Internet Security

by

Alan S H Lam

Internet Security

I. Aware of the Risks
   - The threats

II. How they hack in
   - Two real case studies with live demo

III. Fighting back
   - Counter measures and strategies

IV. Q&A and discussion

Part I Aware of the risks

The Threats

The Threats

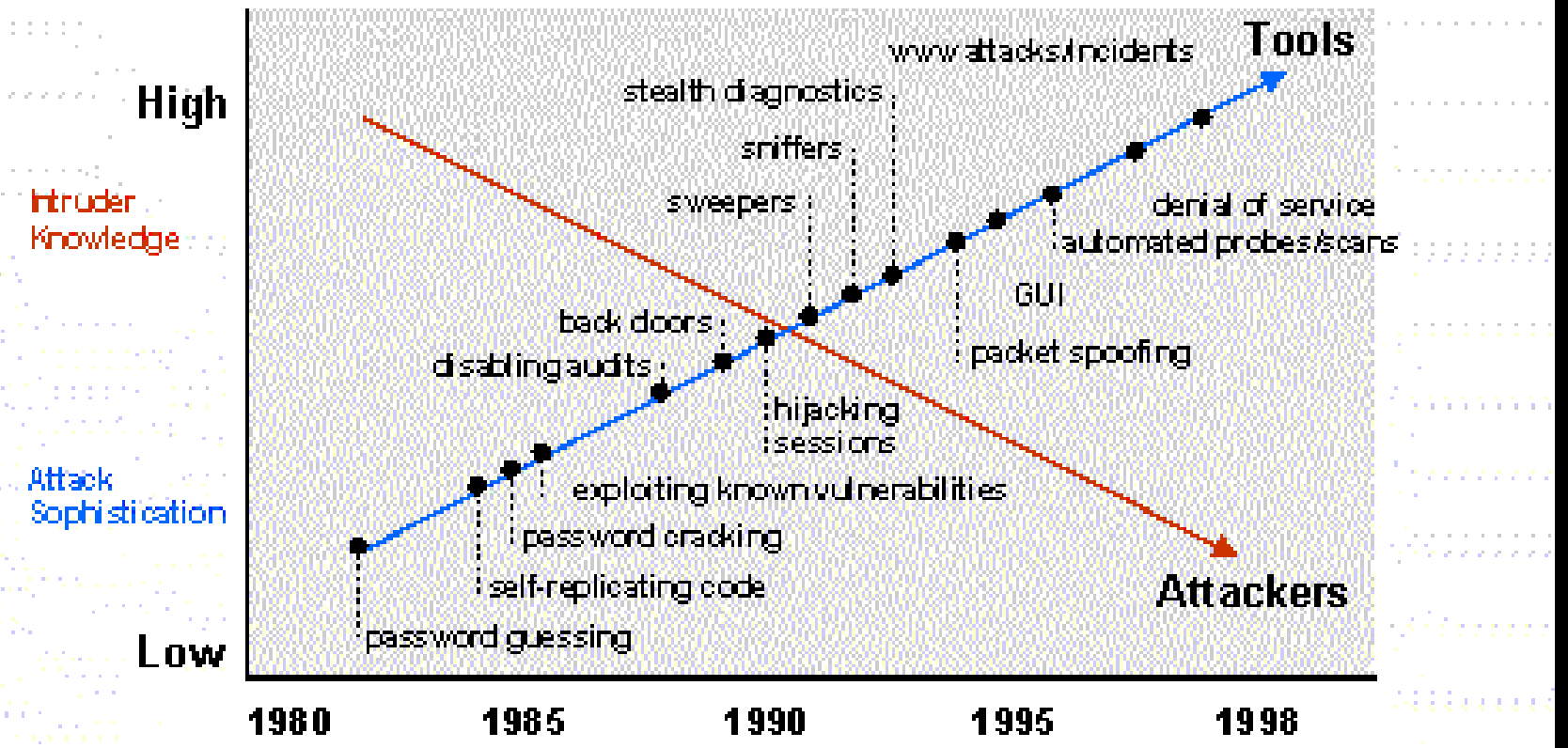
- Hacker Technologies
  - Internet Engineering
  - System Administration
  - Network Management
  - Reverse Engineering
  - Distributing Computing
  - Cryptography
  - Social Engineering

The Threats

- Hacking Tools become more and more sophisticated and powerful in term of
  - Efficiency
  - Distributing
  - Stealth
  - Automation
  - User friendliness

