ရွေးချယ်နိုင်မှုတွေရှိပါသေးသလား? ခင်ဗျားဘယ်လို ရှာတွေ့ပါသလဲ?

Zines

E-zine လို လူသိများတဲ့ zine များက fanzine များမှဆင်းသက်လာတဲ့ ဂါသနာရှင်တွေ၊ တက်သစ်စ သတင်းစာ ဆရာတွေကထုတ်ဝေတဲ့ (စာဖတ်သူ ၁၀,၀၀၀) ခန့်အတွက်သာ အခမဲ့ထုတ်ဝေတဲ့ မဂ္ဂဇင်းတွေဖြစ်ပါတယ်။ Fanzine များကိုစာရွက်ပေါ်မှာရိုက်နှိပ်ထုပ်ဝေပါတယ်။ အင်တာနက်ပေါ်ကလူသိများတဲ့ "2600" (သို့) "Phrack" zine website တွေကိုအပျော်တမ်း၊ စေတနာ့ဝန်ထမ်း သတင်းစာဆရာတွေကရေးသားပြီး တစ်နည်းအားဖြင့် ထုတ်ဝေသူတွေက အဲဒီ zine တွေမှာပါဝင်တဲ့အချက်အလက်တွေနဲ့ နည်းပညာနှင့်မဆိုင်သော အမှားအယွင်းများကို ပြင်ဆင်ထားခြင်းမရှိတဲ့အင်တာနက်မဂ္ဂဇင်းတွေပဲဖြစ်ပါတယ်။ တစ်ခါတစ်ရံ ပြင်းထန်သော အသုံးအနှုန်း ဂေါ်ဟာရများသည် ထိစာပေအမျိုးအစားများနှင့် အကျွမ်းတဝင်မရှိသူများအဖို့ ထူးဆန်းဖွယ်ရာဖြစ်နေတတ်ပါသေးတယ်။

> Zine များမှာ အလွန်အစွဲကြီးသောအကြောင်းအရာ နှင့် အစီအစဉ်များပါဝင်ပြီး အလွန်အယူသီးခေါင်းမာလေ့ရှိကြပါတယ်။ zine သတင်းဆရာတွေက ကြော်ငြာထည့်ဝင်သူတွေ၊ မဂ္ဂဇင်းဖတ်သူတွေအကြိုက်လိုက်၍ ဂရုစိုက်ရန်မလိုကြသဖြင့် အကြောင်းကိစ္စသစများ၏ အဖက်ဖက်မှအမြင်များကို ဖော်ပြရန်၊ အတိုက်အခံလုပ်ရန် ရည်ရွယ်ပုံရှိပါသည်။

Exercises

1.20 အင်တာနက်မှာ hacking အကြောင်းအရာ zine သုံးခုရှာပါ။ ဘယ်လိုရှာတွေ့ပါသလဲ?

1.21 အဘယ်ကြောင့် အဲဒီအရာတွေကို zineတွေလို့ သတ်မှတ်ပါသလဲ? ၄င်းတို့ကို zine လို့ ခေါင်းစဉ်တပ်ထားတိုင်း zine မဟုတ်တာကို သတိရပါ။

Blogs

Blog ဆိုတာ zine တွေရဲ့မသိမသာ တိုးတက်ပြောင်းလဲမှုလို့ ယူဆနိုင်ပါတယ်။ Blog များမှာ zine တွေ၊ မဂ္ဂဇင်း တွေထက်မကြာခဏသတင်းအသစ်များဖြင့် ခေတ်မီအောင်ပြုလုပ်ခြင်းများရှိနေပြီး အလွန်တစ်ယူသန်သော အကြောင်းအရာများဖြင့် ဆက်နွယ်ထားတဲ့မျိုးတူအုပ်စုများကိုဖန်တီးထားမှုတွေပါဝင်ပါတယ်။

> အင်တာနက်မှာ Blog သန်းပေါင်းများစွာရှိပါတယ်၊ ဒါပေမယ့် အဲဒီအထဲကအနည်းငယ်သာရှင်သန်လျက်ရှိပါတယ်။ အဲဒီ Blog အားလုံးပေါ်မှာရှိတဲ့သတင်းအချက်အလက်တွေက မည်သို့ဖြစ်စေ အကြုံးဝင်လျက်ရှိနေပါသေးတယ်။

Exercises

1.22 အင်တာနက်မှာ hacking အကြောင်းblog သုံးခုရှာဖွေပါ။

1.23 မည်သည့်အဖွဲ့အစည်းတွေ၊ အုပ်စုတွေ ပါဝင်ပါသလဲ?

1.24 အဲဒီ blog တွေမှာ လုံခြုံရေး၊ ဥပဒေပြဋ္ဌာန်းချက် သို့မဟုတ် ပညာရေးအကြောင်းအရာတွေ တွေ့ရပါသလား?

