REVA UNIVERSITY

Established as per the Section 2(f) of the UGC Act, 1956
Approved by AICTE, COA and BCI, New Delhi

Lecture 1.3

Introduction to Security Technology, Firewalls

School of Computing and Information Technology

Introduction Class

Recap of previous Lecture

RECAP OF PREVIOUS LECTURE

- Introduction
- Information Security Policy, Standards and Practices
- The Information Security Blueprint
- Contingency plan and a model for contingency plan.

INTRODUCTION TO SECURITY TECHNOLOGY, FIREWALLS

- ✓ Firewalls A firewall is a device that selectively discriminates against information flowing into or out of the organization.

- ✓ A firewall is usually a **computing device** or a specially configured computer that allows or **prevents access to a defined area based on a set of rules.** Firewalls are usually placed on the **security perimeter**, just behind or as part of a gateway router.

- ✓ While the gateway router's primary purpose is to connect the organization's systems to the outside world, it too can be used as the front-line defense against attacks, as it can be configured to allow only set types of protocols to enter.

INTRODUCTION TO SECURITY TECHNOLOGY, FIREWALLS

There are a number of types of firewalls

- packet filtering
- stateful packet filtering
- proxy
- Application level

they are usually classified by the level of information they can filter. A firewall can be a single device or a firewall subnet, which consists of multiple firewalls creating a buffer between the outside and inside networks as shown in Figure 5-11.

