

এভাইডিং আইডিএস, ফায়ারওয়াল এন্ড হানিপটস


এই অধ্যায়ে আমরা যে বিষয়গুলো নিয়ে আলোচনা করবো-

- আইডিএস, ফায়ারওয়াল এন্ড হানিপটস কি?
- কিভাবে আইডিএস, ফায়ারওয়াল এন্ড হানিপটসকে বোকা বানানো যায়?
- আইডিএস, ফায়ারওয়ালকে বোকা বানালেও কিভাবে হ্যাকারকে প্রতিরোধ করা যায়

আইডিএস

আইডিএস হলো ইন্ট্রুশন ডিটেকশন সিস্টেম। যার মাধ্যমে জানা যায় কে কে আমার সিস্টেমে প্রবেশ করার চেষ্টা করছে।

Snort Rules



- Snort's rule engine enables **custom rules** to meet the needs of the network
- Snort rules help in differentiating between **normal Internet activities** and **malicious activities**
- Snort rules must be contained on a **single line**, the Snort rule parser **does not handle rules on multiple lines**
- Snort rules come with two logical parts:
 - **Rule header:** Identifies **rule's actions** such as alerts, log, pass, activate, dynamic, etc.
 - **Rule options:** Identifies rule's **alert messages**

Example:

```
Rule Protocol      Rule Port
  ↓                ↓
alert tcp any any -> 192.168.1.0/24 [111] content: "|00 01 86 a5|"; msg: "mountd access")
```

Rule Action Rule Format Direction Rule IP address Alert message

ফায়ারওয়াল

ফায়ারওয়াল দুই ধরনের হয়ে থাকে। সফটওয়্যার ফায়ারওয়াল আর হার্ডওয়্যার ফায়ারওয়াল। ফায়ারওয়াল দিয়ে সিস্টেমে ইনকামিং এবং আউটগয়িং প্যাকেটগুলোকে ফিল্টার করা যায়।

Firewall: Comodo Firewall



- Keeps you updated on all **suspicious files**
- Prevention-based technology **stops viruses**
- Automatic updates for the most **current protection**



হানিপটস

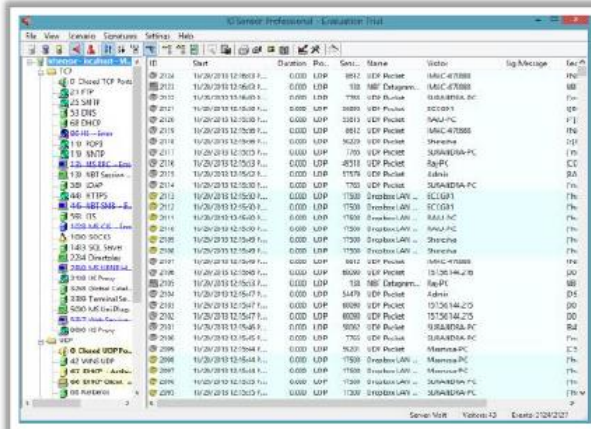
হানিপটসগুলো ব্যবহার করা হয় হ্যাকারকে বোকা বানানোর জন্য। হানিপটস হলো, মনে করেন আপনার নেটওয়ার্কে একটি রাউটার আছে কিন্তু আপনার নেটওয়ার্কে দশটি রাউটার দেখাবে। বাকি নয়টি রাউটারই হলো হানিপটস। সুতরাং হ্যাকার যখন হ্যাক করতে আসবে তখন সে যেকোন একটি ফেইক রাউটারে প্রবেশ করে বসবে। এর ফলে হ্যাকার তো আমার রাউটার এর কোন তথ্য কালেক্ট করতে পারলই না বরং হ্যাকার এর তথ্য আমরা কালেক্ট করে নিলাম।

HoneyPot Tools: KFSensor and SPECTER

CEH
Certified Ethical Hacker

KFSensor

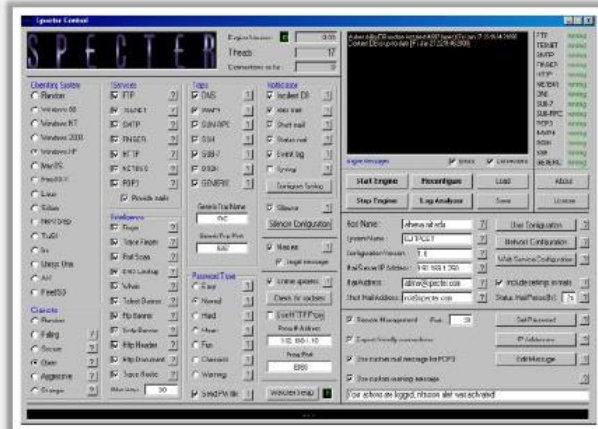
KFSensor is a **host-based** Intrusion Detection System (IDS) that acts as a honeypot to attract and detect hackers and worms by **simulating vulnerable system services and Trojans**