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Forums and Mailing Lists

Forum နှင့် Mailing List တွေဆိုတာ ပါတီပွဲတစ်ခုမှစကားဝိုင်းများကို မှတ်တမ်းတင်ဖမ်းယူထားခြင်းကဲ့သို့ ဖွဲ့ဖြိုးသောအများဆိုင်ဆက်သွယ်ပြန်ကြားရေး တစ်ခုဖြစ်ပါတယ်။ အဲဒီမှာခင်ဗျားဖတ်ရှုသမျှအားလုံးကို အနည်းငယ်မေးခွန်းထုတ်၍ဖတ်ပါ။ ထိုစကားဝိုင်းတွေကမကြာခဏ ရည်ရွယ်ချက်ပြောင်းလဲတတ်ပြီး အဲဒီမှာပြောသမျှအားလုံးနည်းပါးက ကောလဟာလတွေဖြစ်ပြီး တစ်ချို့လူတွေကတော့ ပါလေရာလုပ်နေကြပါတယ်၊ တစ်ချို့က မီးတောက်စစ်ပွဲတွေဖြစ်နေကြပါတယ်။ ပြီးတော့ ပါတီပြီးဆုံးသွားတဲ့အခါ ဘယ်သူကဘာပြောခဲ့တယ်ဆိုတာ မည်သူတစ်ဦးတစ်ယောက်မှ သေချာစွာမမှတ်မိတော့ပါဘူး။ Forum နှင့် Mailling list တွေကလည်း ထိုနည်းလည်းပါပဲ အဘယ့်ကြောင့်ဆိုသော် အဲဒီမှာ လူတွေပါဂင်ပြောဆိုနိုင်တဲ့လမ်းများစွာရှိပြီး မမှန်ကန်တဲ့သတင်းတွေ၊ အလာပသလာပတွေ၊ လူသိသူသိမခံပုံစွာ တစ်စုံတစ်ယောက်ကဲ့သို့ဟန်ဆောင်ပြီး ပါဂင်ပြောဆိုနေကြသူတွေ ရှိကြလို့ဖြစ်ပါတယ်။ အကြောင်းအရာ ခေါင်းစဉ်တွေ လျှင်မြန်စွာပြောင်းလဲနေသောကြောင့် သတင်းအချက်အလက်အားလုံးရရှိနိုင်ရန် ထင်မြင်ချက်၊ ဂေဖန်ချက် ပေးခြင်းများအားလုံးကို ဖတ်ရန်အရေးကြီးပါတယ်။

မဂဿဂဇင်း၊ သတင်းစာ ထုတ်ဝေသူတွေက ၎င်းတို့ထုတ်ဝေသော မဂဿဂဇင်း၊ သတင်းစာ ဆောင်းပါးတွေကို အကြံပြုမှု၊ ဂေဖန်မှုများ ပေးနိုင်ရန် စီစဉ်ပေးထားသောနေရာတွေ နှင့် အကြောင်းအရာအားလုံးနည်းပါးမှာ forum တွေကို တွေ့နိုင်ပါတယ်။ အဘယ်ကြောင့်ဆိုသော် ထိုဆောင်းပါးကို မည်သူကမည်မျှနှစ်သက်နေပါစေ မနှစ်သက်သူ တစ်ချို့လည်းရှိနေမှာသေချာနေလို့ ၎င်း forum တွေက ဆောင်းပါးတစ်ခုပေါ်မှာ တစ်ခုထက်ပိုသော အမြင်တွေ ရရှိနိုင်ရန် တန်ဖိုးမဖြတ်နိုင်သောအရာတွေဖြစ်နေသောကြောင့်ဖြစ်ပါတယ်။

> အထူးအစီအစဉ်တွေအတွက် mailing list တွေ အများအပြားရှိနေပေမယ့် ရှာဖွေရန်ခက်ခဲပါတယ်။ တစ်ခါတစ်ရံ ခေါင်းစဉ်၊ အကြောင်းအရာ တစ်ခုချင်းနဲ့ ဆက်ဆံနေတဲ့ mailing list တွေကိုရရှိနိုင်ရန် အချက်အလက်များရှာဖွေစုဆောင်းခြင်းက အကောင်းဆုံးနည်းပညာဖြစ်ပါတယ်။

Hacker တစ်ယောက်အနေနဲ့ အရေးကြီးဆုံးသိဖို့အချက်က forum နှင့် mailing list တွေကို website နှင့် forum များပေါ်မှာပဲ တိုက်ရိုက်တွေ့နိုင်တာကြောင့် အဓိက search engine တွေကတဆင့် မရှာဖွေနိုင်ဘူး ဆိုတာပါပဲ။

Exercises

1.25 Hacker forum နှစ်ခုရှာဖွေပါ၊ ဘယ်လိုရှာဖွေတွေ့ပါသလဲ?

အဲဒီ website တွေရဲ့ အကြောင်းအရာတွေ၊ အထူးပြုမှုတွေ၊ ရပ်တည်မှုတွေကို ခင်ဗျားဆုံးဖြတ်နိုင်ပါသလား? အဲဒီ forum တွေထဲကအကြောင်းအရာတွေ က အဲဒီwebsite ရဲ့ရပ်တည်မှုနှင့် ကိုက်ညီမှုရှိပါသလား?

1.26 Hacking (သို့) လုံခြုံရေး ဆိုင်ရာ mailing list နှစ်ခုကိုရှာပါ။

အဲဒီ List တွေရဲ့ ပိုင်ရှင်ကဘယ်သူလဲ? အဲဒီ mailing list ထဲကအဖွဲ့ဝင်တွေကို ခင်ဗျားတွေ့နိုင်ပါသလား? (အဖွဲ့ဝင်စာရင်းကို ရရှိနိုင်ရန် အဲဒီ mailing list တွေကို ရေးခဲ့တဲ့ application တွေကို ပုံဖော်ကြည့် ပြီး အဲဒီ web မှာ ဖုံးကွယ်ထားတဲ့ command တွေကိုရှာဖွေရန် လိုအပ်နိုင်ပါတယ်။)

ဘယ် list တွေက ပိုမှန်ပြီး တစ်ယူသန်မှု ပိုနည်းမယ်လို့ မျှော်လင့်ပါသလဲ ၊ ဘာကြောင့်လဲ?

