ISP/NSP Security

Host Security

APRICOT 2007

21 February – 2 March 2007

Vicky Shrestha

vickysh@wlink.com.np

- Introduction
- User Administration
- Securing Services
- System Logging
- Server Monitoring
- File System Integrity
- Network Scanning
- Intrusion Detection System
- Firewall
- Cryptography

"A computer is secure if you can depend on it and its software behave as you expect"

-- Practical Unix and Internet Security

- Confidentiality
  - The information Stored must be protected from those who are not authorized to view them
- Data Integrity
  - The information must be protected from being altered or deleted without the permission or knowledge of the owner
- Availability
  - The information must be available when the authorized user needs them. Failure to deliver information when needed is equivalent to having no information at all

- Consistency
  - The system must behave as expected. A radical change in the behavior of software due to upgrades, bug fixes can be disastrous
- Control
  - A system administrator must make sure that there are no unauthorized users in the system. He should regulate access to the system
- Monitoring
  - Constant Monitoring of system is necessary to detect intrusions and other security issues
- Audit
  - Proper audit must be conducted for a damage made to determine what was done, by whom and what was affected

- Network Connectivity
  - Your host is connected to the network, which makes it more accessible to network based attacks
- Denial of Service Attacks
  - Attacks on network infrastructure or Legitimate services, so that service is denied or unavailable
- Unauthorized Intrusions
  - Unauthorized Intrusions are break-in performed by people who are not authorized to access the network resources
- Buffer Overflow
  - Resulting from coding errors and lack of proper validation of input, an attacker can craft special data that will overwrite the buffer allocated by a program and run arbitrary codes

- Brute Force/Dictionary Attacks
  - Brute Force/Dictionary attacks are performed to find out the credentials necessary for logging in or to gain unauthorized access
- Packet Sniffer
  - Packet sniffer such as tcpdump,ethereal are used to eavesdrop on an existing connection. Telnet and ftp sends clear text passwords that can be sniffed by these packet sniffers
- Spoofing Attacks
  - Spoofing Attacks means forging source address of trusted hosts to access network services
- Web Based attacks
  - Web based attacks include SQL injection, code injection (cross-site scripting), result of improper validation of input in dynamic websites

- BackDoor
  - Intruders generally leaves some sort of backdoor on compromised machines. If not detected it gives an easy way for the intruders to gain privileges in future
- Social Engineering
  - Social Engineering means trying to gain information/credentials, that can compromise network security, from people who are authorized to access the network resources.
  - Social Engineering heavily depends upon Human interaction

- Insecure services running on a host
- Services with security holes
- Insecure configuration of Services
- Presence of Malicious codes in the system
- Use of Weak or Default passwords
- Running vulnerable services such as telnet,rsh,r*,etc
- Running Services where authentication information is send in unencrypted format
- Poorly protected hosts/networks without firewall, IDS
- Insufficient validation of input in applications
- Lack of importance given to security

- A security breach can be performed by hired professionals to steal confidential data
- A curious and intelligent computer savvy person might like to get into your system just for fun
- A very secure system can serve as a challenge for crackers and can earn him respect after a successful break-in
- Ex-Employees after being fired can also breach security for revenge
- A computer user might breach security due to total ignorance

User Administration

- Each user in Unix has a unique User ID
- Each user is also given a separate Home Directory and a default shell
- User has one primary group and may belong to one or more secondary groups
- A valid user name is required to log in to a system
- Different users having the same privilege and access level requirements can be assigned to a group and group permissions can be assigned
- All users in the system don't need shell access

- User root is the super user who has access to virtually everything within a system
- Use of root user should be avoided until absolutely needed
- Most administrative jobs can be done using a normal user account
- One should login as a normal user and use 'su' (Substitute User) only when root privileges are required
- We can also use sudo to run scripts or programs requiring root access
- If an attacker gains root access, then the only way to trust your machine is to have a complete reinstall
- You should disable direct login as user root

- User Details are stored in /etc/passwd
- Passwords are stored in encrypted format using one-way encryption
- Many version of Unix now store the encrypted password in a separate file, which is only readable and writable by user root

Securing Services

- Install only the required services
- Turn off everything else and enable only required services
- Restrict access to running services to only those who should have access
- Use TcpWrappers to restrict access to services
- Update or Patch the programs regularly to fix potential or know security holes
- Verify what services are actually running using ps and netstat commands
- Use Firewall to protect the services
- Use chroot/jail where possible
- Limit the number of processes a service can fork
- Configure limits such as cpu, mem, file descriptors etc from “/etc/login.conf”

- It is advisable not to use clear text proctocls such as telnet,ftp,pop3,http specially those which require authentication info to be sent across the wire
- During telnet, the transmitted data are unencrypted meaning your passwords and session data are sent in plain text
- Anyone running a sniffer on the network can find out what was transmitted and received during a telnet session
- There are better alternatives to telnet, the popular one being ssh
- SSH or Secure Shell provides a secure alternative to telnet

- User names and passwords are send in clear text in ftp
- Use of sftp should be promoted
- Basic Authentication in Apache Web server also sends password in clear text
- One should use SSL for Web server authentication
  - http -> https
- username and passwords are send clear text in pop3 protocol
- One can use pop3s to secure the pop connection via using SSL
- Whenever authentication is done one should use Encrypted channel to protect the authentication data

- Portmap is not needed unless you are running nfs server or NIS
- Proper protection from tcpwrapper and firewall should be provided if portmap must be on
- R services such as rlogin, rsh, rcp should be disabled
- R services can be replaced by SSH ssh, sftp, scp

- NFS (Network File Service) is the most frequently used method of sharing access to file system between Unix systems
- System administrators need to be careful about how they implement NFS and be aware of the vulnerabilities associated with various daemons which collectively make up the NFS service including nfsd, mountd, statd, lockd
- Regular updates/patches should be done for these daemons
- NFS Services must be protected via Tcpwrapper and Firewall

- Tcpwrapper is an utility that intercepts packets and authorizes it before delivering it to the final application
- It can be configured by editing the file:
  - /etc/hosts.allow and /etc/hosts.deny
- It is recommended to allow only selected services and deny the rest as show in the following example
  - ALL : localhost : allow
  - sshd: 192.168.0. : allow
  - ALL : ALL : deny
- However all services that can run on Unix cannot be protected via tcpwrapper, some programs needs to be compiled with tcpwrapper support while others do not use it at all

- When installing softwares, you should verify the integrity /authenticity of the software package
- There are different tools available to verify that :
  - md5, gpg
- You should also be using File Integrity verification programs such as tripwire, aide, osiris etc to check if the system binaries are tampered with
- You should also make sure that the programs installed on your system are up to date
- You need to watch out for new bugs that are discovered and apply security patches as soon as possible
- A good practice is to subscribe to vendor's security mailing lists and other security mailing lists

System Logging

- You should use ntp for synchronizing time which is necessary for effective analysis of system logs
- You can either use 'ntpd' of 'ntpdate' command periodically from cron to sync to a time source
- Install primary and secondary ntp servers in your network that will sync to external ntp servers
- Other servers and network devices can then sync to these local servers

- Unix Systems uses syslogd for system logging
- Some of the important files that needs to be monitored are
  - /var/log/messages
  - /var/log/auth.log
  - /var/log/security
- You will find critical information about network login failures, failed su attempts, and various other useful informations

- You should also run a central network logging server
- Central logging server is important from security perspective because logs residing on a compromised machine can be tampered
- You can send logs to remote syslog server by putting the following in /etc/syslog.conf
  - *.* @ remote-syslog-server
-

- Individual services also generate their own log files
  - Apache
    - /var/log/httpd/access.log
  - Proftpd
    - /var/log/proftpd/auth.log
    - /var/log/proftpd/access.log
  - Squid
  - /var/log/squid/access.log
- As the number of servers grow, it can be quite cumbersome to audit logs of all the servers
- There are numerous programs available on the Internet that can do the job
  - swatch
  - fwlogwatch
  - webalizer