The Threats

Attack Sophistication vs. Intruder Technical Knowledge



The Threats

- These hacking tools could be easily download from the Internet =>
  - –Hacker tool ability increases
  - – Knowledge of hacker decreases
  - – Population of hacker increases
  - – Some day, even elementary school kid may hack into your system

The Threats

- Your host does not need to be as famous as yahoo or ebay to be targeted
  - They need a place to hide their trace
  - They need your host as a stepping stone to hack other sites
  - They need your host resource to carry out their activities

The Threats

- Your host security weakness can be identified by scan tool
- Security of any network on the Internet depends on the security of every other networks
- No network is really secure

The Threats

- The trends
  - Hacking activities become more and more common
  - Poor management networks will become the hackers playground

The Threats

- The Trends
  - Starting from Jan 2000, from time to time, we receive the following security warning
    - Web page defacement
    - Unauthorized system access
    - Port scanning
    - Ping broadcast scanning
    - Telnet probe scanning

    The most recent warning is rpc probe on 26th Feb 2001

The Threats

- Classes of Attackers
  - Script-kiddies
    - Do not have much skill
    - Having a very basic knowledge of networks and OS
    - Just download the packaged software and launch the attack. Often, they do not even know how the software works
    - 95% of the population

The Threats

- Classes of Attackers
  - Intermediate attackers
    - More skilled than script-kiddies
    - Having knowledge of UNIX, Windows, networks, protocols, and services
    - Most of them cannot identify new security holes in software and networks

The Threats

- Classes of Attackers
  - Expert attackers
    - They get their knowledge through work or training
    - They can identify security holes in a system or networks and can write program to exploit these weaknesses.
    - Most of them do not break the law but they feel it is necessary to warn vendors to fix the security problems ("proof of concept")

Part II How They Hack In

Two real case studies

How they hack in

- General Steps
  - Locate the victim host by some scanning program
  - Identify the victim host vulnerability
  - Attack the victim host via this vulnerability
  - Establish backdoors for later access

How they hack in

Some hacking tools can automate the above steps into a single command.

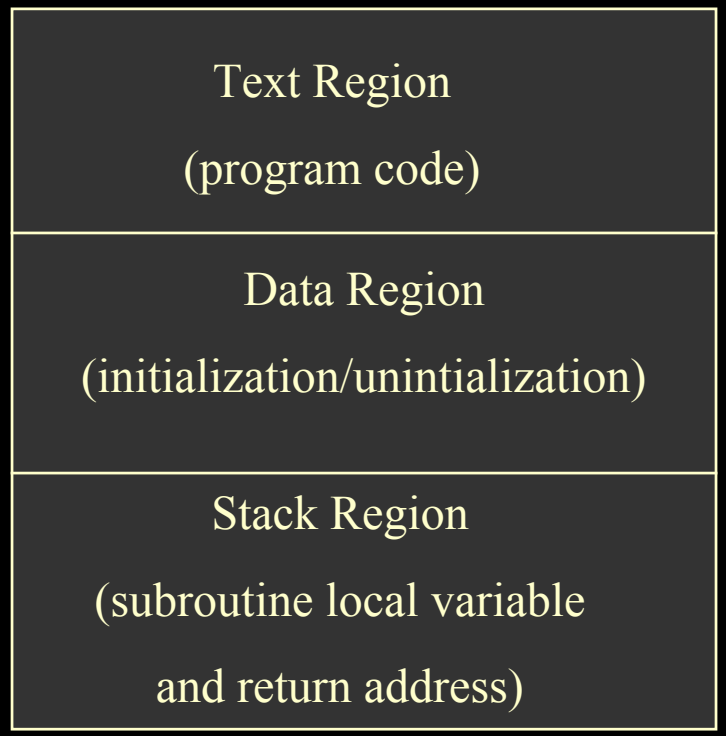
- After break-in, use this victim host to
  - hack other network
  - use this victim host resource to carry out their activities
  - Web page defacement for certain assertion

How they hack in

- Buffer Overflow Exploit
  - stuffing more data into a buffer than it can handle
  - it overwrites the return address of a function
  - it switches the execution flow to the hacker code