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Newsgroups - သတင်းအစုအဝေးများ

Newsgroups များသည် အချိန်ရှည်ကြာစွာ အနှံ့အပြားမှာလှည့်ပတ်တည်ရှိနေခဲ့ပါသည်။ World Wide Web (www) မဖြစ်ပေါ်ခင် newsgroups များတည်ရှိနေခဲ့ပါသည်။ Google က အဲဒီ newsgroups တွေဆီက မှတ်တမ်း(archive) အားလုံးကိုဝယ်ယူခဲ့ပြီး http://groups.google.com မှာ online တင်ဖေါ်ပြခဲ့ပါတယ်။ Newsgroup များက mailing list မှတ်တမ်းတွေပါ ဒါပေမယ့် mail တွေတော့မပါဝင် ပါဘူး။ လူတွေက website တစ်ခုမှာ ဝေဖန်ချက်တွေရေးနေတဲ့ အချိန်တိုင်းမှာ အဲဒီမှတ် တမ်းတွေမှာ တိုက်ရိုက်ဝင်ရေးနေသကဲ့သို့ ဖြစ်နေပါတယ်။ ၁၉၉၀ခုနှစ်အစောပိုင်းမှစ၍ နောက်ပိုင်းအချိန် တွေအထိ ရှိနေသမျှ ဝေဖန်ရေးသားချက် ပို့စ်တွေ အားလုံးကို အဲဒီ newsgroups မှတ်တမ်းတွေမှာ ပြန်လည်ရှာဖွေတွေ့နိုင်ပါတယ်။

> Web မှတ်တမ်းမော်ကွန်းတွေလိုပဲ မည်သူက အတွေးအခေါ်တစ်ခုကို စတင်တီထွင်ခဲ့တာလဲ (သို့) ထုတ်ကုန်တစ်ခုကို ဖန်တီးခဲ့တာလဲဆိုတာ ရှာဖွေရန် ၎င်း newsgroups မော်ကွန်းတွေကို အဓိကလိုအပ်ပါ တယ်။ ထို့အပြင် ၎င်းမှတ်တမ်းတွေက web စာမျက်နှာ တစ်ခုပေါ်က မထင်ရှားသောသတင်းအချက် အလက်တွေကိုရှာဖွေရန် အတွက်လည်း အသုံးဝင်ပါတယ်။

သတင်းအချက်အလက်တွေမျှဝေရန်အတွက် web တွေကအဓိကခေတ်ရေစီးကြောင်း ဖြစ်မလာသေးခင်မှာ newsgroups တွေကိုတွင်ကျယ်စွာအသုံးပြုခဲ့ပေမယ့် ယနေ့အချိန်မှာတော့ အနည်းငယ်တောင်အသုံးမပြုကြ တော့ပါဘူး။ မည်သို့ဖြစ်စေ blog တွေ forum တွေကဲ့သို့ web ဝန်ဆောင်မှုတွေက newsgroups တွေကို အစားထိုးနေရာယူလိုက်ကြတာပဲဖြစ်ပါတယ်။

Exercises

1.27 Google ရဲ့ groups ကိုသုံးပြီး ရှေးအကျဆုံး newsgroup မှ hacking အကြောင်းကိုရှာဖွေပါ။

1.28 newsgroups တွေကိုအသုံးပြုရန် အခြားနည်းလမ်း၊ application များရှိမရှိ ရှာဖွေပါ။

1.29 hacking အကြောင်းပါဝင်တဲ့ newsgroups ဘယ်နှစ်ခုရှာဖွေတွေ့ပါသလဲ?

1.30 လက်ရှိတည်ရှိနေသော မတူညီတဲ့ newsgroups များစာရင်းကိုရှာဖွေနိုင်ပါသလား?

Wikis - ဝီကီများ

Wikis တွေကတော့ အင်တာနက် မှာ တကယ့်အခုံဖွယ်ဖြစ်ရပ်တစ် ခု ဖြစ်ပါတယ်။ wikipedia (www.wikipedia.org) ကလူသိအများဆုံးwiki တစ်ခုဖြစ်ပေမယ့် အခြား wikiတွေ အများကြီးရှိပါသေးတယ်။ အခြား website တွေလိုပါပဲ wiki တွေက အဖွဲ့အစည်းတွေနဲ့ ဖွဲ့စည်းထားတာဖြစ်ပါတယ်။ wiki တွကို ဂါသနာ ရှင်တွေနဲ့ အရူးအမူးစွဲလန်းတတ်သူတွေက ပံ့ပိုးထားတာကြောင့် မမှန်ကန်ဘူးဆိုတဲ့အပြစ်တင်မှုတွေ မကြာခဏ တွေ့ရတတ်ပါတယ်။ ဒါပေမယ့် wiki တွေက စာအုပ်တွေထဲကအမှန်တရားတွေ၊ mailing lists တွေ၊ မဂ္ဂဇင်း တွေ စသည်တို့မှ ပါဝင်ဖေါ်ပြချက်တွေပါ။ ကျွမ်းကျင်သူတွေကပဲ ကြီးကျယ်တဲ့အတွေးအခေါ်ဖန်တီးမှုတွေ၊ မှန်ကန် တဲ့သတင်းတွေ ပြုလုပ်ထုတ်ဖေါ် နိုင်သူတွေမဟုတ်ဘူးဆိုတာ သိထားဖို့အရေးကြီးပါတယ်။ OSSTMM ကရည် ညွှန်းဖေါ်ပြထားသကဲ့သို့ပဲ အမှန်တရားတွေက ရှာဖွေတွေ့ရှိမှုတွေရဲ့ မထူးခြားတဲ့ စိတ်ကူးတွေနဲ့ ဆန်းစစ်အတည် ပြုချက်အယူအဆတွေရဲ့ သေးငယ်တဲ့အဆင့်တွေကနေ ပေါ်ထွက်လာတတ်တာပါ။ ထို့ကြောင့် wiki တွေက ပညာရှင်၊ ဂါသနာရှင် နှစ်မျိုးစလုံးအတွက် ကောင်းမွန်တဲ့ အရင်းအမြစ်တစ်ခုပဲဖြစ်ပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Wikis တွေက အကြောင်းအရာတစ်ခုရဲ့ ရှုထောင့်အမျိုးမျိုးကနေ ဆွေးနွေးဖေါ်ပြတဲ့အပြင် အချက်အလက်တွေ မည်သို့ အငြင်းပွားခံရတယ်၊ ချေပခံရတယ်၊ မွမ်းမံခံရတယ်၊ ပြောင်းလဲခံရတယ် ဆိုတာ ပြင်ဆင်ချက် စာရင်းမှ တဆင့်သိနိုင်ခွင့်ပေးပါတယ်။ အဲဒါကြောင့် ၎င်းတို့ကသတင်းအချက်အလက်တွေ တူးဖေါ်ရန် အကောင်းဆုံးနေရာဖြစ်ပါတယ်။

Exercises

1.31 "Ada Lovelace" ကိုရှာဖွေပါ။ wiki တွေကဖြေရှင်းချက်တွေ တွေ့ပါသလား?