Server Monitoring

- Uptime command will show you details such as current time, time since last reboot, number online users and system load
  - ```
    $ uptime
    5:51pm  up 186 days, 2:06,  6 users,  load average: 0.06, 0.06, 0.05
    ```
  - The above output tells us that current time is 5:51pm
  - system is up for 186 days,2 hr 6 min
  - 6 users are online on the system
  - Load average for 1 minute = 0.06
  - Load average for 5 minute = 0.06
  - Load average for 15 minute = 0.05
    ```

- ps is one of the most important tools for system resource monitoring
- ps reports the running processes in the system
- ps can be used with different options
- 'ps -aux' will print all the processes with/without controlling terminal and will also display the user running the process
- top is just like ps, however it updates its stat in real time
- Additional stats on virtual memory can be seen using vmstat

- netstat/sockstat will show you the network socket information
- For eg.
  - $ netstat -an
    - will show you all sockets
  - $ netstat -n -p tcp
    - will show you the currently open tcp sockets
  - $ netstat -s
    - will show you various networking related informations
- sockstat will you show you additional details such as command opening the port and it's PID
  - $ sockstat -l -4
    - Show all IPV4 Listening sockets

- Process accounting is security system whereby you can keep track of allocation of system resources to users and processes
- It also provides command auditing features
- You can enable process accounting by adding the following to “/etc/rc.conf”
  - accounting_enable=YES
- To see the resource utilization/allocations
  - % sa
- lastcomm can also be used to see the history about command executed on the system or commands run by a particular user
  - % lastcomm ls
  - % lastcomm user

- Nagios
- Big Brother
- Big Sister
- MRTG
- RRD
- Ntop
- Cacti

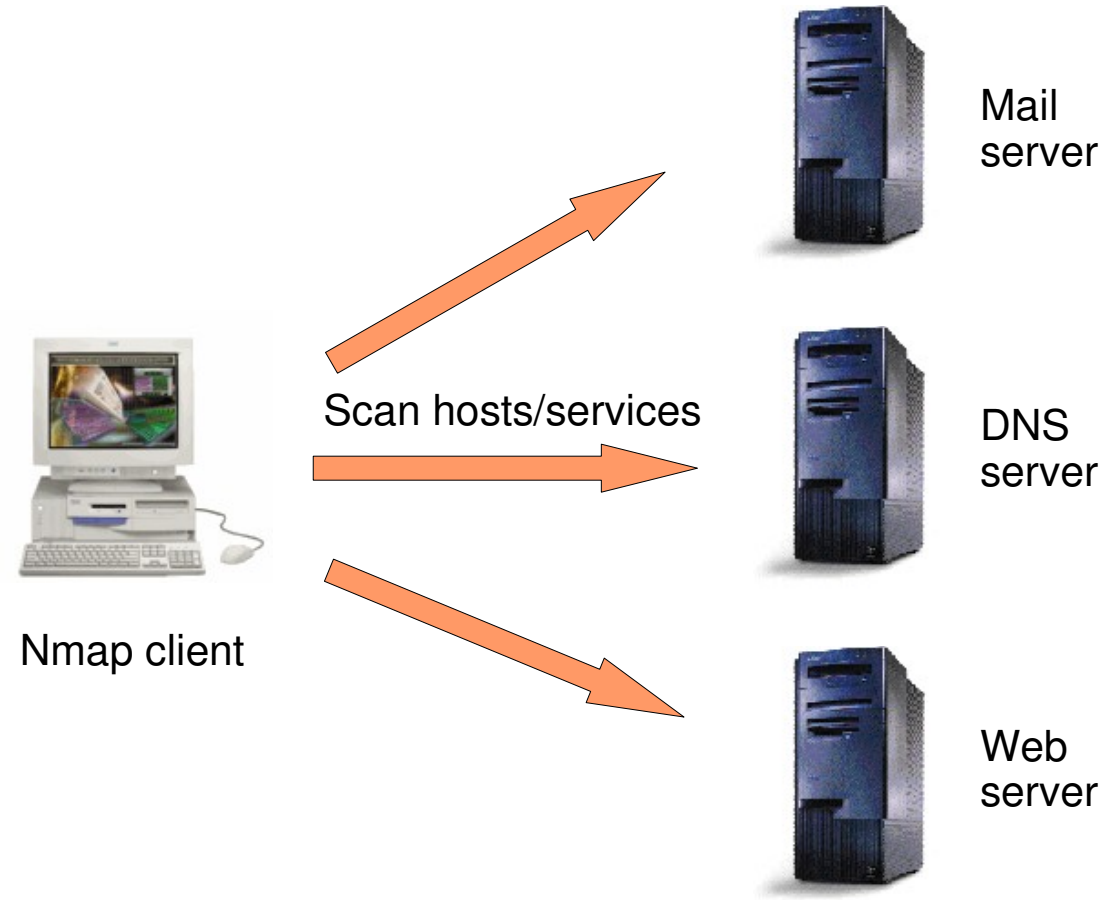
File System Integrity

- A security administrator must ensure that the configuration files and binaries crucial to system security and operation are not tampered with
- It is generally seen that crackers after breaking in a system, most often make changes to system configuration files and leave Trojans
- Trojans are programs that mimic the real program however also conducts certain other tasks as assigned by the cracker

- There are various tools that can report changes to File System
  - AIDE
  - Osiris
  - Tripwire

Network Scanning

- Network Mapper
- Powerful utility for network exploration and security auditing
- Can scan a large network rapidly
- Can determine hosts information available in the network
- Can list ports available in hosts
- Can Reports Operating System versions
- Can report existence of packet filters/Firewalls
- Runs on most Operating systems
- Both Console and Graphical versions available
- Free Software


Mail
server
Scan hosts/services
DNS
server
Nmap client
Web
server

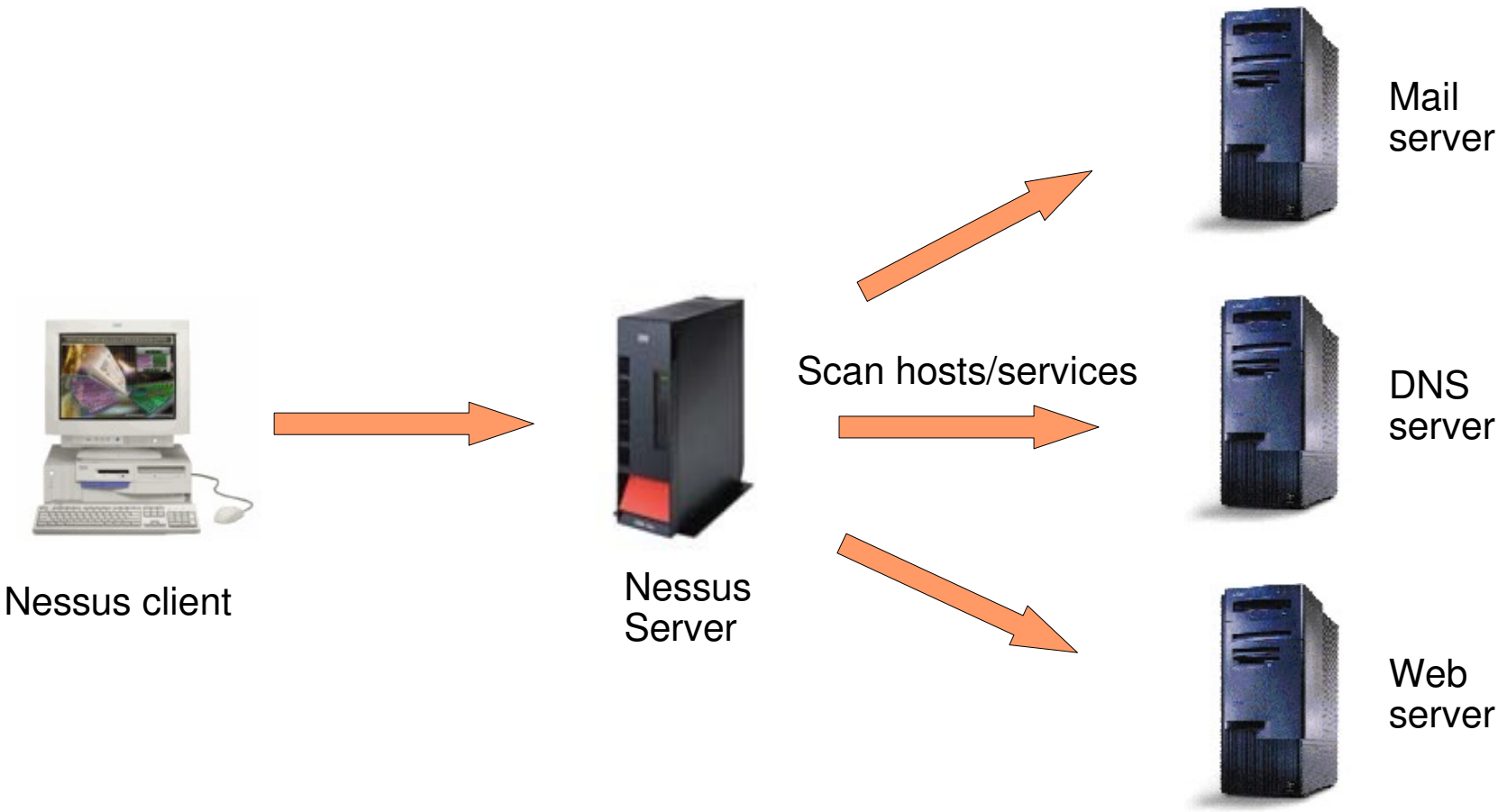
- Target Selection
  - Specify targets on the command line or in a filename with the '-i' option
    - $ nmap 192.168.0.1
    - $ nmap 192.168.0.0/24
    - $ nmap www.nosuchdomain.com
    - $ nmap -i iplist.txt

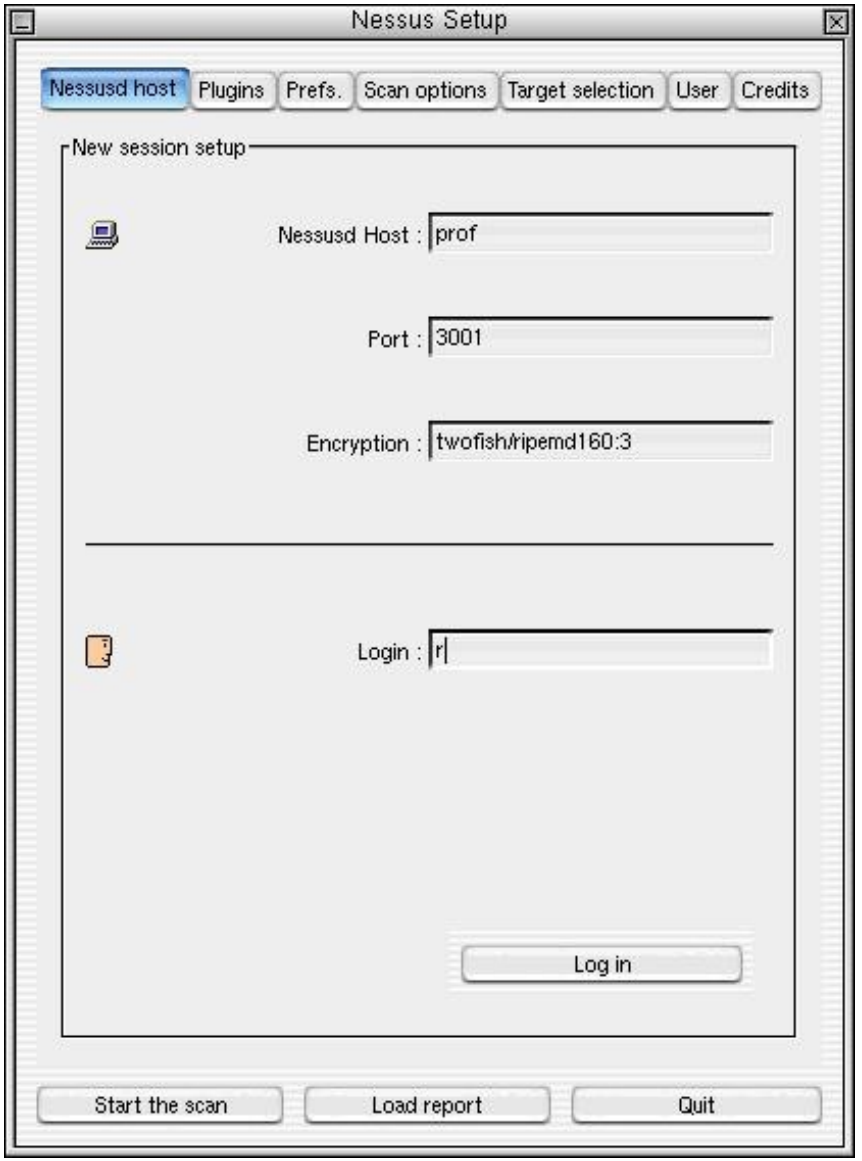
- Ping Scan
  - Sends ICMP echo request
  - Also sends TCP ACK to port 80 and expects RST
  - Third option is to sent TCP SYN to port 80 and expect RST or SYN/ACK
  - Pinging is done by default
  - Ping can be disabled by option '-P0'