How they hack in

- Buffer Overflow Exploit



Process Memory Region

How they hack in

- Buffer Overflow Exploit

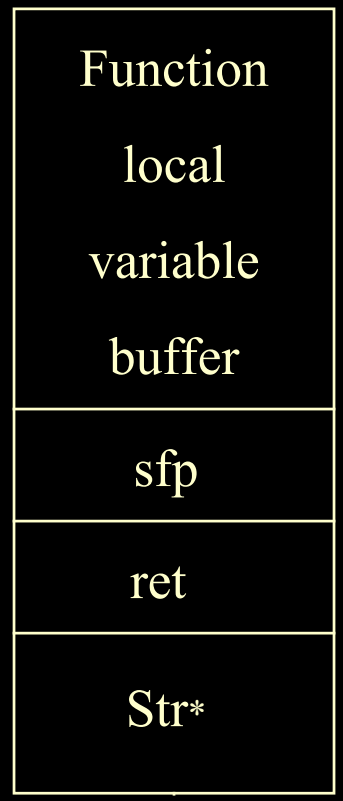
```
void function(char *str) {
   char buffer[16];

   strcpy(buffer,str);
}

void main() {
  char large_string[256];
  int i;

  for( i = 0; i < 255; i++)
    large_string[i] = 'A';

  function(large_string);
}
```



Top of Stack

Save Frame Pointer

Return address

Bottom of stack

How they hack in

- Real Case Study I
  - Hackers first located the victim hosts by sunrpc scan of 137.189 network
  - Break-in the victim hosts via amd (Berkeley Automounter Daemon) buffer overflow vulnerability
  - Created backdoor on port 2222 by starting a second instance of inetd daemon
  - Used the victim hosts to scan other networks

How they hack in

- Real Case Study II
  - Hackers first located the victim hosts by BIND port 53 scanning
  - Identify the victim OS (a telnet probe)
  - Set up a trap DNS daemon at the hacker DNS server
  - Kicked the victim hosts to query the hacker DNS server
  - Break-in victim hosts via BIND buffer overflow
  - Established back door accounts at the victim hosts
  - Distribute, built and operated the IRC Bot (eggdrop)

How they hack in

- Another real case (in Jan 2001)
  - Compromises Via Ramen Toolkit
    http://www.cert.org/incident_notes/IN-2001-01.html
  - Hack in via vulnerability in FTPD
  - After break-in, the hacker perform another ftp port scan to other networks

Part III Fighting Back

- Perform Risk Analysis
- Get Your Security Profile
- Set Your Security Policy
- Shield up your network
  - Build your Firewall and IDS

Perform Risk Analysis

- Identify and locate your assets
  - Identify what you need to protect
  - Assess the important and value of these assets
- Identify the threats to these assets
  - Categorize the likelihood of these assets being stolen or destroyed and identify the the resulting damage to your company if such an occurrence comes to pass
  - Rank those risks by level of severity (e.g. cost for resuming the service)

Get Your Security Profile

- Perform the penetration test

  (Act as a hacker and try to break-in your host)

