



UN-ESCWA

Practical Application of Cyber Crime Issues

Nibal Idlebi and Matthew Perkins

United Nations Economic and Social Commission of
Western Asia (UN-ESCWA)

Information and Communication Technology Division

Practical Applications



- This presentation highlights the techniques and tools used in three realms of cyber crime:
 - Commission
 - Detection
 - Prevention

Background

Understand the Fundamentals



- In order to draft effective legislation, it is necessary to understand the technological background of cyber crime.

Legal Principles



- There can be no crime without a law for it.
- In order for an action to be illegal, there must be a specific law forbidding it.
- Most laws applied to cyber crime are based on efforts to make old law modern. This does not tend to work very well.

How to Commit Cyber Crime



- Cyber crime is a broad and complex field, with many different facets. This presentation highlights ways criminals use to break security systems, such as:

Compromising passwords

How to Commit Cyber Crime

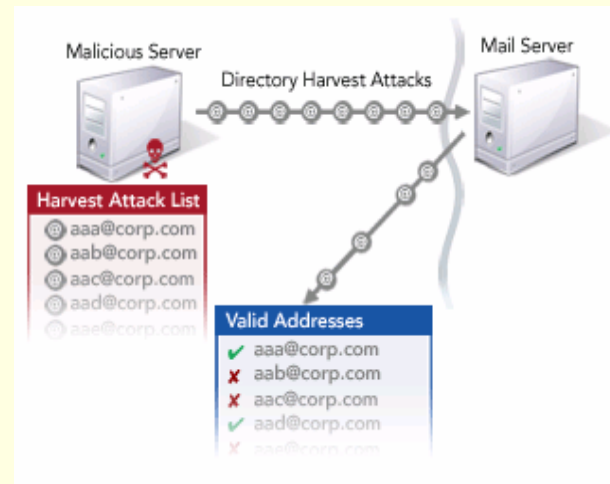


- Most people choose passwords that are relatively easy for a computer to guess using a technique called “**Brute force**”.
- In a brute force attack, the computer attempts to determine the password by using a large number of possibilities.

How to Commit Cyber Crime



- **Brute force** attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message.



How to Commit Cyber Crime Solar Winds



The screenshot displays the SolarWinds SNMP Brute Force Attack application. The main window shows the target IP address as 10.10.17.25 and the attack speed set to Fast. The status indicates the attack is paused. A detailed status table is visible, and a preferences dialog box is open, showing the 'SNMP' tab with the starting community string set to 'apple' and rotation options.

Attack paused ...	
Current Community String	caboS
SNMP Queries	174 total at 9.7 per second
Bandwidth being used	Approximately 0 bps
Target device	10.10.17.25
Target IP Address	10.10.17.25
Response Time	Request Timed Out
Packet Drops	1
DNS Name	
System Name	unknown
Attack Character Set	Alpha-Numeric character:
Maximum community string length	8 characters
Read/Only Community String	unknown
Read/Write Community String	unknown

SNMP Brute Force Attack Preferences ...

General | Character Set | Community Strings | **SNMP**

Starting Community String:
Leave this blank to search all possible community strings

Rotate from right to left
Example : AAAA, AAAB, AAAC, AAAD, AAAE, AAAF

Rotate from left to right
Example : AAAA, BAAA, CAAA, DAAA, EAAA, FAAA

OK Cancel Help

How to Commit Cyber Crime



■ Advantages:

- Can be extremely effective at obtaining unsecure passwords.

■ Disadvantages:

- Can take an extensive amount of time.
- Easily detectable for properly configured systems.

How to Commit Cyber Crime



■ Other applications:

Nessus vulnerability scanner

- Designed to automate the testing and discovery of known security problems before a hacker takes advantage of them.
- Reveals problems in a network, and can be used by both administrators and hackers
- Could be used by a hacker group, a security company, or a researcher to violate the security of a software product.

How to Commit Cyber Crime



- **Nessus vulnerability scanner**
 - Lots of capabilities.
 - Fairly complex
 - Detection of remote flaws
 - Scalable

How to Commit Cyber Crime



- Other applications:

Cain & Abel

- is a password recovery tool for Microsoft Operating Systems.

How to Detect Cyber Crime



- Use of Intrusion Detection System (IDS)
- Anti Virus does not detect such crimes
- One of the most known system is **Snort**:
 - Robust open source tool which exist for monitoring network attacks.
 - Its development started in 1998, and through years, it has evolved into a mature software (de facto standard) and even better than many commercial IDS.

How to Detect Cyber Crime



- It monitors network traffic to detect unusual behavior based on rules established by the administrator:
 - Unauthorized applications
 - Viruses
 - Intrusions
 - Brute force attacks
- There is a large Snort community interacting through Snort web site.