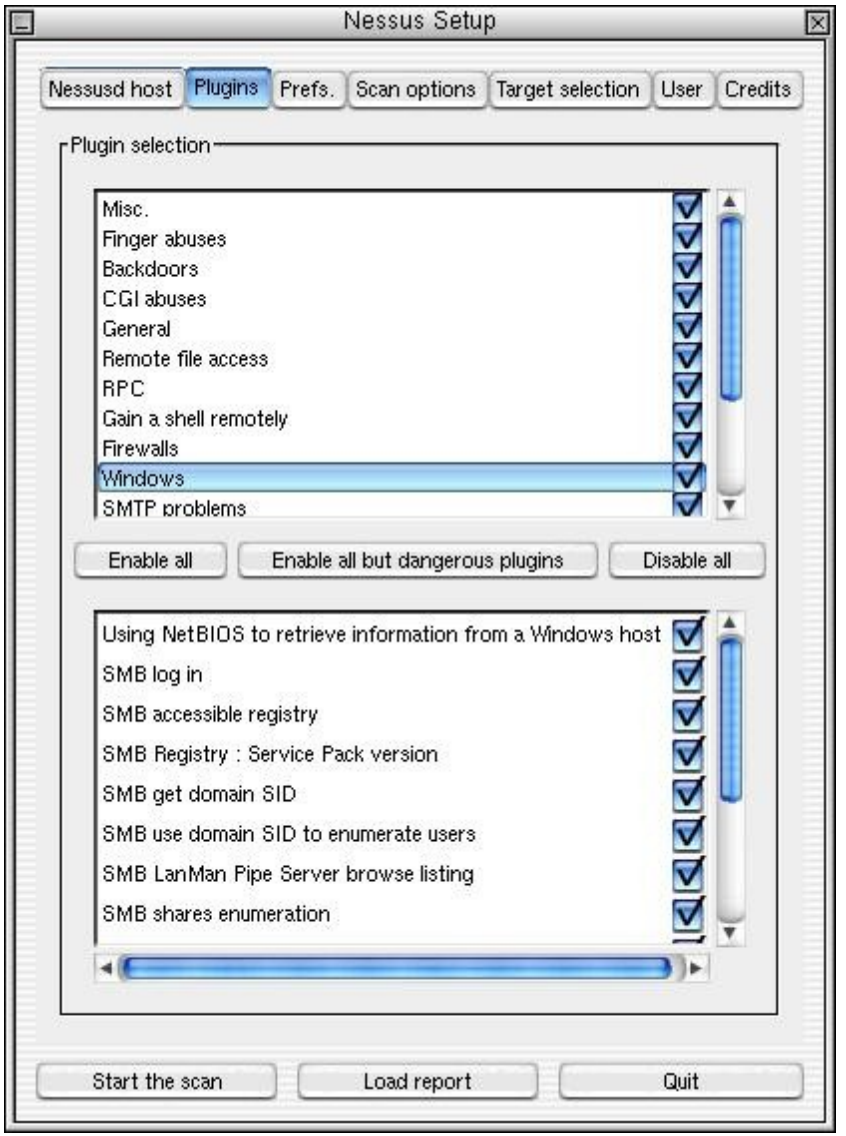
- The vanilla scan is a tcp connect() scan '-sT'
- SYN scan (-sS) also called “half-open” scans sends a SYN packet and looks for a SYN/ACK (open) or RST (closed).
- Syn scan tears down the connection before sending the ACK that would normally complete the TCP 3way Handshake
- FIN (-sF), XMAS (-sX) and NULL (-sN) scans sends following tcp flags to probe networks
  - FIN FIN
  - XMAS FIN,URG,PUSH
  - NULL NULL Flags
- UDP Scanning (-sU) sends 0 sized udp packets to scan udp ports on target machine

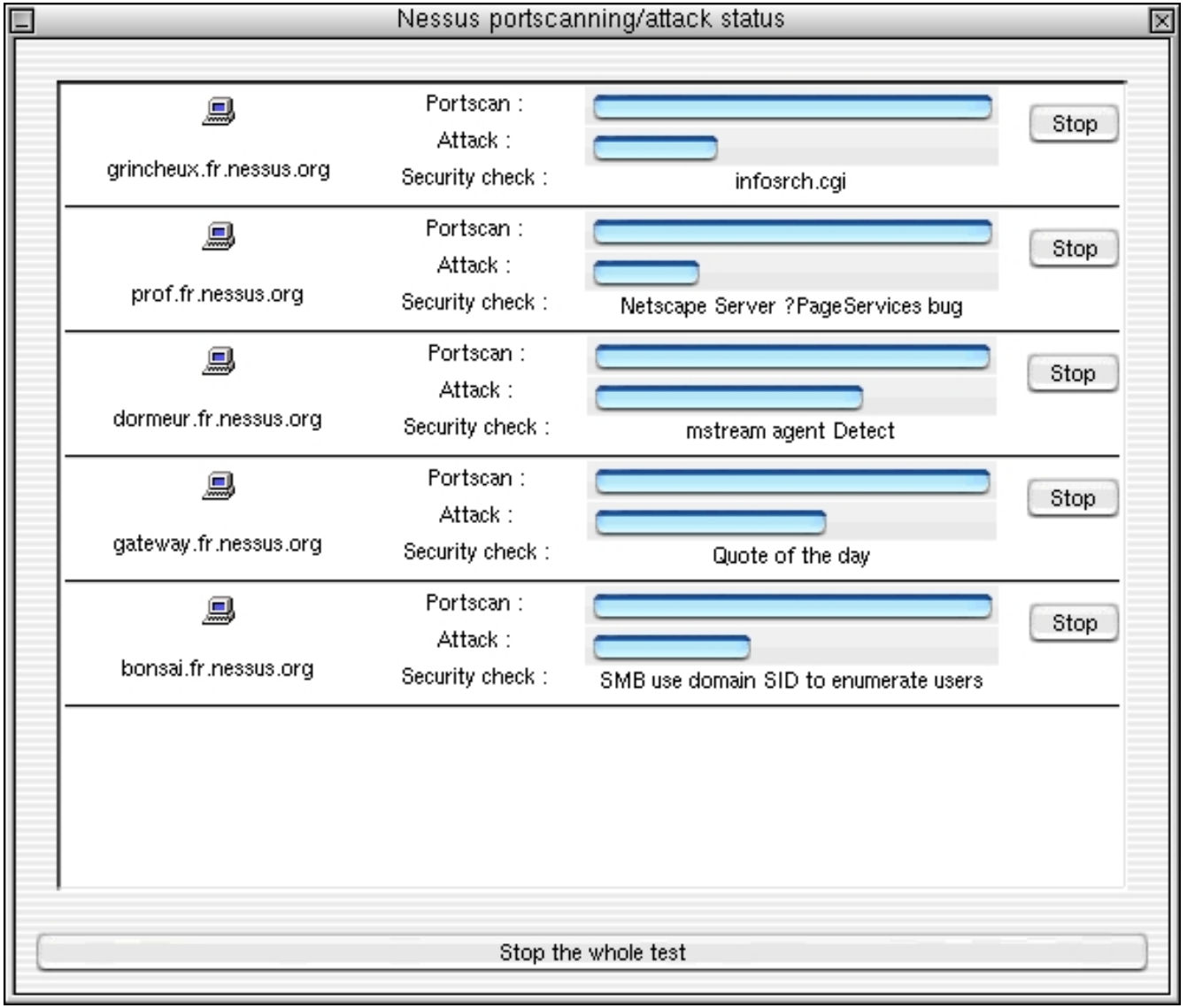
- Security Scanner to remotely audit the network
- Determines what services are running on which hosts and the vulnerabilities associated with them
- Nessus can also detect services running on non standard ports
- Very fast and reliable
- Has Modular architecture
- Plug-ins can be made according to need
- up2date security vulnerabilities database
- Client Server Architecture
- Can test number of hosts at the same time
- Complete report of vulnerabilities, risk level, and fixes
- Exportable report - as ASCII, XML, HTML
- Full SSL support for https, imaps, smtps
- Destructive/Non-Destructive test option

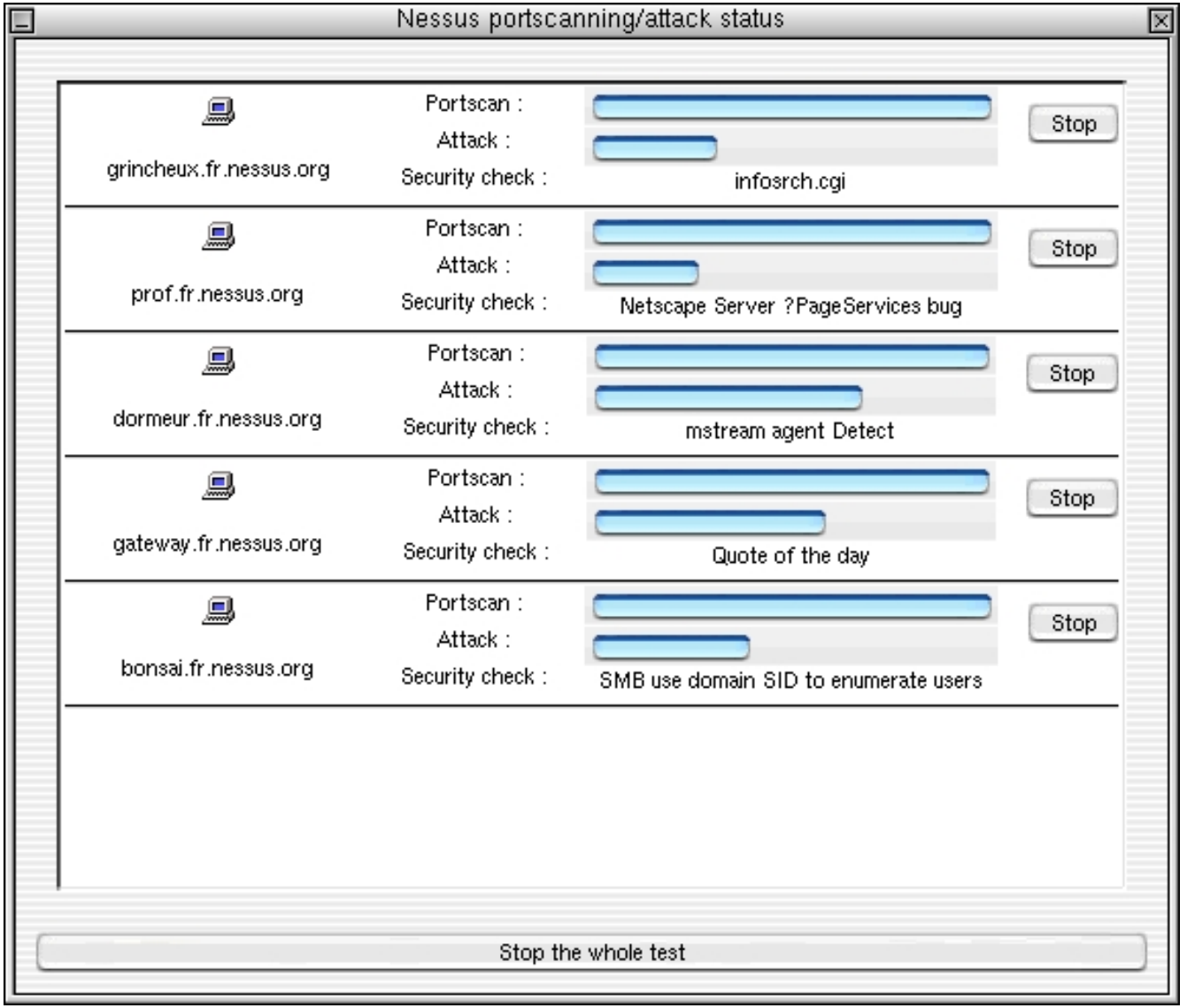
- Nessus is made up of two parts client and server
  - Server: Unix like system required
  - Client: Unix like system / Windows
- Comes as a standalone package that auto-installs itself
- Before running nessus please make sure that nessus can bypass the firewall policy for effective estimation of vulnerabilities


Nessus client
Nessus Server
Scan hosts/services
Mail server
DNS server
Web server


Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
Credits
New session setup
Nessusd Host : prof
Port : 3001
Encryption : twofish/ripemd160:3
Login : r
Log in
Start the scan
Load report
Quit


Nessus Setup
Nessusd host
Plugins
Prefs.
Scan options
Target selection
User
Credits
Plugin selection
Misc.
Finger abuses
Backdoors
CGI abuses
General
Remote file access
RPC
Gain a shell remotely
Firewalls
Windows
SMTP problems
Enable all
Enable all but dangerous plugins
Disable all
Using NetBIOS to retrieve information from a Windows host
SMB log in
SMB accessible registry
SMB Registry : Service Pack version
SMB get domain SID
SMB use domain SID to enumerate users
SMB LanMan Pipe Server browse listing
SMB shares enumeration
Start the scan
Load report
Quit


Nessus portscanning/attack status
grincheux.fr.nessus.org
Portscan :
Attack :
Security check :
infosrch.cgi
Stop
prof.fr.nessus.org
Portscan :
Attack :
Security check :
Netscape Server ?PageServices bug
Stop
dormeur.fr.nessus.org
Portscan :
Attack :
Security check :
mstream agent Detect
Stop
gateway.fr.nessus.org
Portscan :
Attack :
Security check :
Quote of the day
Stop
bonsai.fr.nessus.org
Portscan :
Attack :
Security check :
SMB use domain SID to enumerate users
Stop
Stop the whole test

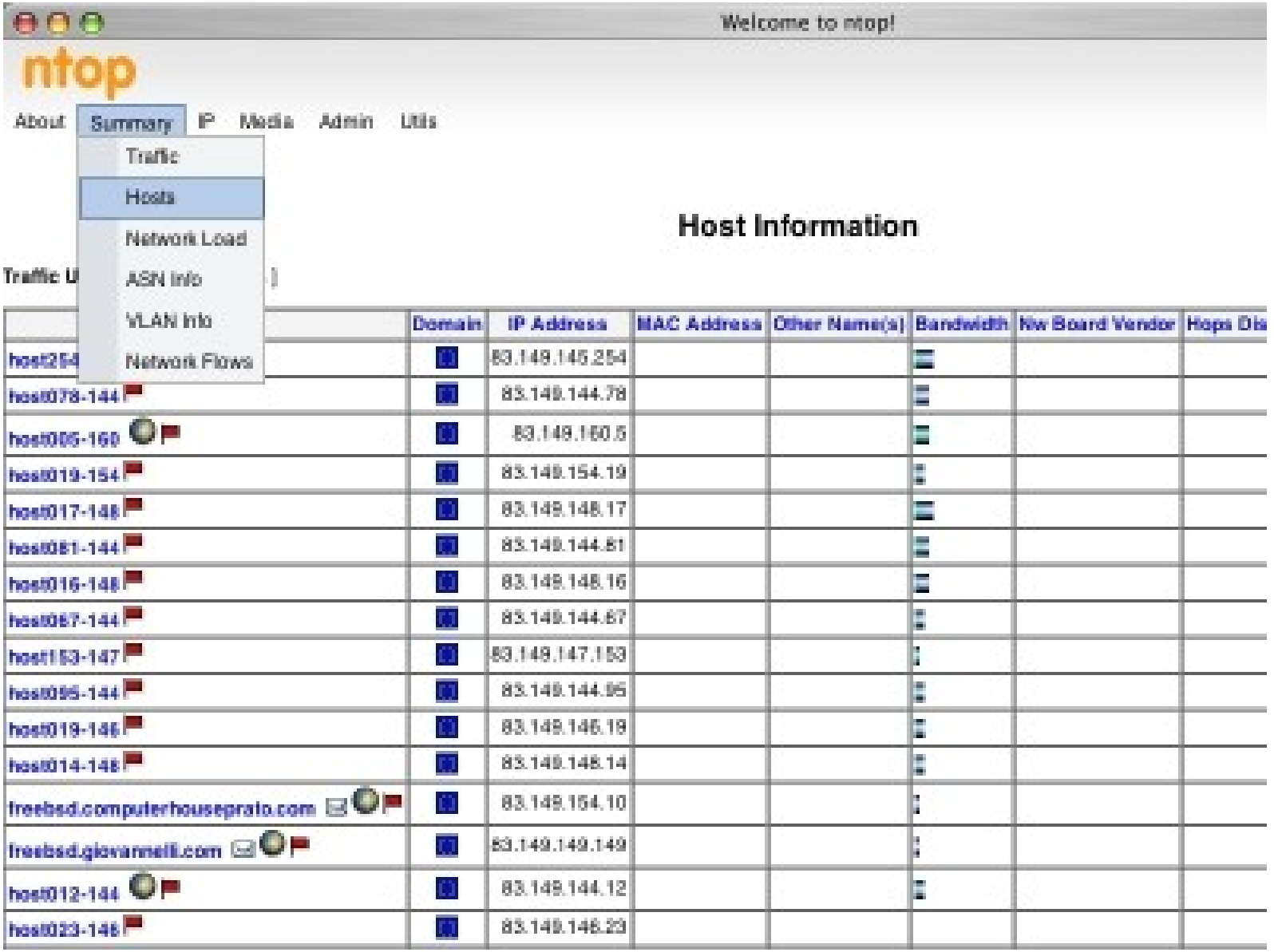

Nessus portscanning/attack status
grincheux.fr.nessus.org
Portscan :
Attack :
Security check :
infosrch.cgi
Stop
prof.fr.nessus.org
Portscan :
Attack :
Security check :
Netscape Server ?PageServices bug
Stop
dormeur.fr.nessus.org
Portscan :
Attack :
Security check :
mstream agent Detect
Stop
gateway.fr.nessus.org
Portscan :
Attack :
Security check :
Quote of the day
Stop
bonsai.fr.nessus.org
Portscan :
Attack :
Security check :
SMB use domain SID to enumerate users
Stop
Stop the whole test

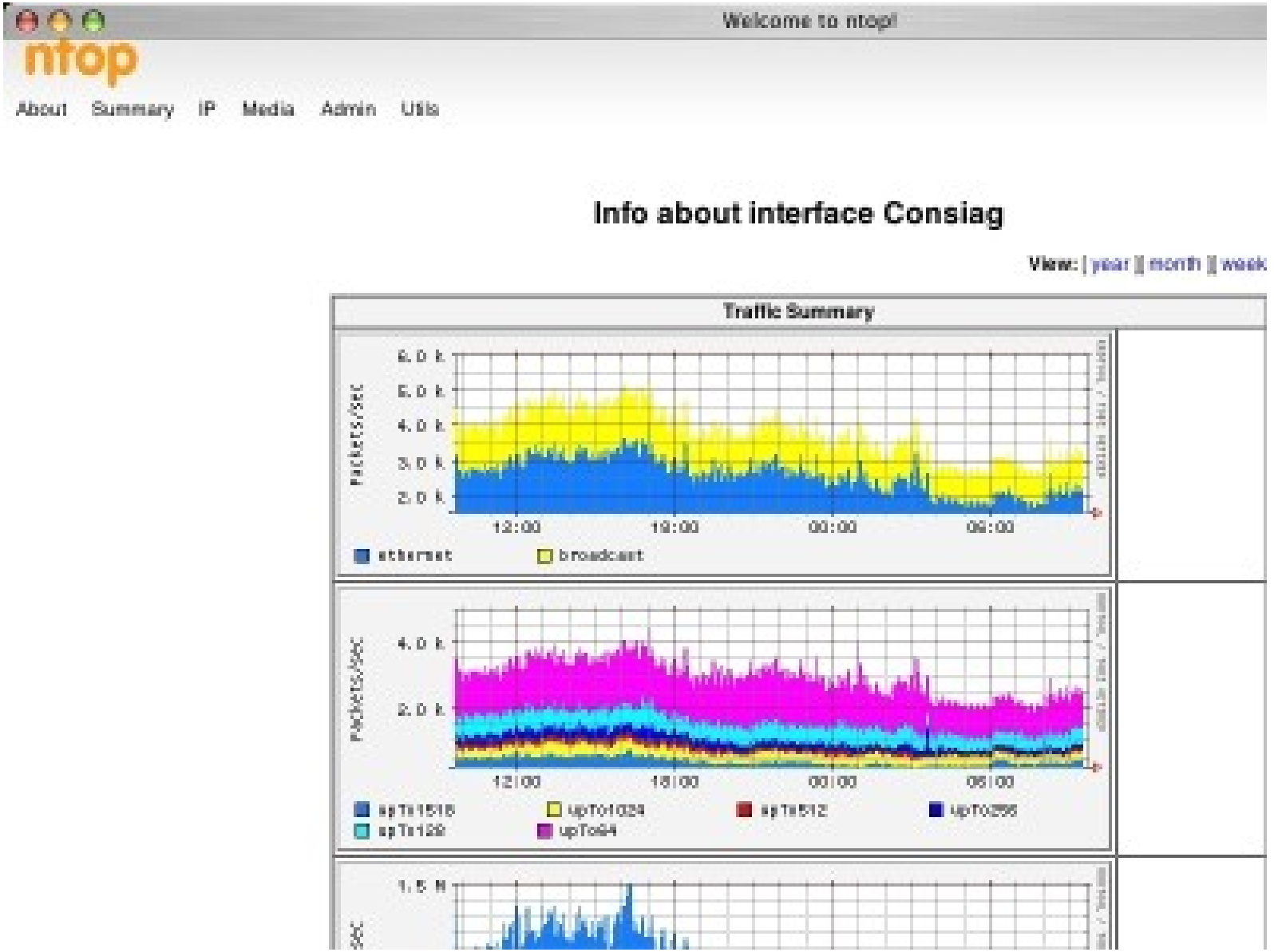