1.32 Wikipedia ကိုသွားပြီး ထိုအချက်ကိုပဲထပ်ရှာပါ။ သူမအကြောင်း ဆောင်းပါးကိုကြည့်ပါ။ ထိုဆောင်းပါးက ရှေ့ကခင်ဗျားရှာဖွေမှုရလာဒ်တွေမှာပါ ပါခဲ့သလား?

1.33 Wikipedia စာမျက်နှာမှ edit တွေကိုစစ်ကြည့်ပါ ဘယ်လိုအရာတွေကိုပြင်ဆင်ထားလဲ? ပြောင်းလဲမှု ပြန်လည်ပြောင်းလဲမှု များရှိပါသလား? အခု ခင်ဗျားကြိုက်တဲ့ အဆိုတော် (သို့) သရုပ်ဆောင်ကို wkipedia မှာရှာကြည့်ပြီး ပြင်ဆင်ချက်တွေကို ဖတ်ကြည့်ပါ။ ကွဲပြားချက်ကို သတိထားမိပါသလား?

1.34 အခြား wiki site တွေကိုရှာကြည့်ပြီး အလားတူရှာဖွေဆန်းစစ်မှုတွေ ထပ်လုပ်ပါ။ ခင်ဗျားရဲ့ မူလ search engine မှာ wiki တွေမှာတွေ့ရတဲ့ ရလာဒ်နဲ့တူတာတွေကို တွေ့နိုင်ပါသလား?

Social Media - လူမှုဆက်သွယ်ပြန်ကြားရေး

ခင်ဗျား လူမှုဆက်သွယ်ရေး ကွန်ယက်တစ်ခုခု သို့မဟုတ် အများအပြားသုံးပါသလား? Hacker တစ်ယောက် အနေနဲ့တော့ ခင်ဗျားက ကာလတစ်ခုမှာခေတ်စားတဲ့ လူမှုဆက်သွယ်ရေးကွန်ယက်တစ်ခုကို ကောင်းစွာဂရုစိုက်ကြည့်ဖို့လိုပါတယ်။ များသောအားဖြင့် အရင်လိုမထင်ရှားတော့တဲ့ လူမှုကွန်ယက်တွေမှာလည်း အချက်အလက်တွေကျန်ရှိနေပါသေးတယ်။

ကျွန်တော်တို့အကြောင်းသတင်းအချက်အလက်တွေရဲ့ကြီးမားတဲ့သိုလှောင်ရုံတွေရှိနေတယ်လို့ဆိုလိုတာဖြစ်ပါတယ်။ အဲဒီသိုလှောင်ရုံတွေထဲကအများစုကိုအသုံးမပြုတော့ပေမယ့် ထာဝရတည်ရှိနေပါတယ်။

လူမှုကွန်ယက်တွေမှာပုံမှန်အားဖြင့် စိတ်ဝင်စားမှုအသီးသီးရဲ့ အုပ်စုတွေ၊ အုပ်စုကွဲတွေရှိပါတယ်။ ကျွမ်းကျင်ပညာရှင်အကြောင်းများဖြင့်ဖွဲ့စည်းထားတဲ့နေရာတွေမှ ၁ cyber လုံခြုံရေးအဖွဲ့တွေ ရှိတတ်ပြီး၊ လျှို့ဝှက်ချက်များဖြင့် ဖွဲ့စည်းထား သောအဖွဲ့အစည်းများမှာ Hacker တွေရှိတတ်ပါတယ်။ ကျွမ်းကျင်ပညာရှင် site တွေမှာ လူတိုင်းနာမည်အစစ်တွေသုံးရန်လိုအပ်ပြီး Hackersite တွေမှာတော့ မလိုအပ်ပါဘူး။

အရေးကြီးဆုံးအချက်ကတော့ လူမှုဆက်သွယ်ရေးကွန်ယက်တွေမှာ ခင်ဗျားနာမည်အစစ်သုံးသလား?"အစားထိုး" မှတစ် ခု (Handle) ကိုသုံးသလား? ပြီးတော့ခင်ဗျားရဲ့ အဲဒီအစားထိုးမှကနေတဆင့် ခင်ဗျားနာမည်အစစ်ကို ခြေရာခံနိုင်သလား? ဆိုတာတွေပါပဲ။ လူအများစုကသူတို့ Handle တွေမှာ သူတို့နာမည်အစစ်၊ ကျောင်း၊ နေရပ်လိပ်စာ၊ မြို့၊ အလုပ်အကိုင်တွေ မတင်သင့်ဘူးဆိုတာကို သေချာသဘောမပေါက်ကြပါဘူး။ အကယ်၍ အခြား Hacker တစ်ဦးက ခင်ဗျား Handle ကို Doxs (အရှက်ရစေရန် ရည်ရွယ်၍ hack ခြင်း)ပြုလုပ်ခဲ့လျင် အဲဒီအမှားသေးလေးတွေကြောင့် ခင်ဗျားဘယ်သူဆိုတာ ထို hacker က အလွယ်လေးရှာဖွေတွေ့ရှိနိုင်ပါလိမ့်မယ်။ ခင်ဗျားက ခင်ဗျားကိုယ်ခင်ဗျား ဖုံးကွယ်ဖို့ Handle သုံးတာဆိုရင် ထိုအချက်ကိုဂရုစိုက်ပါ ပြီးတော့ခင်ဗျား handle တွေ အများအပြားရှိနေရင်လည်း မရှုပ်ထွေးစေရန်ဂရုစိုက်ပါ။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Exercises

1.35 ခင်ဗျားကိုယ်ခင် ဗျား ရှာဖွေပါ။ ရလဒ်တွေရရှိပါသလား၊ အဲဒီရလဒ်တွေက တကယ်ခင်ဗျားလား၊ လူမှုကွန်ယက် site တွေကပဲရှာတွေ့တာလား?