  – The steps

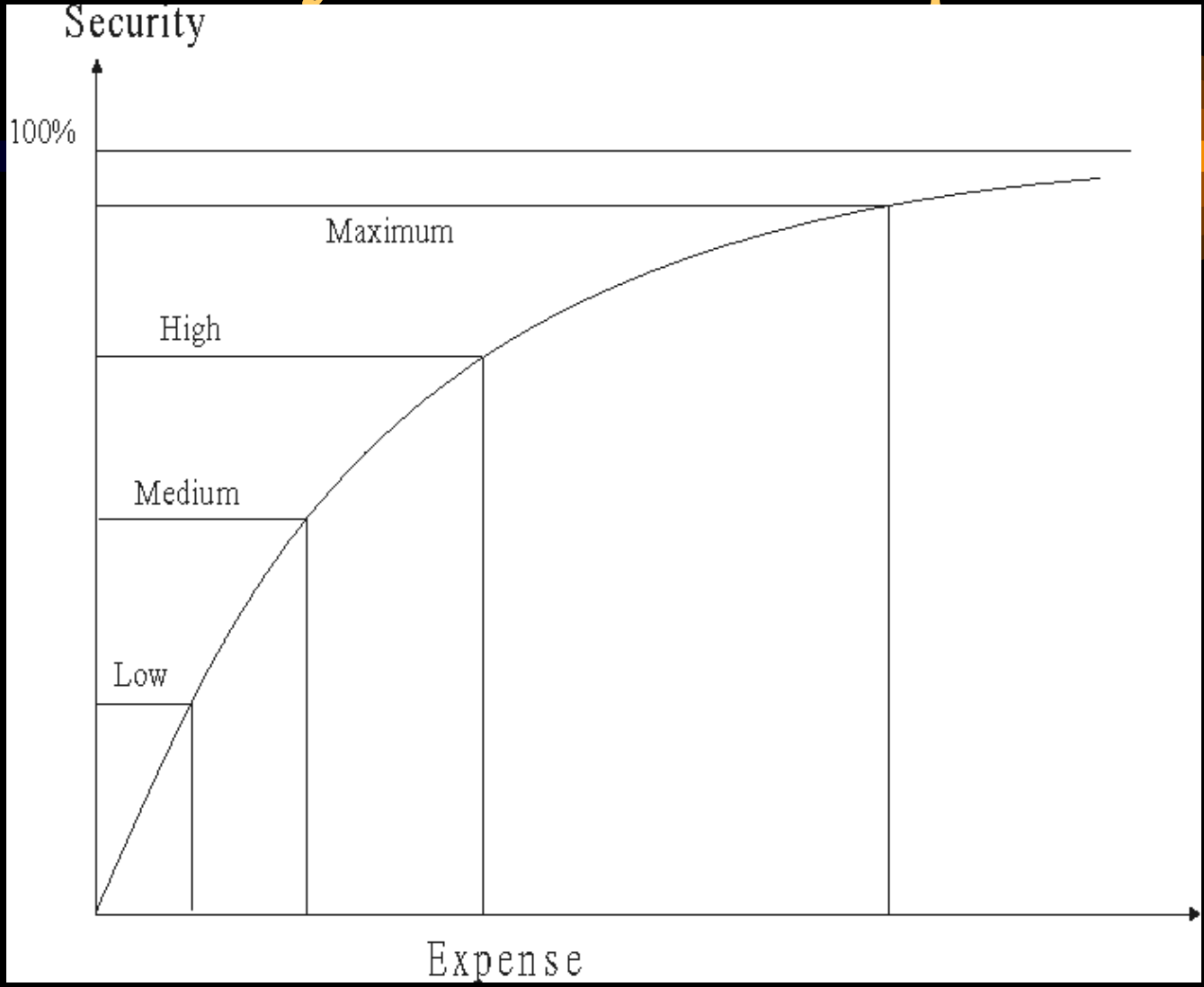
  http://personal.ie.cuhk.edu.hk/~shlam/talk/BA/ptest.html

  – Can you attack your assets during the test?