How to Detect Cyber Crime



Snort IDS Console - Microsoft Internet Explorer

Address: https://[redacted]

Snort IDS Console Unfilter Refresh every 30 secs. View alerts since 6 AM or on <---->

Alert Information		Sensors			Top Sources			Top Targets			Top Target Ports			
#	%	Sensor	Sigs	Alerts	IP Address	Sigs	Alerts	IP Address	Sigs	Alerts	TCP	#	UDP	#
Signatures:	62	[redacted]	19	482	[redacted]	6	186	[redacted]	6	186	80	513	1434	1,259
TCP Alerts [View]:	1,126 42%	[redacted]	13	177	[redacted]	5	5	[redacted]	5	5	139	186	53	242
UDP Alerts [View]:	1,523 57%	[redacted]	11	240	[redacted]	3	21	[redacted]	3	24	443	122	177	9
ICMP Alerts [View]:	0 0%	[redacted]	11	131	[redacted]	2	108	[redacted]	2	352	1433	23	111	6
Total Alerts [View]:	2,649 100%	[redacted]	9	298	[redacted]	2	92	[redacted]	2	92	3389	19	69	2

Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12

Signatures					
Prio	Signature	# Sensors	# Alerts	# Srcs	# Dests
1	WEB-MISC cross site scripting attempt [sid 1497]	2	353	2	2
1	P2P Fastrack kazaa/morpheus traffic [sid 1699]	2	145	3	49
1	MS-SQL/SMB raiserror possible buffer overflow [sid 1386]	2	117	1	1
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]	1	110	1	1
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]	2	33	1	1
1	WEB-MISC PCT Client Hello overflow attempt [sid 2515]	2	25	1	8
1	MS-SQL xp_cmdshell - program execution [sid 687]	1	17	2	1
1	MS-SQL/SMB xp_reg* registry access [sid 689]	2	12	1	1
1	MS-SQL/SMB sp_password password change [sid 677]	2	10	1	1
1	MS-SQL/SMB sp_delete alert log file deletion [sid 678]	2	10	1	1
1	MS-SQL sp_start_job - program execution [sid 673]	2	6	1	1
1	MS-SQL sa login failed [sid 688]	1	5	1	1

Done Internet

How to Detect Cyber Crime



Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03
Latest Alert: 2004-12-29 15:57:12

Prio	Signature
1	WEB-MISC cross site scripting attempt [sid 1497]
1	P2P Fastrack kazaa/morpheus traffic [sid 1699]
1	MS-SQL/SMB raiserror possible buffer overflow [sid 1386]
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]
1	WEB-MISC PCT Client Hello overflow attempt [sid 2515]

How to Detect Cyber Crime



■ Advantages

- Allows monitoring of network traffic
- Flexible rules set by administrator
- Open source

■ Disadvantages

- Can create extensive logs
- Effectiveness depends on configuration

How to Prevent Cyber Crime



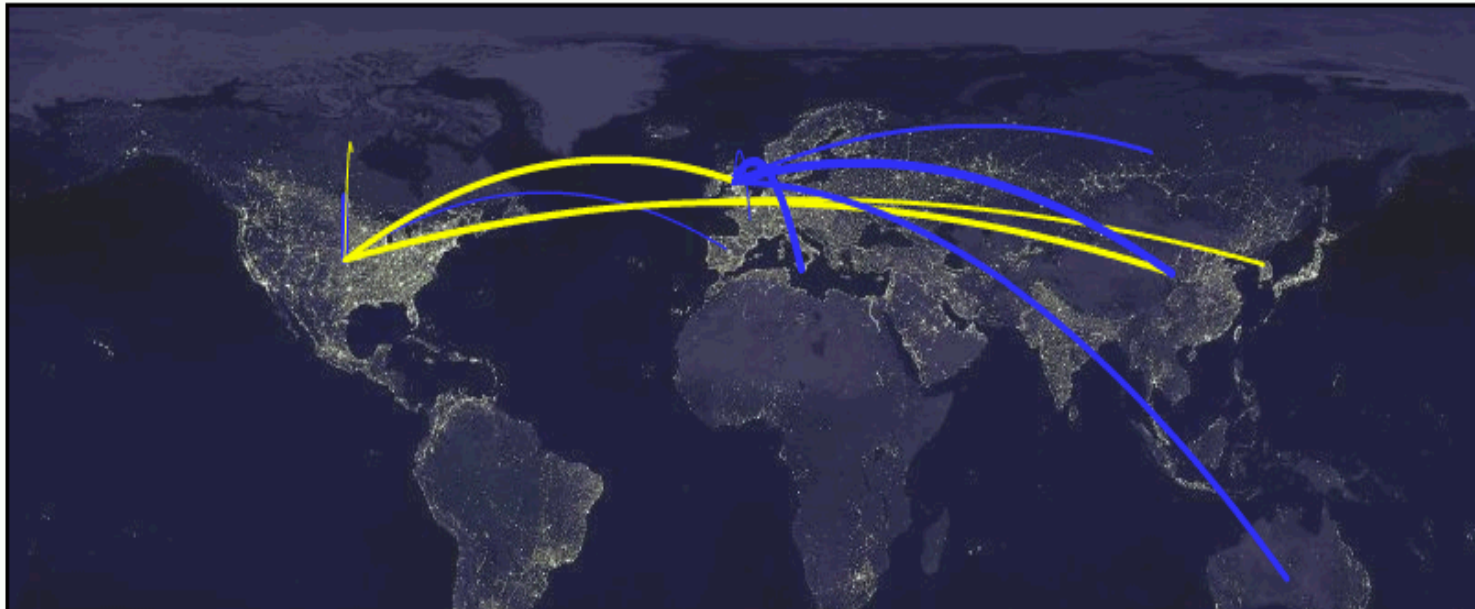
Vitally important to have current information on emerging issues.