1.36 ခင်ဗျားသုံးတဲ့ လူမှုကွန်ယက် site ကိုသွားပြီး Login မလုပ်ပဲခင်ဗျားကိုယ်ခင်ဗျားအပြင်လူအနေနဲ့ ထပ် ရှာဖွေပါ။ ဘာတွေရှာဖွေတွေ့ ပါသလဲ?

1.37 ခင်ဗျားသူငယ်ချင်းတွေရဲ့ လူမှုကွန်ယက် site တွေကိုသွားပါ၊ Login မလုပ်ပဲ ၎င်းတို့ကိုရှာဖွေပါ။ ဘာတွေရှာဖွေတွေ့ ပါသလဲ?

Chat

Chat ဆိုတာ **Internet Relay chat (IRC)** နှင့် **Instant Messaging (IM)** ကဲ့သို့ အရာတွေဖြစ် ပြီး ဆက်သွယ်မှုပြုရန် ခေတ်စားတဲ့နည်းလမ်းတွေပါ။

> လေ့လာဆန်းစစ်မှု ရင်းမြစ်တစ်ခုအရတော့ chat တွေကအလွန်ပြောင်းလဲဖြစ်တည်နေကြပါတယ်၊ အဘယ့် ကြောင့်ဆိုသော် ၎င်းတို့ကိုအသုံးပြုပြီး အချိန်နှင့်အမျှ လူအသီးသီးတို့ ဆက်သွယ်နေကြလို့ပဲဖြစ်ပါတယ်။ အချို့ကရင်းနှီးခင်မင်စွာ၊ အချို့ကရိုင်းပြစွာ၊အချို့ကစိတ်မဆိုးစတမ်းစနောက်လျက်၊ အချို့ကအနာသတရာယ်ရှိစွာ လိမ်လည်လျက်၊ အချို့ကထက်မြက်စွာ၊ အချို့က အသိပညာတွေမျှဝေလျက်၊ အချို့ ကတော့ မူမမှန်စွာ ဆက်သွယ်ပြောဆိုလျက် ရှိကြသဖြင့် ဘယ်သူကဘာဆိုတာ သိဖို့ရန် အလွန်ခက်ခဲပါတယ်။

မည်သို့ဖြစ်စေ ခင်ဗျားက အုပ်စုတစ်ခုနဲ့ အပေးအယူမျှသွားတာနှင့် အဲဒီအုပ်စုမှာခင်ဗျားပါဝင်သွားပါတယ်။ ခင်ဗျား သိချင်တာမှန်သမျှမေးမြန်းပြီး ခင်ဗျားယုံကြည်နိုင်မယ့်သူဆီကနေ လေ့လာခွင့်ရမှာဖြစ်ပါတယ်။ နောက်ဆုံးမှာ တော့ အသစ်စက်စက် hacking exploit တစ်ခုကို အသုံးပြုခွင့်ရရှိနိုင်ပါတယ်၊ ပြီးတော့ခင်ဗျားကိုယ်ပိုင် ဗဟု သုတ တွေကိုရှေ့ဆက်နိုင်မှာဖြစ်ပါတယ်။ (အသစ်စက်စက် hacking exploit ဆိုတာ zero day (ယဿခုလေး တင်ရှာဖွေတွေ့ရှိမှု)) လို့လည်းသိနိုင်ပါတယ်။

Exercises

1.38 instant messaging program သုံးခုရှာပါ။ ၎င်းတို့ကို ဘယ်အချက်က ကွဲပြားစေသလဲ၊ ၎င်းတို့အားလုံး ကို တစ်ဦးနှင့်တစ်ဦး စကားပြောရန်သုံးနိုင်သလား?

1.39 IRC ဆိုတာဘာလဲ ဘယ်လိုချိတ်ဆက်နိုင်သလဲ? ရှာဖွေပါ။ ISECOM ရဲ့ channel တွေမှာ ဘယ် ကွန်ယက်တွေပါဝင်တယ်ဆိုတာ ဖော်ထုတ်နိုင်ပါသလား။ ခင်ဗျား ကွန်ယက်တစ်ခုနှင့်ဆက်မိတာနဲ့ ဘယ်လို isecom-discuss channel မှာဘယ်လိုပါဝင်ပါသလဲ?

1.40 IRC မှာ ဘယ် channelတွေပါဝင်တယ် ဆိုတာဘယ်လိုသိနိုင်ပါသလဲ? လုံခြုံရေး channel နှင့် hacker channel သုံးခုစီကို ရှာဖွေပါ။ အဲဒီ channel တွေကို ခင်ဗျားဝင်လို့ရပါသလား? အဲဒီမှာရှိသူ တွေက လူတွေလား bot တွေလား?

P2P - (မျိုးတူ မှ မျိုးတူ)

Peer to Peer ကို P2P လို့ခေါ်ပြီး ၎င်းက အင်တာနက်အတွင်းမှာရှိတဲ့ကွန်ယက်တစ်ခုဖြစ်ပါတယ်။ ကွန်ပြူ တာတွေကို (ဗဟိုချိတ်ဆက်မှုဝန်ဆောင်မှုပေးသော Computer) Central Server မှတဆင့်ချိတ်ဆက်တဲ့ ပုံမှန်