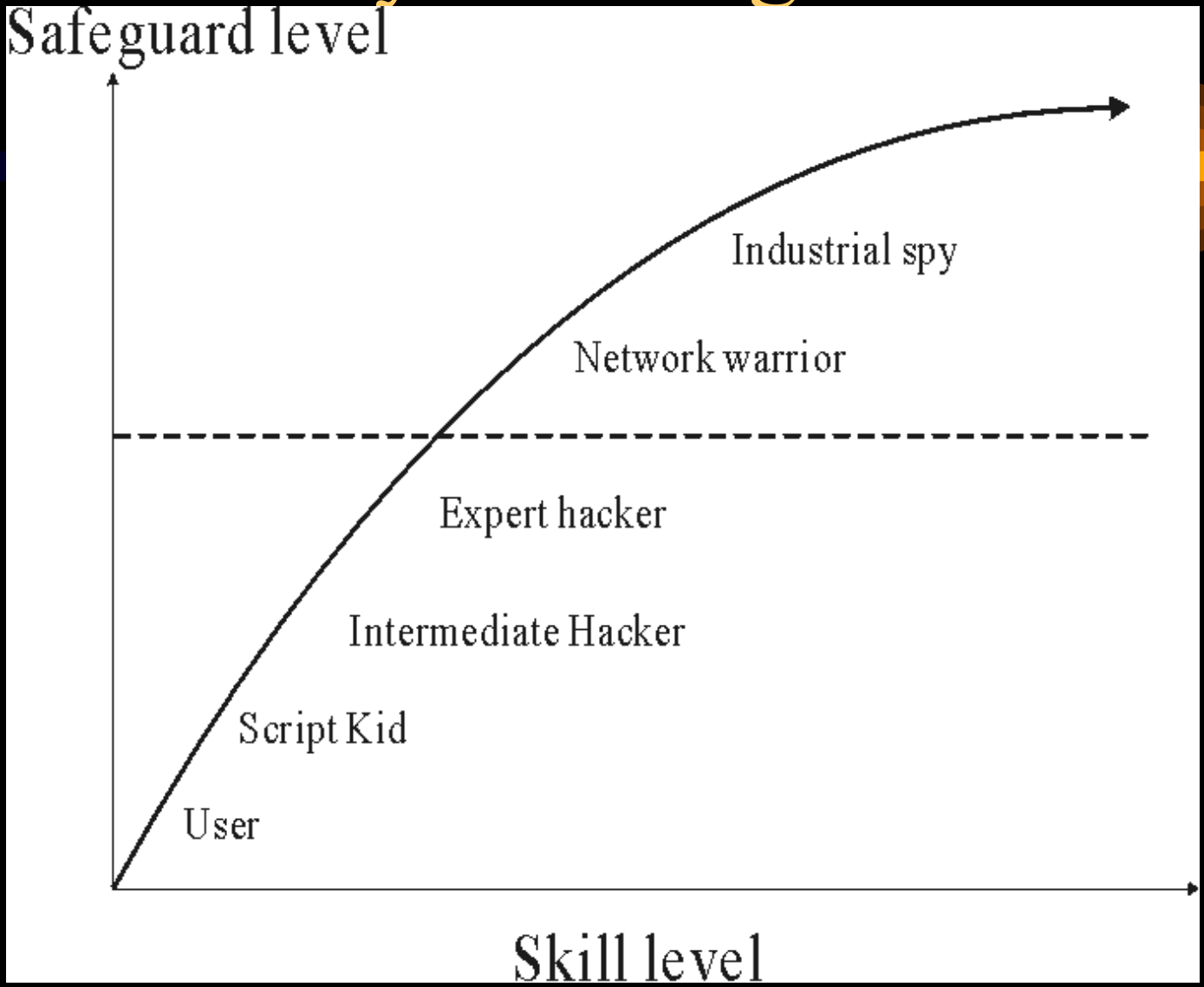
  – Can you cover up your trace after break-in? (Does your host have any monitoring or intrusion detection system)