- tcpdump is a traditional utility available in Unix to sniff packets
- Based on libpcap
- Can sniff packets destined for local hosts
- Can sniff packets for the whole network in promiscuous mode
- Various options are available for sniffing packets
- Wireshark(formerly known as ethereal) is GUI based analyzer which can capture packets itself or read tcpdump files to analyze traffic

- Source network 192.168.0.0/24
  - # tcpdump -i em0 src net 192.168.0.0/24
- Without Hostname Translation
  - # tcpdump -i em0 -n src net 192.168.0.0/24
- Without Port name translation
  - # tcpdump -i em0 -nn src net 192.168.0.0/24
- Src 192.168.0.0/24 and Destination 192.168.0.1
  - # tcpdump -i em0 src net 192.168.0.0/24 and dst 192.168.0.1

- Protocol Specific
  - # tcpdump -i em0 tcp
  - # tcpdump -i em0 ! arp
- Print packets in Hex and ASCII
  - # tcpdump -X -i em0

- ntop is a network traffic monitoring program
- It is based on libpcap
- It can also act as a netflow collector
- Some of the features of ntop are
  - Traffic Statistics
  - Sort network traffic according to protocol,source/destination address,ports etc
  - Identify Host OS on the network
  - Report IP traffic Usage
  - Monitor suspicious traffic
  - Web page to monitor and administer ntop


Welcome to ntop!
ntop
About
Summary
IP
Media
Admin
Utils
Traffic
Hosts
Network Load
ASN Info
VLAN Info
Network Flows
Host Information
Traffic U
Domain
IP Address
MAC Address
Other Name(s)
Bandwidth
Nw Board Vendor
Hops Dis
host254
83.149.145.254
host078-144
83.149.144.78
host005-160
83.149.160.5
host019-154
83.149.154.19
host017-148
83.149.148.17
host081-144
83.149.144.81
host016-148
83.149.148.16
host067-144
83.149.144.67
host153-147
83.149.147.153
host095-144
83.149.144.95
host019-146
83.149.146.19
host014-148
83.149.148.14
freebsd.computerhouseprato.com
83.149.154.10
freebsd.giovanneli.com
83.149.149.149
host012-144
83.149.144.12
host023-148
83.149.148.23


Welcome to ntop!
ntop
About
Summary
IP
Media
Admin
Utils
Info about interface Consiag
View: [year][month][week
Traffic Summary
Packets/Sec
6.0 k
5.0 k
4.0 k
3.0 k
2.0 k
12:00
18:00
00:00
06:00
ethernet
broadcast
Packets/Sec
4.0 k
2.0 k
12:00
18:00
00:00
06:00
upTo1024
upTo512
upTo256
upTo64
1.5 M

Intrusion Detection

- Intrusion Detection System (IDS) analyzes IP packets looking for know patterns in real time
- IDS can give valuable information on unauthorized access to your network
- IDS can be Host based of Network Based

- Watches for packets coming into a single host
- The host based IDS doesn't listen on interfaces in promiscuous mode
- Programs that parse the system log files for security related informations can also be termed as Host based IDS
- HIDS reports incidents that seems suspicious and alert the administrators
- Examples
  - Portsentry
  - fwlogwatch
  - chkrootkit
  - swatch
  - AIDE
  - Osiris
  - Tripwire

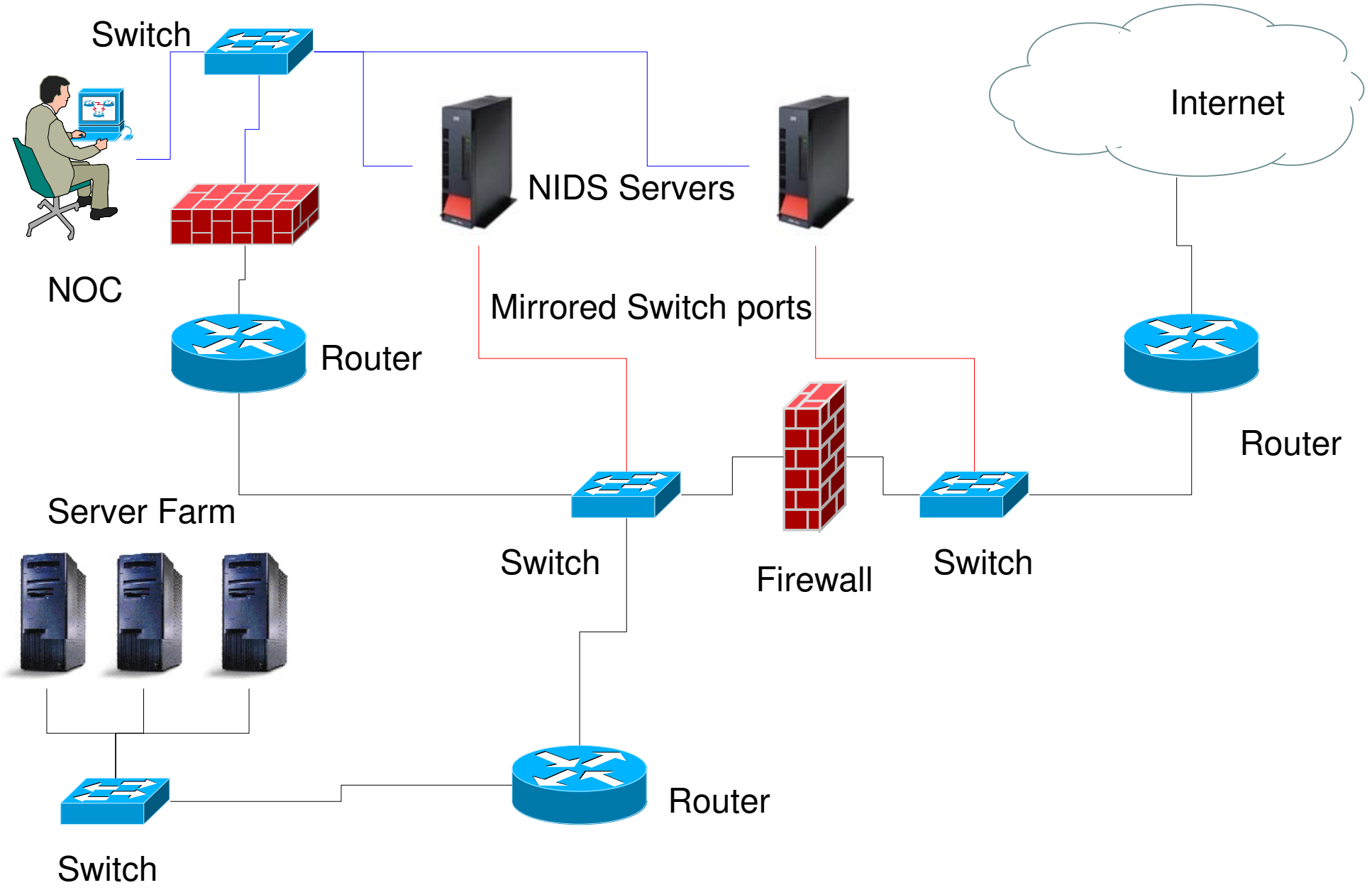
- Tool written to detect know Trojans and root kits installed in the system
- Check if the Ethernet interface is promiscuous mode
- Check if the lastlog/wutmp files are modified
- Check for logs created by sniffer programs

- http://www.chkrootkit.org

- Analyzes all IP packets coming into the network
- NIDS are generally deployed with port mirroring facility provided by most managed switches
- Such switches are configured to copy all data on port/ports and send it the port where NIDS is connected
- NIDS generally listen on interface in promiscuous mode and analyzes all data it receives