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Client/Server (ဝန်ဆောင်မှုခံယူသူ/ဝန်ဆောင်မှုပေးသူ) စနစ်နှင့် မတူပဲ P2P ကွန်ယက်အတွင်းက ကွန်ပြူတာတွေက တစ်လုံးနှင့်တစ်လုံးတိုက်ရိုက်ဆက်သွယ်မှုပြုလုပ်နိုင်ပါတယ်။ လူအများစုက P2P ကိုအင်တာနက်မှ mp3 သီချင်းများရယူရန်၊ လိုင်စင်မဲ့ဇာတ်ကားများရယူရန် လူသိနည်းတဲ့ Napster မှဆက်သွယ်မှုပြုလုပ်ပါတယ်။အခြား P2P ကွန်ယက်တွေများစွာလည်းရှိပါသေးတယ်။ သတင်းအချက်အလက်တွေလဲလှယ်ရန်နှင့်၊ မျှဝေဖြန့်ချီထားသော သတင်းအချက်အလက်တွေ အပေါ်မှာလေ့လာဆန်းစစ်မှုတွေကို စီမံကြီးကြပ်ရန်ရည်ရွယ်ချက်နှစ်မျိုးလုံးအတွက်P2P ကိုသုံးကြပါတယ်။

P2P ရဲ့ ပြဿနာကတော့ အဲဒီကွန်ယက်ပေါ်မှာ မည်သည့်အရာမဆိုရှာဖွေနိုင်ပေမယ့် အချို့အရာတွေကတရားဝင်ဖြစ်နေခြင်း၊ အချို့အရာတွေကတရားဝင်သော်လည်း ထိုအရာတွေကိုဖန်တီးခဲ့တဲ့ကုမ္ပဏီတွေကအခကြေးငွေ ရယူရန် ဆန္ဒဒဏ်ရှိနေသေးခြင်းတွေပဲဖြစ်ပါတယ်။

> အဲဒီကာလမှာ အဲဒီပါဝင်မှုတွေကို download လုပ်ရန်အသုံးပြုသွားတဲ့အင်တာနက်လိုင်းပိုင်ရှင်က တာဝန်ရှိမရှိ (သို့) ရဲတွေက download လုပ်သွားသူကို တကယ်ဖမ်းမဖမ်း ဆိုတဲ့အချက်အပေါ်မှာ ညှိနှိုင်းမှုသိပ်မရှိပါဘူး။ ထိုအချက်က ကားတစ်စီးကိုဒုစရိုက်မှုလုပ်ရာမှာအသုံးပြုခံရပြီး ပြုလုပ်သူမဟုတ်တဲ့ ကားပိုင်ရှင်က ထောင်ထဲသွားရမယ်လို့ပြောနေသလိုဖြစ်နေပါတယ်။ အင်တာနက်ဥပဒေက ယဉ်သုအချိန်မှာ မျှတမှု မရှိတဲ့အတွက် သတိကြီးကြီးထားပါ။

ခင်ဗျားက မူပိုင်ခွင့်ရှိတဲ့ပိုင်ဆိုင်မှုကို စွန့်စားသဖြင့် download လုပ်သူဟုတ်သည်ဖြစ်စေ၊ မဟုတ်သည်ဖြစ်စေ P2P ကွန်ယက်တွေက သတင်းအချက်အလက်တွေရှာဖွေရန် အရေးပါသောအရင်းအမြစ်ဖြစ်နိုင်သလားဆိုတာ မေးရန် ပင်မေးခွန်းမရှိပါဘူး။ သေချာမှတ်သားပါ ၊ P2P ကွန်ယက်မှာ တရားဝင်ဆိုတာမရှိပါဘူး အဲဒီနေရာတွေမှာ များပြားတဲ့ လိုင်စင်တွေနဲ့ အခမဲ့ဖြန့်ဝေထားတဲ့ ဖိုင်တွေအများအပြားရှိနေပြီး အဲဒီနေရာမှာ မရှိသင့်တဲ့အချက် အလက်တွေလည်းရှိနေပါတယ်။ P2P ကွန်ယက်တွေကို အသုံးပြုရန်မကြောက်ရွံ့ပါနဲ့ ဒါပေမယ့် အနဿတရာယ်ဖြစ်နိုင် တဲ့ အရာတွေနဲ့ ခင်ဗျား download လုပ်မယ့်အရာတွေကိုတော့ သတိထားပါ။

Exercises

1.41 ကျော်ကြားတဲ့ P2P ကွန်ယက်သုံးခုနဲ့ အသုံးများတဲ့သုံးခုက ဘာတွေလဲ? တစ်ခုချင်းစီက ဘယ်လိုအလုပ်လုပ်သလဲ၊ ၎င်းတို့ကိုသုံးရန် ဘယ် ပရိုဂရမ်တွေ လိုအပ်သလဲ?

1.42 အဲဒီ P2P ကွန်ယက်တွေရဲ့ protocol တွေကိုလေ့လာပါ၊ ၎င်းဘာလုပ်သလဲ ပြီးတော့ download ပိုမြန်စေရန် ၎င်းကဘယ်လို လုပ်ဆောင်သလဲ?

1.43 "download linux" ဆိုတဲ့ စကားလုံးကို ရှာပါ၊ P2P ကိုသုံးပြီး Linux ရဲ့ ဖြန့်ဝေမှုတွေ (သို့ distro) တွေကို download လုပ်နိုင်ပါသလား?

Certifications - အသိမှတ်ပြုလက်မှတ်များ

OSSTMM ရဲ့ Security Tester (လုံခြုံရေးစမ်းသပ်သူ) နှင့် Security Analyst (လုံခြုံရေး စိစစ်သူ) အသိမှတ်ပြုလက်မှတ်တွေ Hacker ရောင်စုံ အသိမှတ်ပြုလက်မှတ်တွေ၊ "best-practices" အကောင်းဆုံးလေ့ကျင့်မှုများအပေါ်မှာအခြေခံတဲ့ အသိမှတ်ပြုလက်မှတ်တွေ စသည်ဖြင့်ရှိပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