  – Can you easily establish back door after break-ins? (Have you built any firewall?)

Security Level VS Expense



Determine your safeguard level



Set Your Security Policy

- After the risk analysis and security profile, you should have some ideas to shape your security policy
- Some key components of a security policy
  - Physical Security
  - Network Security
  - Access Control
  - Authentication
  - Encryption
  - Key Management
  - Incident Response & Disaster Contingency Plan

Set Your Security Policy

- Some key components of a security policy (con't)
  - Acceptable Use Policy
  - Security Awareness
  - Auditing and Review
  - Compliance and Enforcement

Set Your Security Policy

- There is always a trade off between security and convenience
- Some examples in your security policy may be:
  - Identify your host services
    - shutdown any unnecessary ports and build the kernel as minimum as possible
  - Identify your target users, trusted hosts and networks so that you can formulate your host access lists
  - Set up your firewall
    - use private IP network
    - use proxy servers

Set Your Security Policy

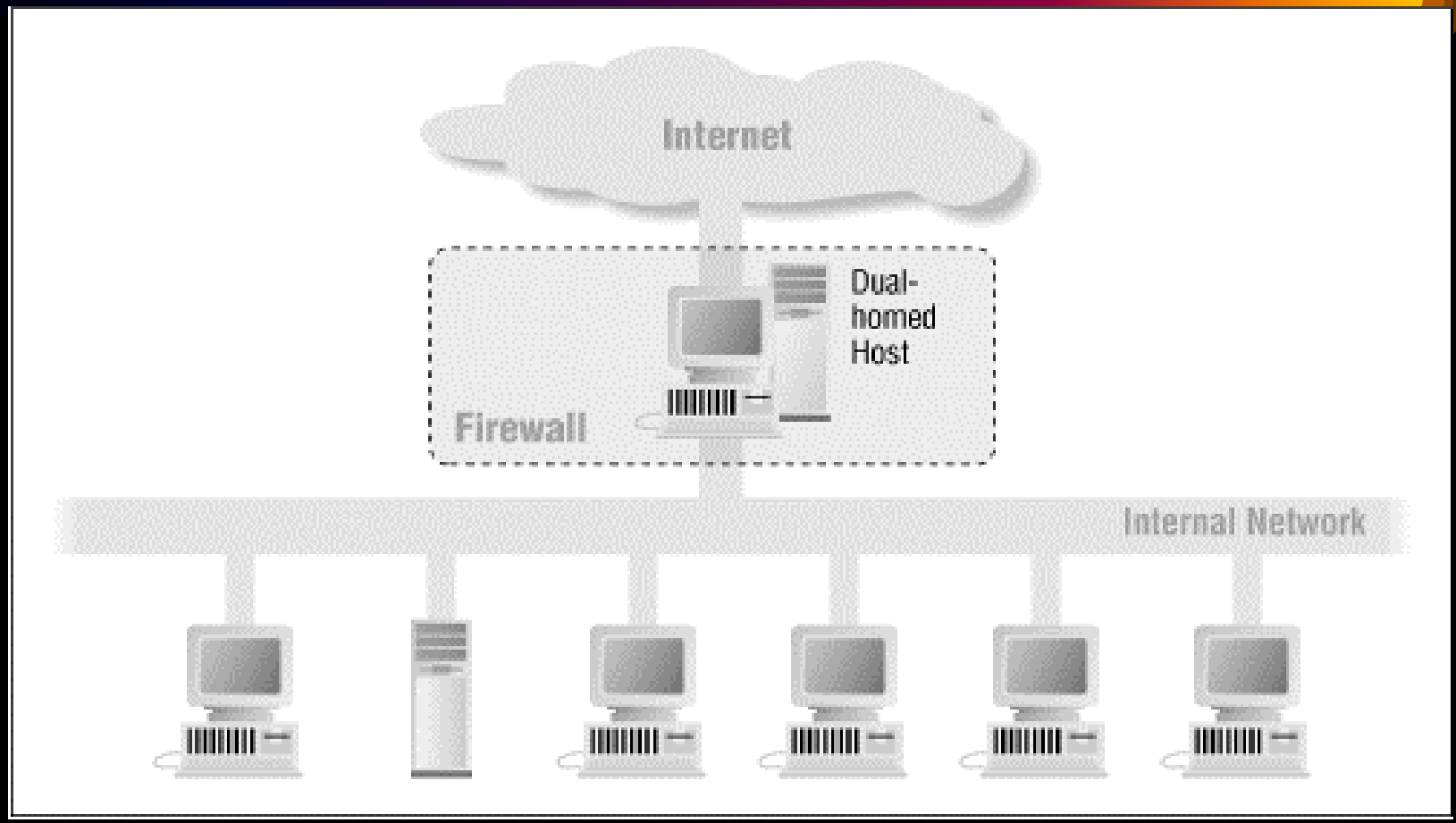
- Some examples in your security policy may be: (con't)
  - Set up your monitoring and intrusion detection systems
    - e.g . COPS, tripewire, tcpdump, snmp, snort, nessus
  - Set up you operation codes/rules such as
    - read only file system mounting
    - ssh login, sudo , restrict login shell
  - Set up your recovery plan
    - recovery procedure and backup scheme
- You may reference other site security policies as your template
  - http://secinf.net/info/policy/isptg.en/ISPTG-Contents.html
  - http://secinf.net/info/policy/fips191/

Build your Firewall and IDS

- Control and monitor the traffic IN and OUT of your network
- Block any unnecessary network connection from non-trusted hosts and networks
- Define your access rules according to your security policy
- Use packet filtering and Application Proxy
- Build IDS to monitor your internal network traffic