- Can also be used in Bridging Mode
- Snort is one of the most popular Network based IDS, and is also open source

- Network Intrusion Detection System (NIDS)
- Inspects/Sniffs all network traffic for abnormal contents
- Has built in signature base and anomaly detection
- String search for Known signatures with logging and reset features
- Rules based logging to perform content pattern matching detect a wide variety of attacks and probes
- Detects buffer overflows, stealth port scans, CGI attacks, SMB probes and much more
- Has Real-Time Alerting capability
  - syslog
  - SMB(Winpopup)
  - alert file

- Place snort before a firewall for maximum detection
- Use a Mirrored port if available
- Can also be operated in bridging mode


Switch
Internet
NIDS Servers
NOC
Mirrored Switch ports
Router
Router
Server Farm
Switch
Firewall
Switch
Router
Switch

Firewall

- People often think that a firewall provides the ultimate security, but they are wrong
- In most cases a mis configured firewall gives less or no security
- A firewall is a piece of software and should be treated the same way as any other softwares, because it is just as likely to contain bugs
- Firewall are used to enforce Access Control Policy between two networks such as the Internet and the Local Network

- Firewall are used to filter out unauthorized / Malicious traffic in or out of the network
- Firewall are used to protect the Internal Network from External network
- Firewall are used to protect services running in the network
- Firewall can not protect traffic that does not go through it

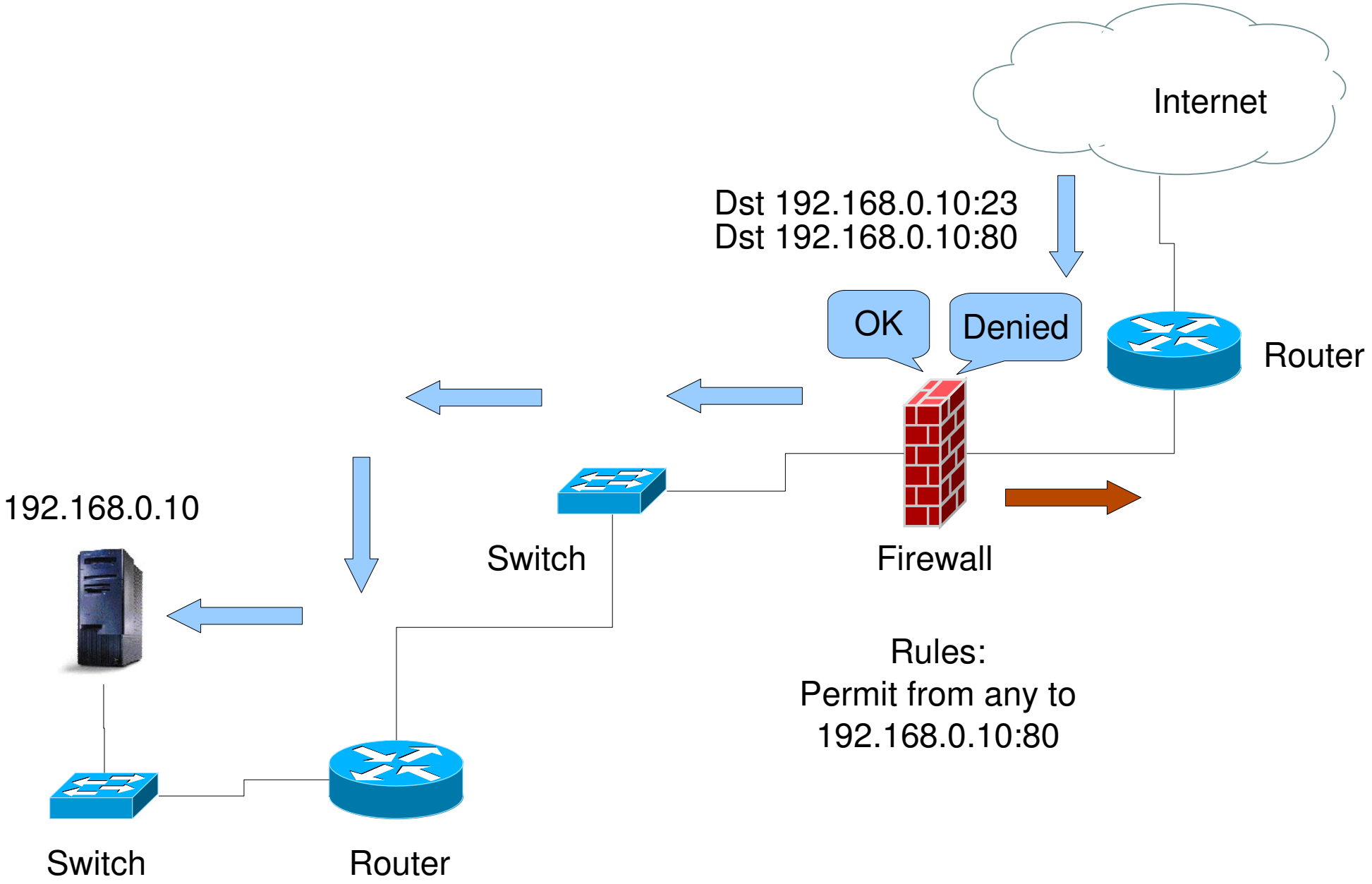
- Basically there are two Modes of Firewall
  - Packet Filtering Firewall
  - Application Gateway Firewall

- All network traffic are sent in the form of packets
- Large amount of data is split up into small packets for easy handling/routing and then reassembled when it arrives at destination
- In packet header of every packets contains information on how and where it should be delivered
- This very information is used by Packet Filtering Firewalls to implement Access control

- Packet Filtering is done on the basis of
  - Source/Destination IP address
  - Source/Destination Port
  - Protocol
  - Flags within a specified protocol
  - Combination of Above
- Examples
  - ipfw
  - pf
  - ipf

- Stateful Packet Filtering
  - Examines the state and the context of the packets (connection tracking)
  - An entry is made for each outgoing packet (request) and only replies (response) to these packets are allowed, and vice versa
  - Don't need to explicitly allow higher ports (1024:) as the stateful firewall will allow all required packets

- Advantages
  - Simple and Easy to Implement
  - Can give warnings of a possible attack
  - Good for stopping SYN Attacks and PING flood
- Disadvantages
  - Address information can be spoofed
  - Data within allowed packets can contain malicious codes that can exploit bugs
  - Usually a single point of failure


Internet
Dst 192.168.0.10:23
Dst 192.168.0.10:80
OK
Denied
Router
192.168.0.10
Switch
Firewall
Rules:
Permit from any to
192.168.0.10:80
Switch
Router

- The application gateway is a proxy for applications
- Exchange data with remote systems on behalf of the clients
- The Actual client is not visible to the Internet
- Protects the clients from the outside network by proxying request for them

- Filtering is done on the basis of
  - Source/Destination IP address