> အဲဒီလက်မှတ်တွေကိုမည်သည့်အသက်အရွယ်မှာမဆိုရယူနိုင်တာကြောင့်၊ အဲဒီလက်မှတ်တွေရဖို့ကောလိပ်ဘွဲ့တွေတက်နေဖို့မလိုတာကြောင့်၊ အဲဒီလက်မှတ်တွေက ခင်ဗျားကို လိုချင်သူများတဲ့သူ ဖြစ်လာရန် ထောက်ပံ့ပေးနိုင်တာကြောင့် ခင်ဗျားအသိမှတ်ပြုလက်မှတ်တွေရယူရန်ဂရုစိုက်တာဖြစ်ပါ တယ်။

အကောင်းဆုံးလေ့ကျင့်မှုများက ို နောက်တစ်မျိုးအနေန ` ့ "လူတိုင်း ယဿခုဘာလုပ်နေကြလဲ" လို့ခေါ်ဆိုနိုင်တာကြောင့်၊ ၎င်းကိုအခြေခံတဲ့ အသိမှတ်ပြုလက်မှတ်ရဲ့ ပြဿဿနာက မတည်မြဲခြင်းဖြစ်ပါတယ်။

သုတေသန အခြေခံတဲ့လက်မှတ်တွေကတော့ လူတွေနဲ့စနစ်သဘောတရားတွေရှိနိုင်ပြီး ထပ်တလဲလဲ ပြုလုပ်နိုင်သော သုတေသနအချက်တွေပေါ်မှာအခြေခံပါတယ်။ ကျွန်တော်တို့ ပင်မအဖွဲ့အစည်း ISECOM ကတော့ ပြောဖို့မလိုအောင် သုတေသန အခြေခံသော အသိမှတ်ပြုလက်မှတ် (research-based certification) အခွင့်ဖြင့် လောကထဲကို အံဝင်ခွင်ကျ ဆင်းသက်လာတဲ့အဖွဲ့အစည်းဖြစ်ပါတယ်။ ISECOM ကပဲဖြစ်ဖြစ် အခြားဘယ်ကဖြစ်ဖြစ် ကျွမ်းကျင်မှုကို အခြေခံသော (skill-based)၊ စိစစ်မှုကို အခြေခံသော (analysis-based)၊ ဗဟုသုတကြွယ်မှုကို အခြေခံသော အသိမှတ်ပြုလက်မှတ်တွေကို ရှာဖွေရယူပါ ဒါမှ ခင်ဗျားလေ့လာသင်ယူထားပါတယ်လို့ပြောတဲ့အရာတွေကို တကယ် တတ်မြောက်ကြောင်းသက်သေခံပြနိုင်မှာဖြစ်ပါတယ်။ ခင်ဗျားသက်သေပြဖို့ လိုလာတဲ့အခါ ထိုထောက်ခံချက်လက်မှတ်တွေက အသုံးဝင်လာပါလိမ့်မယ်။

Seminars

ဆွေးနွေးပွဲတွေကိုတက်ခြင်းသည် သီအိုရီတွေကိုအသေးစိတ် ရှင်းလင်းမှုများကြားသိနိုင်ရန်၊ လက်တွေ့ကျွမ်းကျင်မှုများကိုမြင်တွေ့နိုင်ရန် အကောင်းဆုံးနည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ ထုတ်ကုန်အသားပေးပြုလုပ်တဲ့ဆွေးနွေးပွဲတွေဖြစ်နေပြီး ၎င်းတို့ကရောင်းချဖို့ပဲ ရည်ရွယ်တယ်ဆိုတာ သိနေရင်တောင်မှ အဲဒီထုတ်ကုန်ကို ဘယ်လိုရည်ရွယ်ချက်နဲ့သုံးကြတယ်ဆိုတာသိနိုင်ရန်တက်သင့်ပါတယ်။

အကယ်၍ Hacker High School Seminars တွေကို နေရာများစွာမှာ ပြုလုပ်နိုင်ပြီး ရရှိနိုင်တဲ့သင်ခန်းစာတွေကိုပြောကြားနိုင်တယ်ဆိုတာ မဖေါ်ပြခဲ့ရင် ကျွန်တော်တို့လည်းပေါ့လျော့နေနိုင်ပါတယ်။ အဲဒီဆွေးနွေးပွဲတွေမှာ တကယ့် Hackerတွေက ကျောင်းသား၊သူတွေကို hacking အကြောင်းနှင့် Hacker ဖြစ်နိုင်ရန်အကြောင်းများကို အဆို၊ အကောင်း အမြင်နှစ်မျိုးလုံးနဲ့ ဆွေးနွေးခြင်းများပါဝင်ပြီး Hacker အစစ်တွေက Hacker Profiling Project မှာဘာတွေကိုလေ့လာဆန်းစစ်ကြတာလဲ၊ ဘယ်သူတွေက Hacker တွေဖြစ်ပြီး၊ ဘာလို့ Hack ကြတာလဲဆိုတာတွေကို ရှင်းလင်းစွာသိမြင်နိုင်စေမှာပါ။ (Hacker Profiling Project ဆိုတာ နိုင်ငံအဖွဲ့အစည်းတွေနဲ့ ပူးပေါင်းဆောင်ရွက်ခြင်း စီမံကိန်းတစ်ခုဖြစ်ပါတယ်)။ သူတို့က hacking ဆိုတာအမြဲတမ်း မကောင်းတဲ့အရာမဟုတ်ဘူးဆိုတာ နှင့် Hacking ရဲ့ကောင်းမွန်မှုတွေကို ရှင်းလင်းဆွေးနွေးကြပါလိမ့်မယ်။

ခင်ဗျားနားလည်နိုင်ရန် ကျွန်တော်တို့ ကူညီနိုင်တဲ့ စွမ်းအားကြီးတဲ့တစ်ခုထဲသောအရာက hacker တစ်ယောက်လိုထက်မြက်စွာ စူးစမ်းသိလိုစိတ်နှင့် လုပ်ရည်ကိုင်ရည်ရှိမှုဖြစ်ပါတယ်။ hacker တွေကသူတို့ကိုယ်သူတို့ကိုယ်တိုင် မည်သို့သင်ကြားရမယ်ဆိုတာသိတာကြောင့် သူတို့လုပ်ဆောင်မှုတွေမှာအောင်မြင်မှုရကြပါတယ်။ သူတို့က ရှိသမျှသင်ခန်းစာတွေကိုကျော်လွန်အောင်လေ့လာပြီး ရှေ့ဆက်ဖို့လိုအပ်တဲ့အရည်အချင်းတွေ တတ်မြောက်အောင် သင်ယူကြပါတယ်။