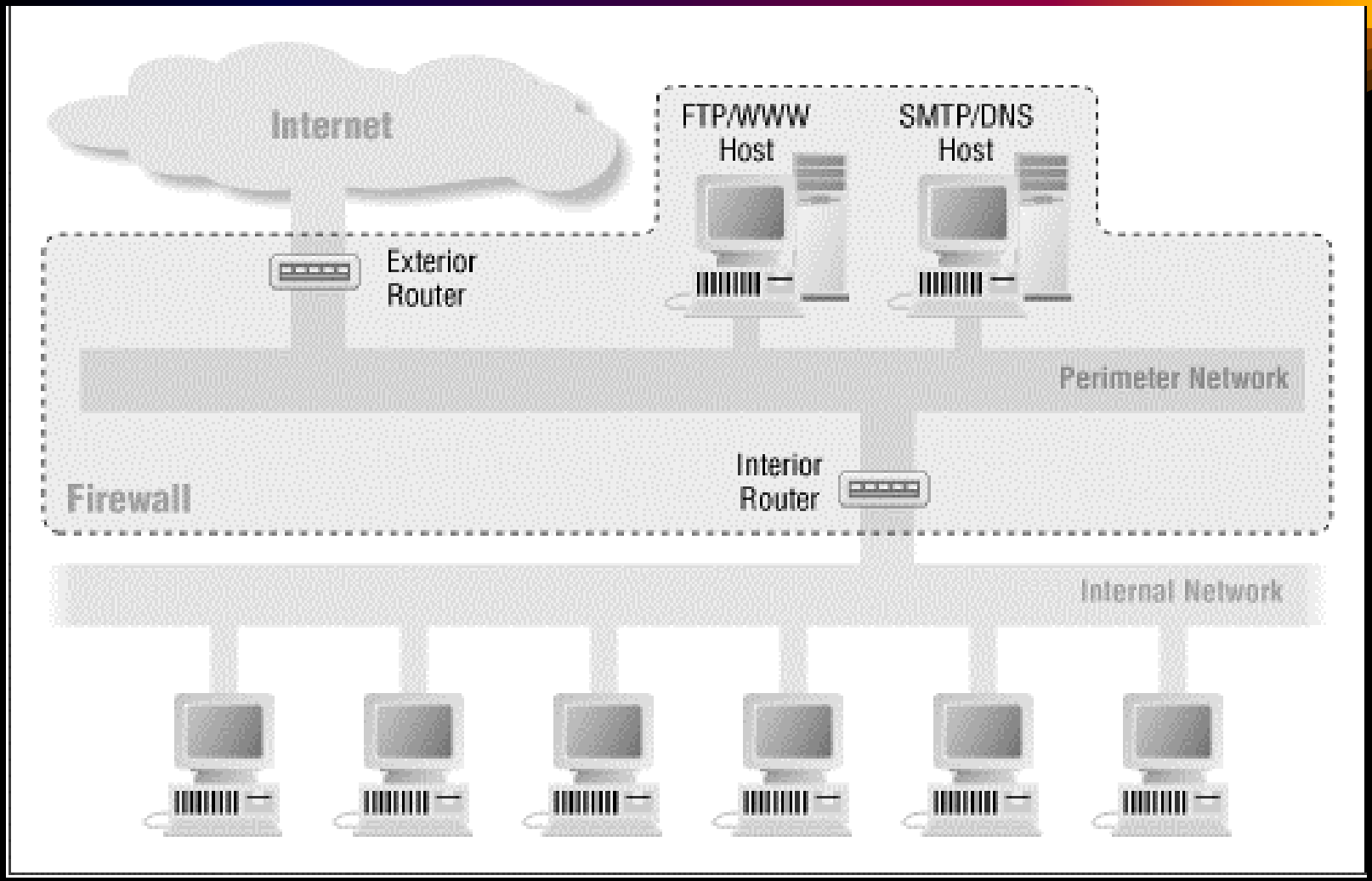
Firewall Architecture

- Dual-home host architecture



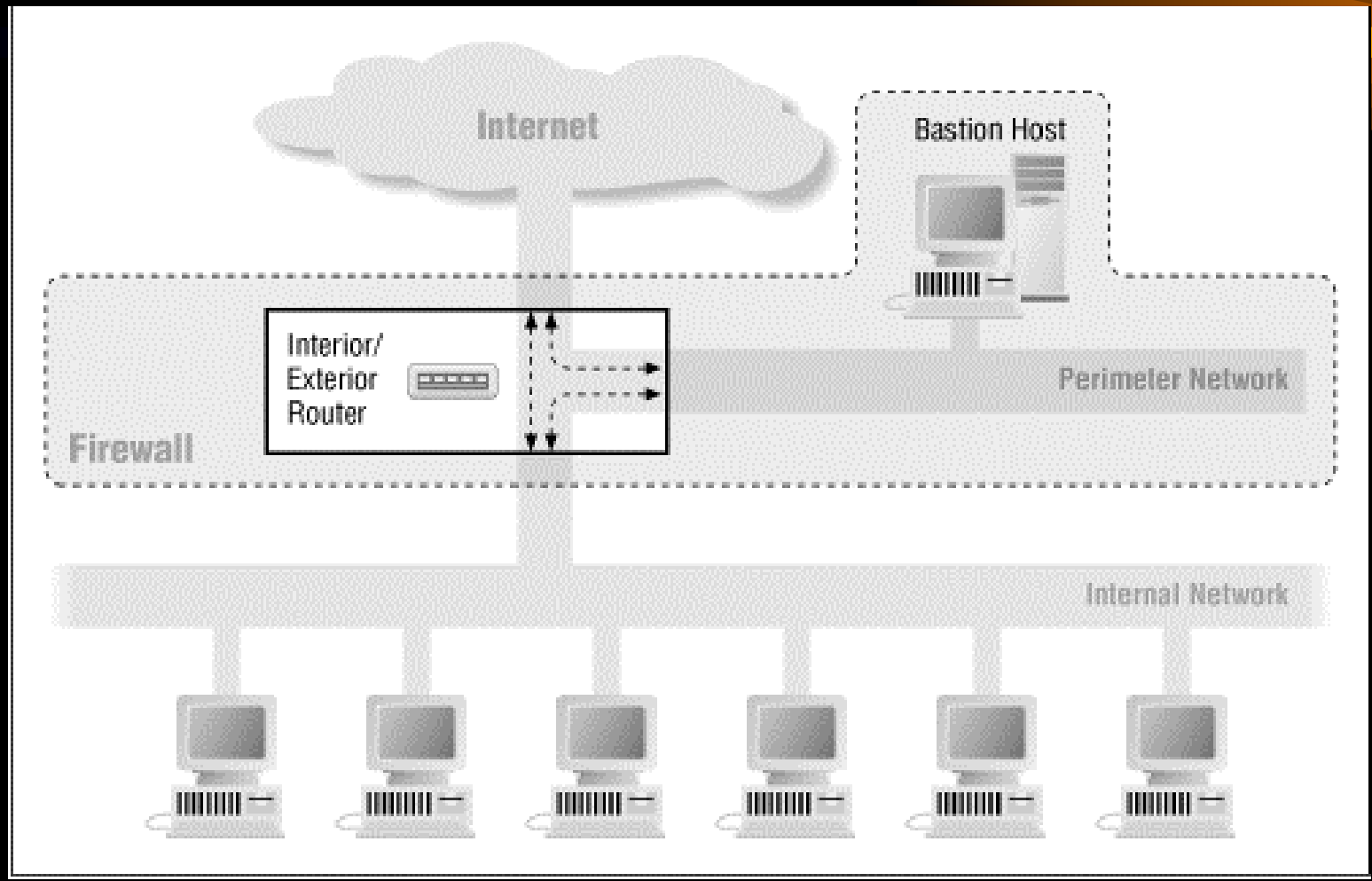
Firewall Architecture

- Architecture using two routers



Firewall Architecture

- Architecture using a merged interior and exterior router



Build Your Firewall

How it protects your network

- prevent port scanning
- prevent DDOS attack and IP spoofing from your host
- block any unnecessary network port opening
- increase the difficulty of creating back door after break-in
- facilitate the network monitoring and network intrusion detection

Set up your Intrusion Detection System (IDS)

- Network intrusion detection systems (NIDS)

  monitors packets on the network wire and attempts

  to discover if a hacker is attempting to break into a system. (e.g snort)

- Host based intrusion detection system

  monitors system files to find when a intruder changes them (e.g tripewire)

Summary

- Perform regular penetration test on your network (some scanner tools can help)
- Set up your Firewall and IDS (both network and host based)
- Review your security policy regularly so as to catch up the changes of your network