<http://www.keyfocus.net>

SPECTER

SPECTER is a smart **honeypot-based** intrusion detection system that offers common **Internet services** such as SMTP, FTP, POP3, HTTP, and TELNET which appear perfectly normal to the attackers but in fact are traps



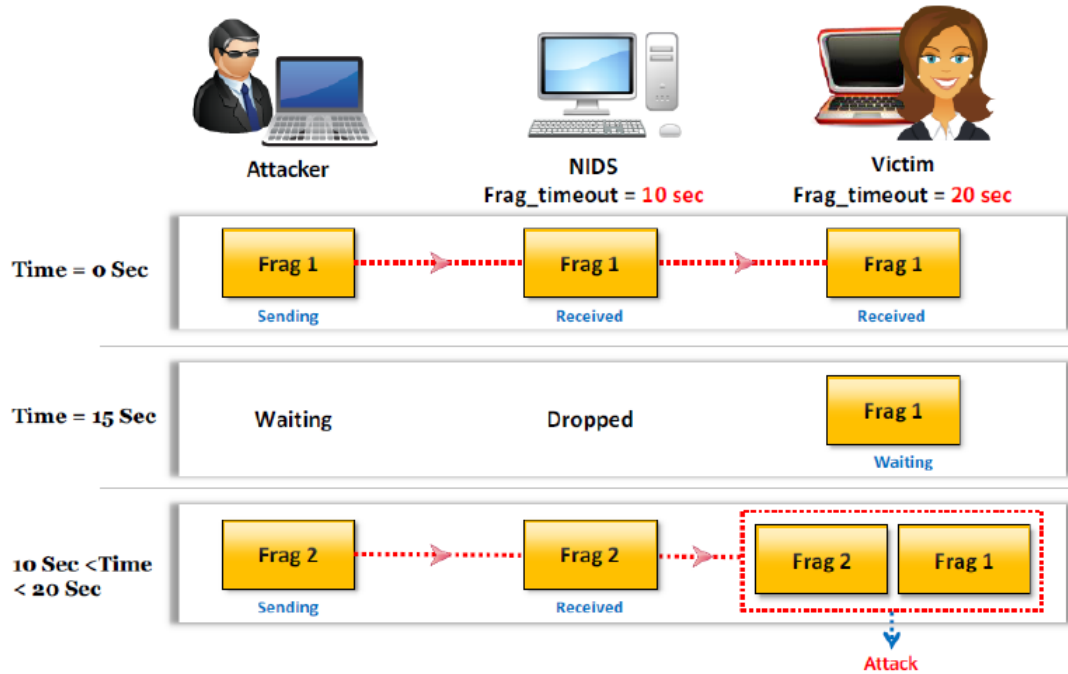
<http://www.specter.com>

কিভাবে আইডিএসকে বোকা বানানো যায়?

আইডিএস বা ইন্ট্রুশন ডিটেকশন সিস্টেমকে বলা দেওয়া কি ধরনের প্যাকেট আসলে ডিটেকট করবে। সুতরাং হ্যাকাররা যখন জানতে পারে এখানে ইন্ট্রুশন ডিটেকশন সিস্টেম রয়েছে তখন হ্যাকাররা প্যাকেটগুলো ভেংগে ছোট ছোট করে সেভ করে ফলে ইন্ট্রুশন ডিটেকশন সিস্টেম তা ধরতে পারে না। এই কাজটি হ্যাকাররা খুব সহজেই করতে পারে।

Fragmentation Attack (Cont'd)

CEH
Certified Ethical Hacker



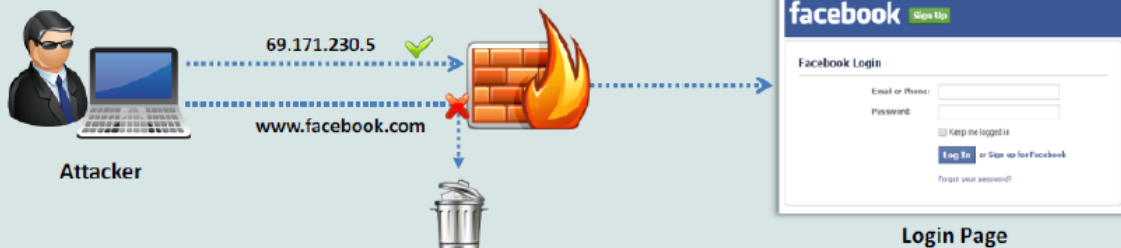
ফায়ারওয়ালকে বোকা বানানো যায়?