  - Source/Destination Port
  - Packet Content
  - File Type and Extensions
  - Time of Day
  - User Authentication
- Examples
  - squid

- Advantages
  - Can cache files for increased network performance
  - Detailed logging of all connections
  - Scalability, cache sharing , redundancy
  - No direct access to clients from Outside networks, not reachable from the Internet
  - Can alter packet contents on the fly
  - Considered to be the most secure since these services don't need to be run as root
- Disadvantages
  - Configuration and Implementation is complex

- Allow only needed services
- The default policy should be to Reject
- Firewall is an addition to the level of security, take other measures as well
- Regularly review/update firewall rules
- Regularly audit firewall logs for potential attacks
- Apart from the Main firewall, install firewall on individual hosts too
- Make sure traffic can't bypass the Firewall
- A central firewall should be running only the firewall software and sshd, and nothing else

ipfw

- FreeBSD has three different Firewall Packages
  - ipfw - IPFIREWALL
  - ipfilter - IPFILTER
  - pf - OpenBSD Packet Filter
- ipfw can be enabled at boot time by adding the following to rc.conf
  - firewall_enable=”YES”
  - firewall_script=”/etc/rc.firewall”
  - firewall_logging=”YES”
- The amount of logs can be controlled by adding the following to sysctl.conf
  - net.inet.ip.fw.verbose_limit=200
- ipfw can also be used for bandwidth limiting using Dummynet

- The following options can be used in the kernel config to build ipfw directly in the kernel
  - options IPFIREWALL
  - options IPFIREWALL_VERBOSE
  - options IPFIREWALL_VERBOSE_LIMIT=200
  - options IPFIREWALL_DEFAULT_TO_ACCEPT
    - Change the default rule to accept
  - options IPDIVERT
    - To enable NAT functionality using divert sockets

- List Firewall rules
  - ipfw list
  - ipfw l
- List Firewall rules with packet accounting information
  - ipfw -a list
- List Firewall rules with timestamps of last matches
  - ipfw -t list
- List the dynamic rules
  - ipfw -d list
- List the expired dynamic rules
  - ipfw -d -e list
- Clear the packet accounting counters
  - ipfw zero
  - ipfw zero RULENUM

- Adding a rule
  - ipfw add deny ip from any to any
- Rule number
  - Each rule is associated with a rule number in range 1 – 65535. The last rule number is reserved for the default rule. If a rule number is not specified , it is automatically assigned by the kernel
  - ipfw add 2000 allow ip from any to me
- Deleting a rule
  - ipfw delete 100

- The action of the rule define the fate of the packet
  - allow | accept | pass | permit
    - This action will accept the packet
  - check-state
    - This action will the check the packet against the dynamic rules table and if there is a match then executes the action associated with the rule which generated the dynamic rule
  - deny | drop
    - This action will discard the packet
- If logging is desired for the packet matching the rule, “log” keyword can be added after the action. It may also be followed by “logamount” keyword to limit the logs
  - ipfw add deny log logamount 200 ip from any to any

- You can specify the protocols in an ipfw rule
- Any protocols from /etc/protocols can be used
  - ip All IP Protocols
  - tcp TCP Packets
  - udp UDP Packets
  - icmp ICMP Packets
  - esp ESP Packet

  - ipfw add allow udp from me to any
    - Allow all udp packets from this host
  - ipfw add deny tcp from any to any