- Appoint someone to be responsible for security policy enforcement

References

- Hacking Lexicon - buffer-overflow
  - http://www.robertgraham.com/pubs/hacking-dict.html#buffer-overflow
- Systems Compromised Through a Vulnerability in am-utils
  - http://www.cert.org/incident_notes/IN-99-05.html
- CERT Advisory CA-99-12 Buffer Overflow in amd
  - http://www.cert.org/advisories/CA-99-12-amd.html
- Real Case Study I (Buffer Overflow in amd)
  - http://home.ie.cuhk.edu.hk/~shlam/ed/hack/case1

References

- CERT Advisory CA-99-14 Multiple Vulnerabilities in BIND
  - http://www.cert.org/advisories/CA-99-14-bind.html
- Real Case Study II (Vulnerabilities in BIND)
  - http://home.ie.cuhk.edu.hk/~shlam/ed/hack/case2
- Scans and Probes
  - http://www.cert.org/current/current_activity.html#scans
- Building Internet Firewall
  - By Chapman & Zwicky, O'Reilly ISBN 1-56592-124-0

References

- Network Security Information: Security Policy
  http://secinf.net/ipolicye.html
- Vulnerability Assessment Scanners
  http://www.nwc.com/1201/1201f1b1.html
- Network Intrusion Detection: An Analyst's Handbook, Second Edition
  - By Stephen Northcutt and Judy Novak, ISBN: 073510082
- NTEC Security Link
  http://hkntec.net/ref/security/