ফায়ারওয়াল দিয়ে বিভিন্ন সাইট/সার্ভিস অফ করা থাকলেও অনেক সময় ডিভাইসের অনেক পোর্ট ওপেন থাকে। তাই পোর্ট স্ক্যান করে ওপেন পোর্টগুলো ব্যবহার করে হ্যাক করা যায়। আবার আপনি হয়তো ওয়েবসাইটের নাম দিয়ে ব্লক করেছেন কিন্তু প্রত্যেক ওয়েবসাইটের বিপরীতে একটা আইপি থাকে চাইলে সেই আইপি দেওয়াও লগিন করে হ্যাক করা যায়।

Bypass Blocked Sites Using IP Address in Place of URL



- 01 This method involves typing the **IP address** directly in browser's address bar in place of typing the **blocked website's domain name**
- 02 For example, to access Orkut, type its **IP address** instead of typing domain name
- 03 Use services such as **Host2ip** to find the IP address of the blocked website
- 04 This method fails if the blocking software **tracks the IP address** sent to the web server



হানিপটসকে কিভাবে বোকা বানানো যায়?

হ্যাকাররা ফেক হানিপট চেক করার জন্য বিভিন্ন ধরনের টুলস ব্যবহার করে। যেমন- Send-safe honeypot hunter

Honeypot Detection Tool: Send-Safe HoneyPot Hunter

CEH
Certified Ethical Hacker

Send-Safe HoneyPot Hunter is a tool designed for checking **lists of HTTPS and SOCKS proxies** for "honey pots"

Features:

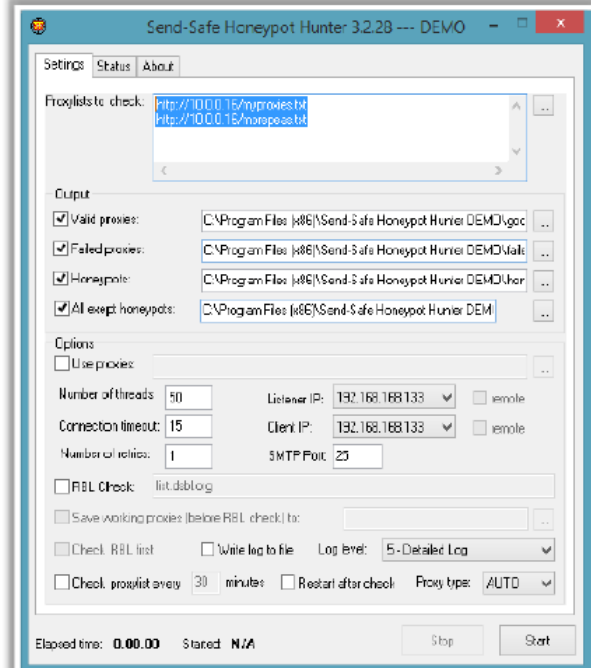
01 Checks lists of **HTTPS, SOCKS4, and SOCKS5 proxies** with any ports

02 Checks **several remote or local proxylists** at once

03 Can upload "**Valid proxies**" and "**All except honeypots**" files to FTP

04 Can process **proxylists** automatically every specified period of time

05 May be used for **usual proxylist** validating as well



আইডিএস, ফায়ারওয়ালকে বোকা বানালেও কিভাবে হ্যাকারকে প্রতিরোধ করা যায়

১. আইডিএস যেন টুকরা টুকরা প্যাকেটগুলোকেও স্ক্যান করে সেইভাবে কনফিগার করতে হবে।

২. অপ্রয়োজনীয় পোর্ট/ সার্ভিসগুলো বন্ধ রাখতে হবে।

৩. ডিভাইসের যে ইন্টারফেসগুলো ব্যবহার করা হয় না সেই ইন্টারফেসগুলো ডিসেবল রাখতে হবে।

৪. ডিভাইসের ওএস/প্যাচ সবসময় আপডেট রাখতে হবে।