    - Deny all tcp packets from any to any
  - ipfw add deny icmp from any to me icmptypes 8
    - Disable icmp echo-request packets
- You can also specify port numbers in the rule
  - ipfw add allow tcp from any to me 80
    - Allow tcp packets from any to this machine on port 80

- You can match on the basis of packet direction
  - ipfw add allow tcp from me to any out
    - Match outgoing tcp packets from this host
  - ipfw add allow tcp from any to me 80 in
    - Match incoming tcp packets to port 80
- You can also use the via keyword to check the interface of the packet
  - ipfw add allow ip from any to any via lo0
    - Allow all packets coming in or going out from loopback interface

- You can match a start packet of a tcp session using the setup keyword. It will match the packets having the SYN only flag
  - ipfw add allow tcp from me to any 80 setup
- You can match a packet which has ACK or RST flag set using the established keyword
  - ipfw add allow tcp from any to any established
- keep-state keyword can be used to create stateful rules. keep-state will create dynamic rules which will be consulted during the processing of reply packets via check-state or the first keep-state rules
  - ipfw add allow tcp from me to any setup keep-state
  - ipfw add allow udp from me to any keep-state

- ipfw also provides ratelimiting
- limit keyword can be used to limit the number of packets matching based on :
  - source address
  - source port
  - destination address
  - destination port

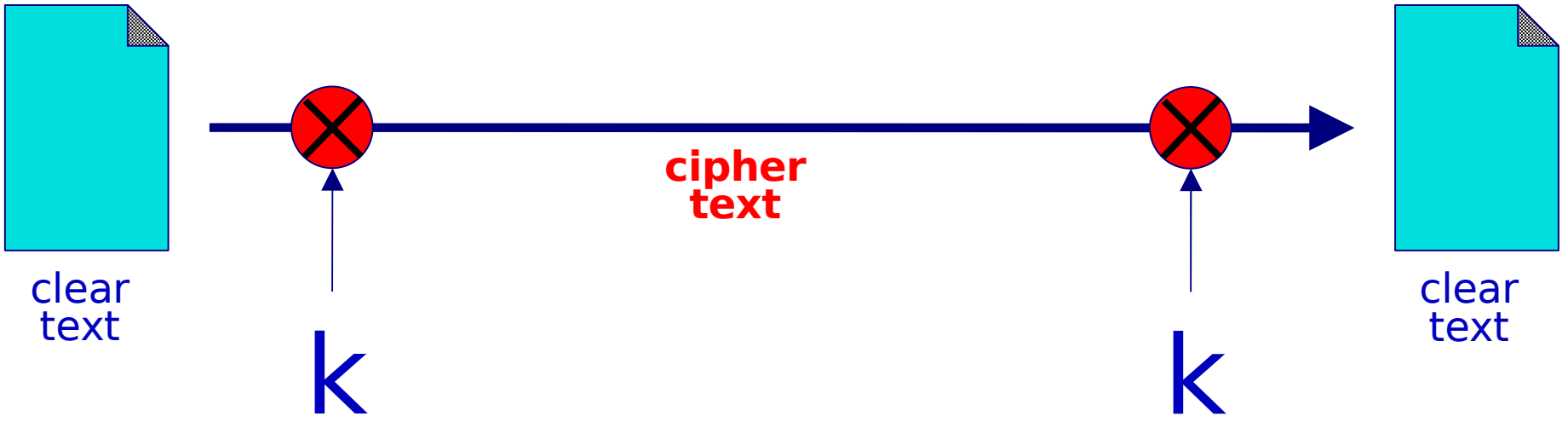
  - ipfw add allow tcp from any to me 80 limit src-addr 10
    - Only allow 10 connection per host on port 80

Cryptography

- Cryptography comes from a Greek word for “Secret writing”
- A cipher is a character-for-character or bit-for-bit transformation without regard to the linguistic structure of the message
- A code replaces one word with another word or symbol, not in used nowadays
- In cryptography the message to be encrypted,known as plaintext are transformed by a function that is parameterized by a key. The output of the encryption process is know as the ciphertext

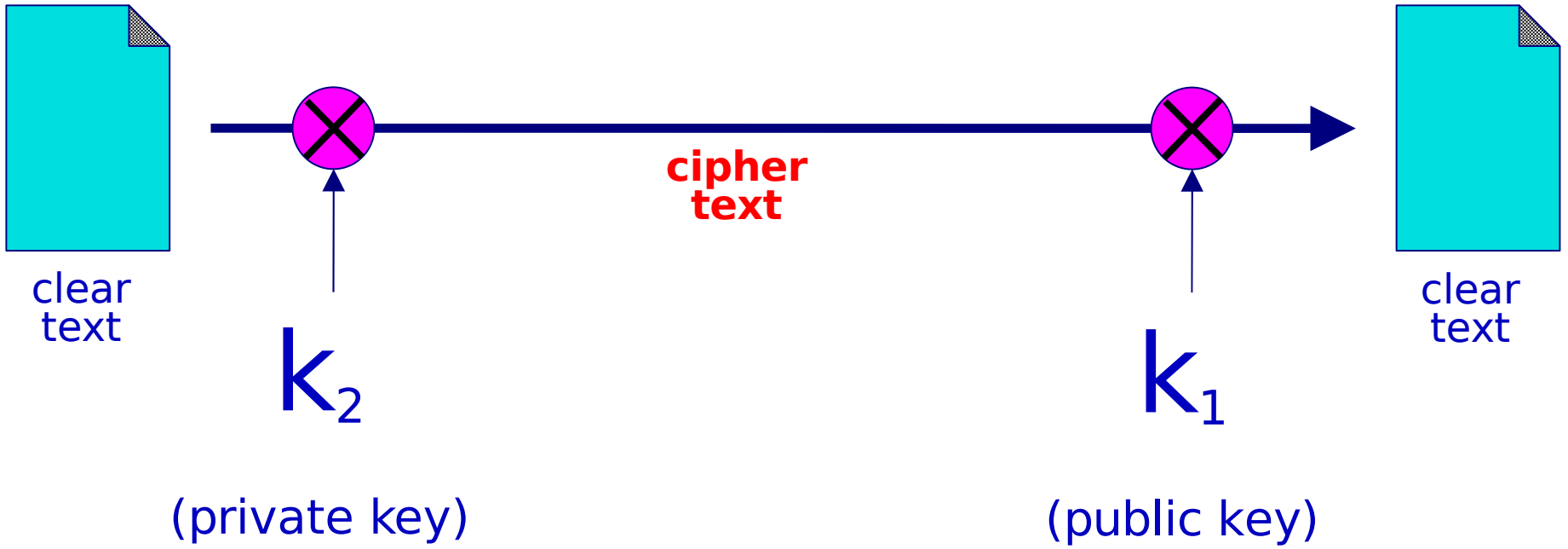
- Traditional Ciphers
  - Substitution ciphers
    - each letter of group of letters is replaced by another letter of group of letters
  - Transposition Ciphers
    - Reorder the the letters
  - One time pad
    - Here the plaintext is converted into a bit string which is Xor(exclusive OR) with another one time bit string

- Same key is used for encryption and decryption process
- The strength of the Encryption is related to the key length of the cipher
- Examples
  - DES (Data Encryption Standard)
  - Triple DES
  - AES (Advance Encryption Standard)
  - Blowfish
  - IDEA (patented not free)

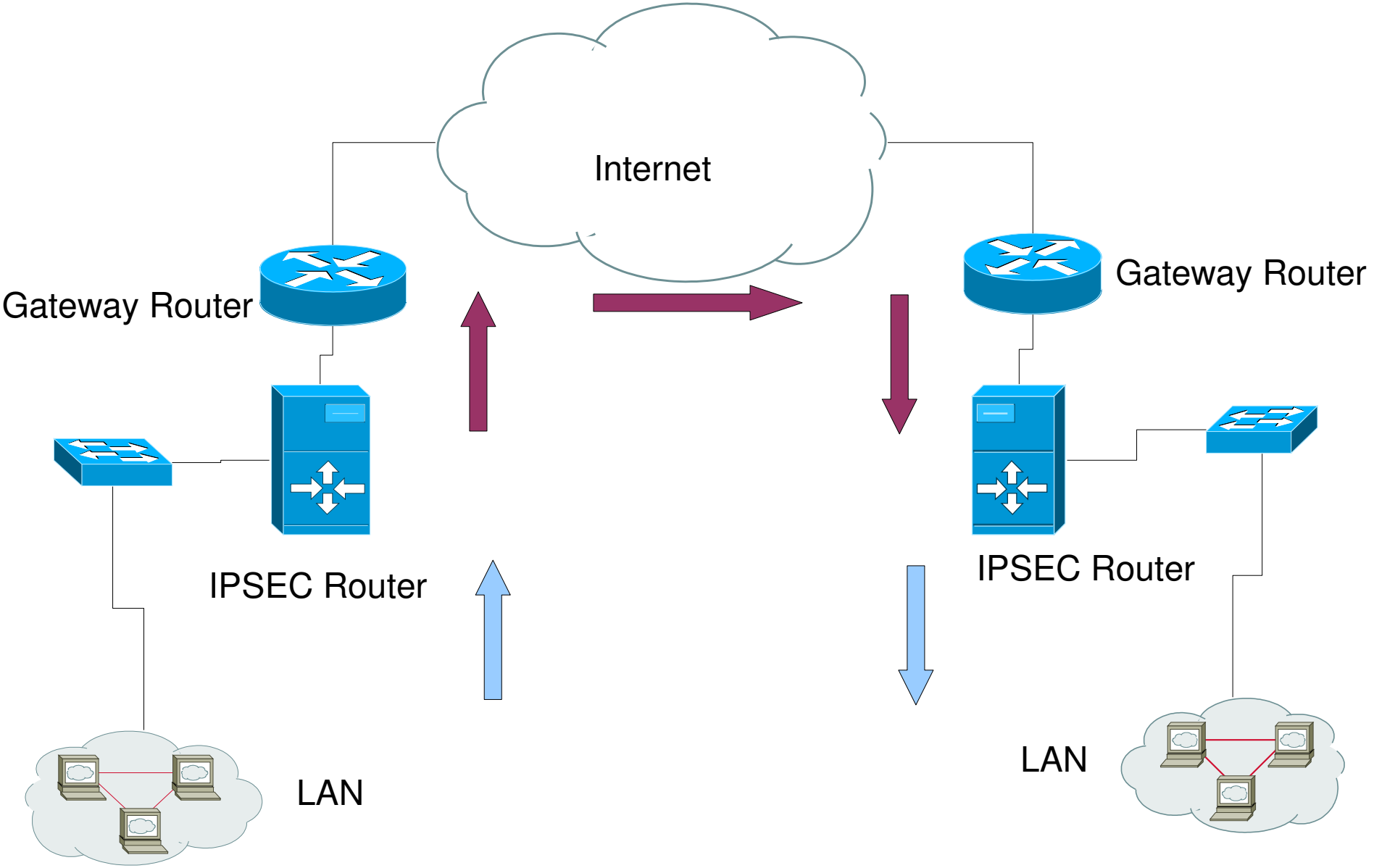

clear
text
k
cipher
text
k
clear
text

- Two keys are used for encryption and Decryption process
  - Private Key
  - Public Key
- The public key and private key are mathematically related (generated as pair)
- We can generate public key from private key but not private key from public key
- Public key cryptography can be used to encrypt or digitally sign messages
- Example : RSA (Rivest Shamit Adleman)

- The security of Private key is of paramount importance. Should be kept private as the name implies
- You must not loose it
- Prefer to have a backup on encrypted File systems at multiple places
- Protect the private key with a pass phrase