How to Monitor Cyber Crime



"Packet Attack"

A little flash movie showing a sample of traffic submitted to dshield within the last 5 minutes. For the 'static' old wo



www.dshield.com



How to Monitor Cyber Crime

Home Computer Network Defence Operational Picture Home

Security News
from the SecurityNewsPortal.com

Powered and Protected by the BRICKServer from SAGE Inc

Computer viruses for Valentine's Day to break out
China View

Microsoft Anti-Spyware Removes Norton Anti-Virus Slashdot

Computer Network Defence Alert State

Novell	Microsoft	Lotus
1	1	1

Powered by E-Secure-IT

Internet Traffic Report
GLOBAL RESPONSE TIME
Index: 83 Trend: [graph]
2/13/2006 23:45 MST

symantec.
Security Alerts

Latest Threats

- 11-25-05 W32.Beagle.CQ@mm
- 11-23-05 W32.Secefa.A
- 11-23-05 Trojan.Lodear.D
- 11-23-05 Backdoor.Spymon
- 11-23-05 Trojan.Anserin

Use this feed on your s

ALERTCON

Port Probe Distribution

dshield Geographic Port Probe Distribution

2006-02-13 <http://www.dshield.org>

Latest Tool Versions

Cain & Abel	11Feb06	2.8.4
Nmap	31Jan06	4.00
Nessus Client	13Jan06	1.0 RC4
Nessus	08Jan06	3.0.1
Ethereal	27Dec05	0.10.14
Metasploit	21Oct05	2.5
Snort	17Oct05	2.4.3
Kismet	15Aug05	05-08-R1

Latest IDS Signatures

Proventia	11Feb06	24.28
Cisco IPS	03Feb06	S215
Symantec IPS	25Jan06	v39
Intrushield 2.1	05Oct05	2.1.26.2
SecureNetPro	28Feb05	3.9
Manhunt 3.0	09Feb05	v10

Los Angeles Chicago New York GMT/UTC London Europe Baghdad Tokyo Sydney Wellington NZ

23:02 01:02 02:02 07:02 07:02 08:02 10:02 16:02 18:02 20:02

Latest Threats

Latest Tools

<http://securitywizardry.com/radar.htm>

How to Monitor Cyber Crime



■ **Advantages:**

- Provides information on threats, tools and responses.

■ **Disadvantages:**

- Information very technical
- Little Response time

How to Prevent Cyber Crime



- Detailed acceptable use policies for the organization
- Firewall strategy
- Threat specific protection
- Use of Spyware Prevention Programs
- Some of Intrusion Detection System (IDS) are also preventing cyber crime

How to Prevent Cyber Crime



■ Basic features:

- Detect and protects system and network from external attacks: Spywares, Adwares and other Malwares.
- Provide real-time protection
- Consume PC power and network bandwidth
- Complements existing antivirus and firewall installation.
- Example : eTrust Pest Patrol

How to Prevent Cyber Crime



■ **eTrust Pest Patrol features:**

- Scan files and directories
- Cleaning Spyware
- Removes cookies
- Report all activities to a central log

■ **Characteristics:**

- Centralized management with transparent deployment and operation
- Efficient resource usage
- Customized protection for different levels of vulnerability

Conclusion



- Many technological tools are dual use, can serve both commission and prevention of cyber crime.
- Example:

Encryption

Conclusion



- Encryption
 - Provides privacy and freedom of speech
 - Can also facilitate criminal activity.

Conclusion



- Comprehensive approach would have several layers:
 - Adoption of strong legislation against cybercrime
 - Development of technical measures
 - The establishment of industry partnership
 - Education of consumer and industry players about anti-crime measures
 - International cooperation to allow global coordination approach to the problem

Conclusion



- Cyber legislation must be responsive and adapt to emerging technological developments.