ခင်ဗျားမိဘတွေနဲ့၊ သင်ခန်းစာပို့ချသူတွေကို မည်ကဲ့သို့ကူညီမှုတွေပေးရမလဲဆိုတာ လေ့လာရန်နှင့်၊ ခင်ဗျားပတ်ဝန်းကျင်ကသင်တန်းတွေမှာ Hacker High School သင်ခန်းစာတွေ မည်ကဲ့သို့ စတင်ရမလဲဆိုတာ လေ့လာရန်တိုက်တွန်းဖို့ ခင်ဗျားကိုဖိတ်ခေါ်ပါတယ်။ ISECOM ကိုဆက်သွယ်ပြီး အသေးစိတ်စုံစမ်းနိုင်ပါတယ်။

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Further Study - ရှေ့ဆက်လေ့လာရန်

အခုတော့ research ပြုလုပ်ခြင်းမှာ ဆရာတစ်ပါး ဖြစ်လာအောင် လေ့ကျင့်သင့်ပါပြီ။ ခင်ဗျားကျွမ်းကျင်လာလေ လေ အချက်အလက်တွေမြန်မြန်စုဆောင်းနိုင်လေလေဖြစ်ပြီး မြန်ဆန်စွာလေ့လာနိုင်လေလေဖြစ်မှာပါ။ ဆိုးဝါးတဲ့ မျက်လုံးတွေကို အမြင်ကျယ်စေဖို့တော့ဂရုစိုက်ပါ၊ သတင်းတိုင်းကအမှန်မဟုတ်လို့ဖြစ်ပါတယ်။

> လူတွေ ဘာကြောင့်လိမ်နေကြလဲ၊ ကောလဟာလပုံပြင်တွေ အမြဲတည်ရှိနေစေခြင်း၊ မရိုးသားမှု၊မမှန်ကန်မှုတွေ ရှိနေခြင်း တွေမှာ ငွေကြေးတွေ ပါဝင်ပက်သက်နေသလား၊ အမှန်တရားကဘယ်ကလာတာလဲ၊ အရေးကြီးဆုံးကဘာလဲ ဆိုတာတွေ ကိုယ့်ကိုယ်ကို ပြန်မေးဖို့ အမြဲသတိရပါ။

Hacking အားလုံးကဲ့သို့ သုတေသနပြုခြင်းက နယ်ပယ်တစ်ခုအနေနဲ့ပါဝင်ပါတယ်။ (အပိုင်းကိန်း၊ ရာခိုင်နှုန်း၊ ဒဿဿသမ စတဲ့.) သခဿသဿဂျာကဲ့သို့ ကိန်းဂဏန်းတွေမြင်တဲ့အခါ ထိုဆန်းစစ်လေ့လာခြင်းက တကယ့်ကိုအရေးကြီးပါတယ်။ နယ်ပယ်တစ်ခုကဘယ်မှာဖြစ်မှားလဲဆိုတာ ၁ မြင်နိုင်ရန်၊ အဲဒီနယ်ပယ်ကို အသုံးပြုနိုင်တယ်ဆိုတာနားလည်ရန် အမြဲ တမ်းကြည့်နေပါ။ ခင်ဗျားသိတဲ့သာမန်နေရာဖြစ်တဲ့ နိုင်ငံရေး၊ ဒုစရိုက်မှု၊ ကျန်းမာရေး စာရင်းတွေက နိုင်ငံတစ်ခု ရဲ့ တစ်စိတ်တစ်ဒေသပဲ ဖြစ်ပါတယ်၊ အဘယ်ကြောင့်ဆိုသော် မြို့တစ်မြို့မှာရှိတဲ့ လူ ၂၀၀ ရဲ့ ၁၀% အပေါ်သက် ရောက်မှုဖြစ်ခြင်းက နိုင်ငံရဲ့ သဒ၀% အပေါ်သက်ရောက်တယ်လို့ မပြောနိုင်သောကြောင့်ဖြစ်ပါတယ်။ ထို့ကြောင့် သတင်းတစ်ခုကို ဘယ်လိုရှာတယ်ဆိုတာသာမက မည်သို့ဖတ်တယ်ဆိုတာတွေကို သပ်သပ်ရပ်ရပ် ဆောင်ရွက်ပါ။ သတင်းတစ်ခုရဲ့ နယ်ပယ်ကို ပုံဖော်ကြည့်ခြင်းက အမြဲတမ်း ကြီးမားတဲ့ပြောင်းလဲမှုကို ဖြစ်စေပါတယ်။

ခင်ဗျားကို Hacker High School စီမံကိန်းအတွက် ပိုမိုပြည့်စုံတဲ့ researcher တစ်ဦးဖြစ်စေဖို့ အောက်ပါ အကြောင်းရာများဖြင့် ကူညီပေးထားပါတယ်...

- Meta Search
- The Invisible Web
- Google Hacking
- How Search Engines Work
- The Open Source Search Engine
- The Jargon File
- OSSTMM
- ISECOM Certifications:
  - OPST (OSSTMM Professional Security Tester)
  - OPSA (OSSTMM Professional Security Analyst)
  - OPSE (OSSTMM Professional Security Expert)
  - OWSE (OSSTMM Wireless Security Expert)
  - CTA (Certified Trust Analyst)
  - SAI (Security Awareness Instructor)

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2012, ISECOM.
www.isecom.org - www.osstmm.org - www.hackerhighschool.org - www.badpeopleproject.org - www.osstmmtraining.org

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

Creative Commons 3.3 Attribution-Non-Commercial-NoDerivs 2012, ISECOM