- Public key is meant to be distributed to others so that you can have secure communications with them

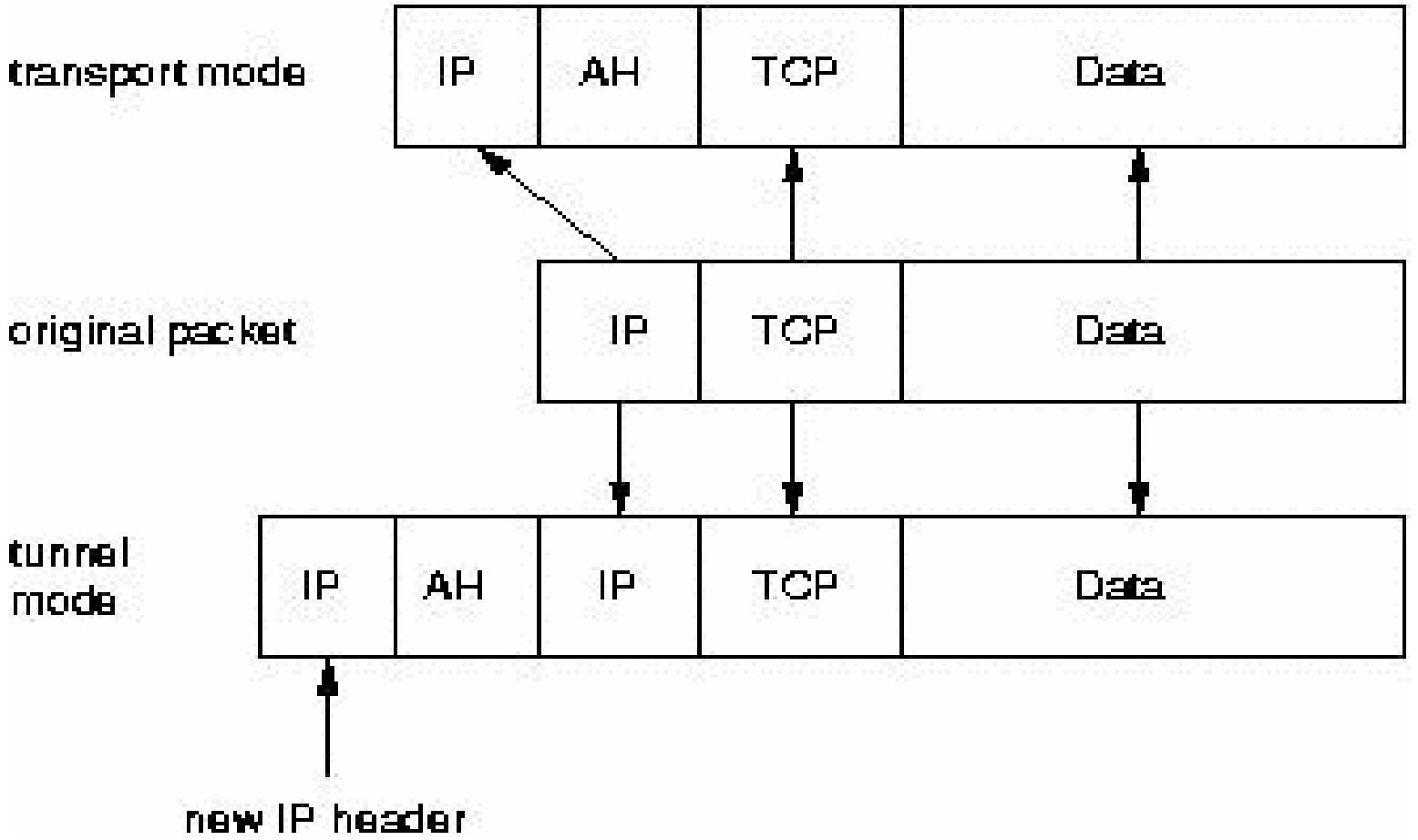

clear
text
cipher
text
clear
text
k_2
k_1
(private key)
(public key)

- Internet Protocol Security
- An effort by IETF to create cryptographically secure communications at the IP network level
- Uses Strong cryptography for both authentication and encryption services
- You can build secure tunnels through unsecure networks such as the Internet
- The data passing by this tunnel is encrypted by the originating gateway and decrypted by the terminating gateway
- It can be used to build Virtual Private Networks
- It was first developed for the IPv6 standard and then back ported to IPv4

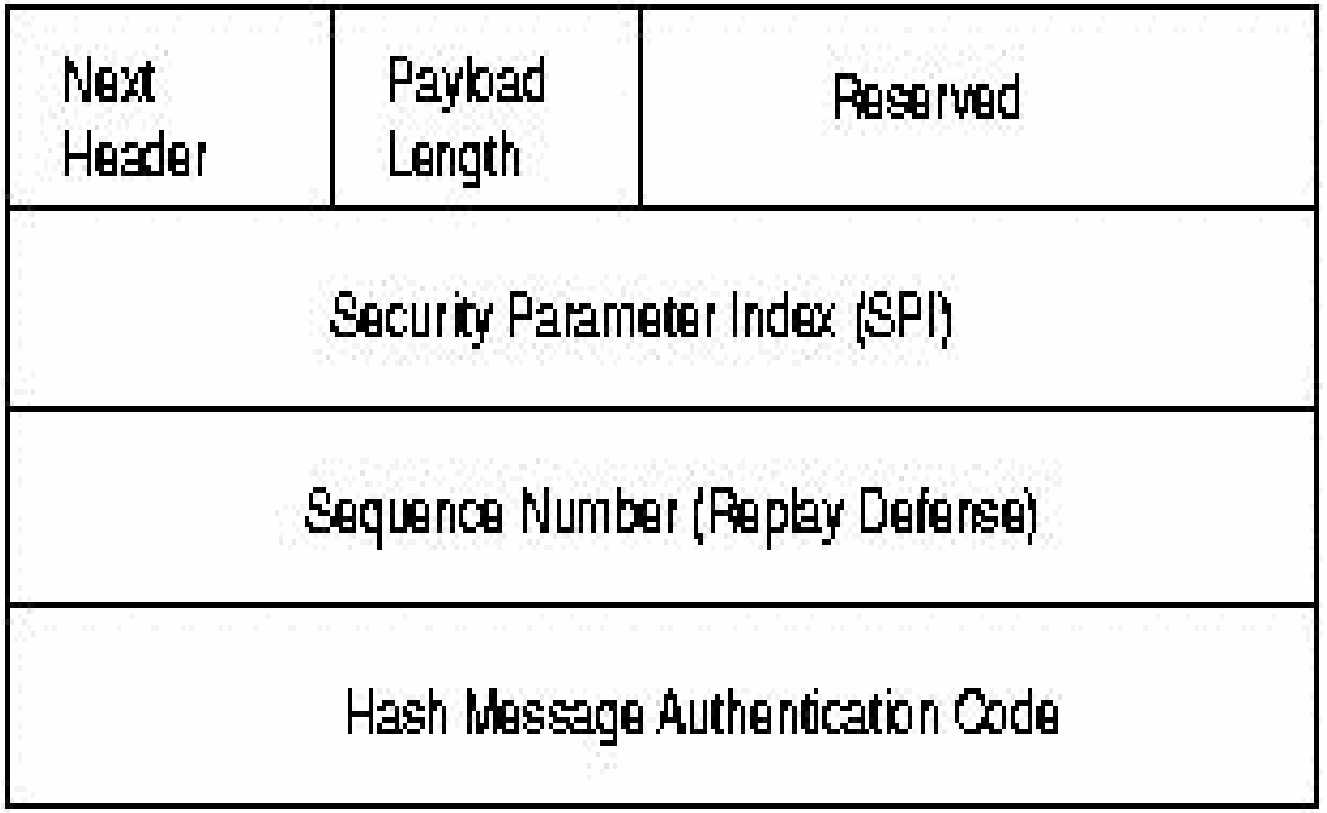

Internet
Gateway Router
Gateway Router
IPSEC Router
IPSEC Router
LAN
LAN

- To protect the integrity of the IP datagrams IPSEC uses Hash Message Authentication Codes (HMAC)
- To derive this HMAC , It uses hash algorithms such as MD5 and SHA to calculate a hash based on a secret key and the contents of the IP datagram
- This HMAC is then included in the IPSEC protocol header and the receiver of the packet can check the HMAC if it has access to the same secret key

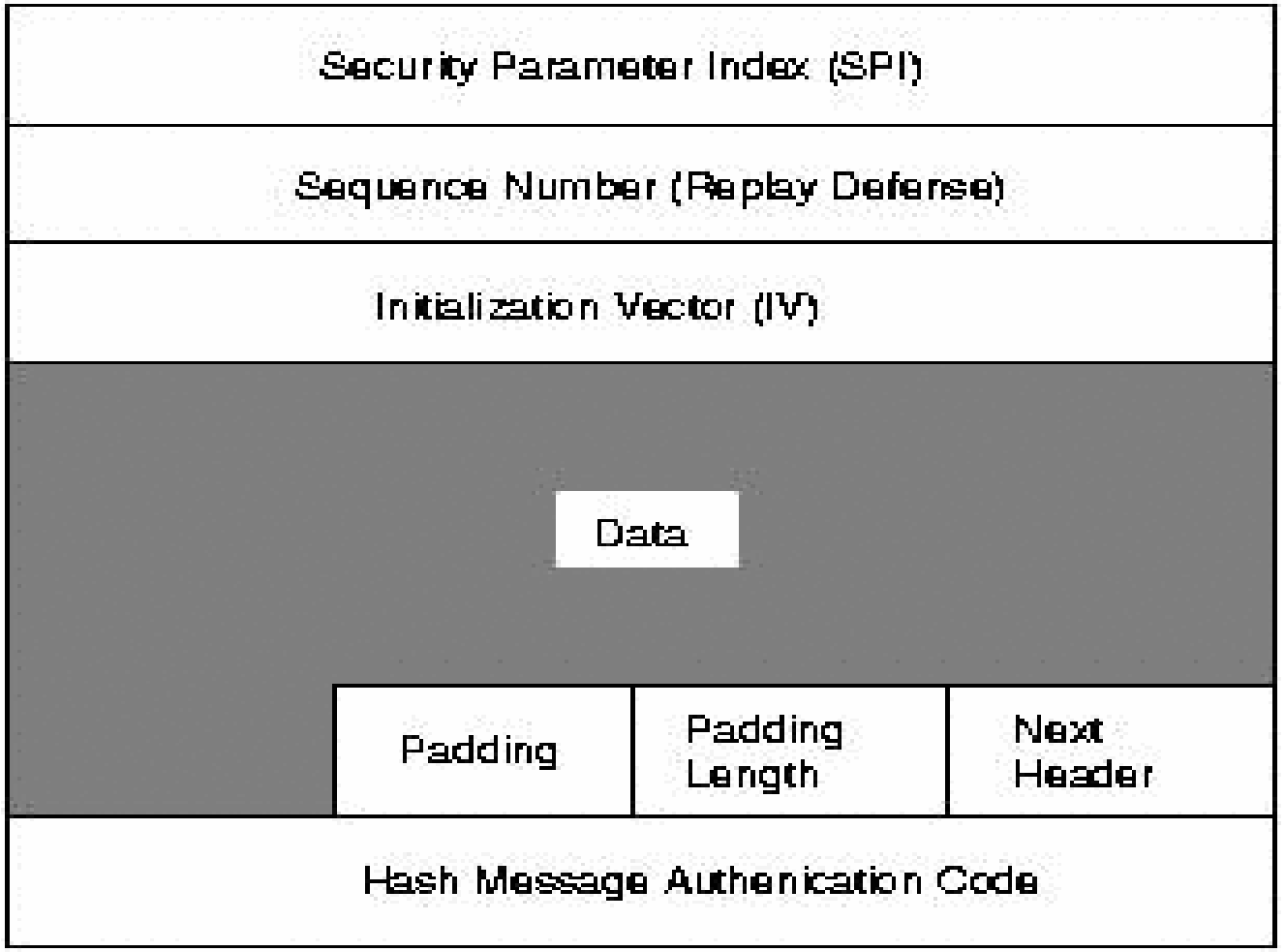
- To protect the confidentiality of the IP datagrams, IPSEC protocol uses standard symmetric encryption algorithms
- For the peer to be able to encapsulate and decapsulate the IPSEC packets they need a way to store the secret keys, algorithms and IP addresses involved
- All these parameters needed for the protection of the IP datagram are stored in a Security Association (SA).
- The Security Associations are in turn stored in a Security Association Database (SAD)


transport mode
IP
AH
TCP
Data
original packet
IP
TCP
Data
tunnel mode
IP
AH
IP
TCP
Data
new IP header

- Authentication Header (AH)
  - The AH protocol protects the integrity of the IP datagram
  - The AH protocol calculates a HMAC on the basis of the secret key, payload of the packet and immutable parts of the IP header like IP addresses
  - It then adds the AH header to the packet


Next Header
Payload Length
Reserved
Security Parameter Index (SPI)
Sequence Number (Replay Defense)
Hash Message Authentication Code

- Encapsulated Security Payload (ESP)
  - ESP protocol can both ensure the integrity of the packet using a HMAC and the confidentiality using encryption
  - After encrypting the packet and calculating the HMAC the ESP header is generated and added to the packet


Security Parameter Index (SPI)
Sequence Number (Replay Defense)
Initialization Vector (IV)
Data
Padding
Padding Length
Next Header
Hash Message Authentication Code

- IKE Protocol
  - The IKE protocol solves the most prominent problem in the setup of secure communication
    - Authentication of Peers
    - Exchange of symmetric keys
  - It then creates the security associations and populates the SAD
  - The IKE protocol usually requires a user space daemon and is not implemented in the Operating System
  - It used 500/udp port for its communication

- The IKE protocol functions in two phases
  - The first phase establishes a Internet Security Association Key Management Security Association (ISAKMP SA)
  - In the second phase the ISAKMP SA is used to negotiate and setup the IPSEC SAs
- The authentication of the peers in the first phase can usually be based on Pre-Shared Keys (PSK), RSA Keys and X.509 certificates

Thank You