FIREWALLS

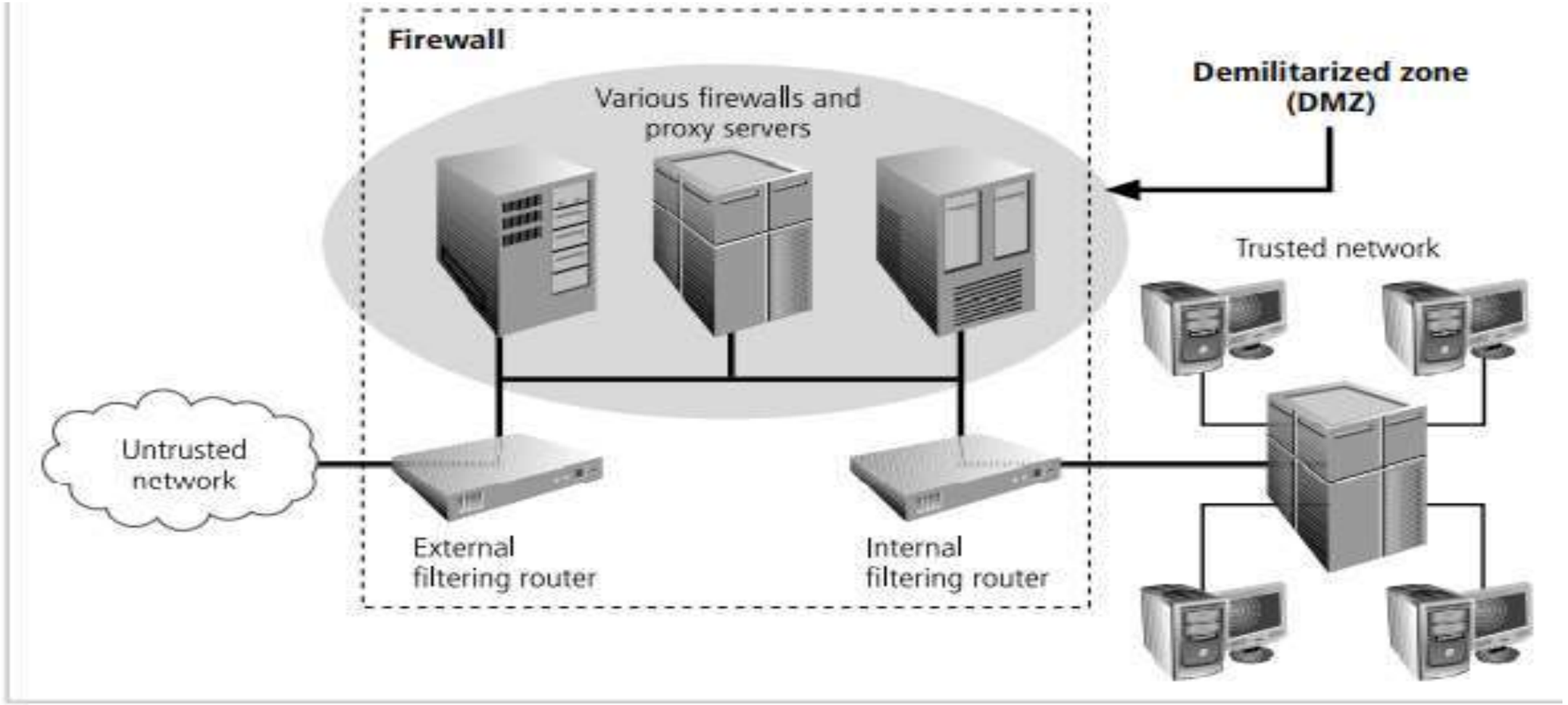


Figure 5-11 Firewalls, Proxy Servers, and DMZs

FIREWALLS

- ✓ DMZs A buffer against outside attacks is frequently referred to as a demilitarized zone (DMZ). The DMZ is a no-man's-land between. the inside and outside networks; it is also where some organizations place Web servers. **These servers provide access to organizational Web pages, without allowing Web requests to enter the interior networks.**

- ✓ Proxy Servers An alternative to firewall subnets or DMZs is a proxy server, or proxy firewall. A proxy server performs actions on behalf of another system.

- ✓ A proxy server is configured to look like a **Web server and is assigned the domain name** that users would be expecting to find for the system and its services. When an outside client requests a particular Web page, the proxy server receives the request as if it were the subject of the request, then asks for the same information from the true Web server (acting as a proxy for the requestor), and then responds to the request.

FIREWALLS, PROTECTING REMOTE CONNECTIONS

This gives requestors the response they need without allowing them to gain direct access to the internal and more sensitive server. The proxy server may be hardened and become a **bastion host** placed in the public area of the network, or it might be placed within the firewall subnet or the DMZ for added protection.

PROTECTING REMOTE CONNECTIONS

Definition:

Remote desktop is a program or an operating system feature that **allows a user to connect to a computer in another location,** see that computer's desktop and interact with it as if it were local. For example (Any Desk application)

How to Set Up Remote Desktop Connection?

Remote Desktop Connection (RDC) is a **Microsoft technology that allows a local computer to connect to and control a remote PC over a network or the Internet**.

It is done through a Remote Desktop Service (RDS) or a terminal service that uses the company's proprietary Remote Desktop Protocol (RDP).

PROTECTING REMOTE CONNECTIONS

- Advantages of firewall over Protecting Remote Connections

- Top Security
- Working Remotely
- Easy Access
- Savings

INTRUSION DETECTION SYSTEMS (IDS)

- ✓ To detect unauthorized activity within the inner network or on individual machines, organizations can implement intrusion detection and prevention systems (IDPSs).
- ✓ IDPSs come in two versions :
- ✓ Host-based IDPS are usually installed on the machines **they protect to monitor the status of various files stored on those machines.** The IPDS(intrusion prevention detection sytem) learns the configuration of the system, assigns priorities to various files depending on their value, and can then alert the administrator of suspicious activity.
- ✓ Network-based IDPSs look at **patterns of network traffic and attempt to detect unusual activity based on previous baselines**. This could include packets coming into the organization's networks with addresses from machines that are within the organization . It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial-of-service attack). The prevention component enables such devices to respond to intrusions by creating a new filtering rule that severs communications or other activity as configured by the administrator

INTRUSION DETECTION SYSTEMS (IDS)

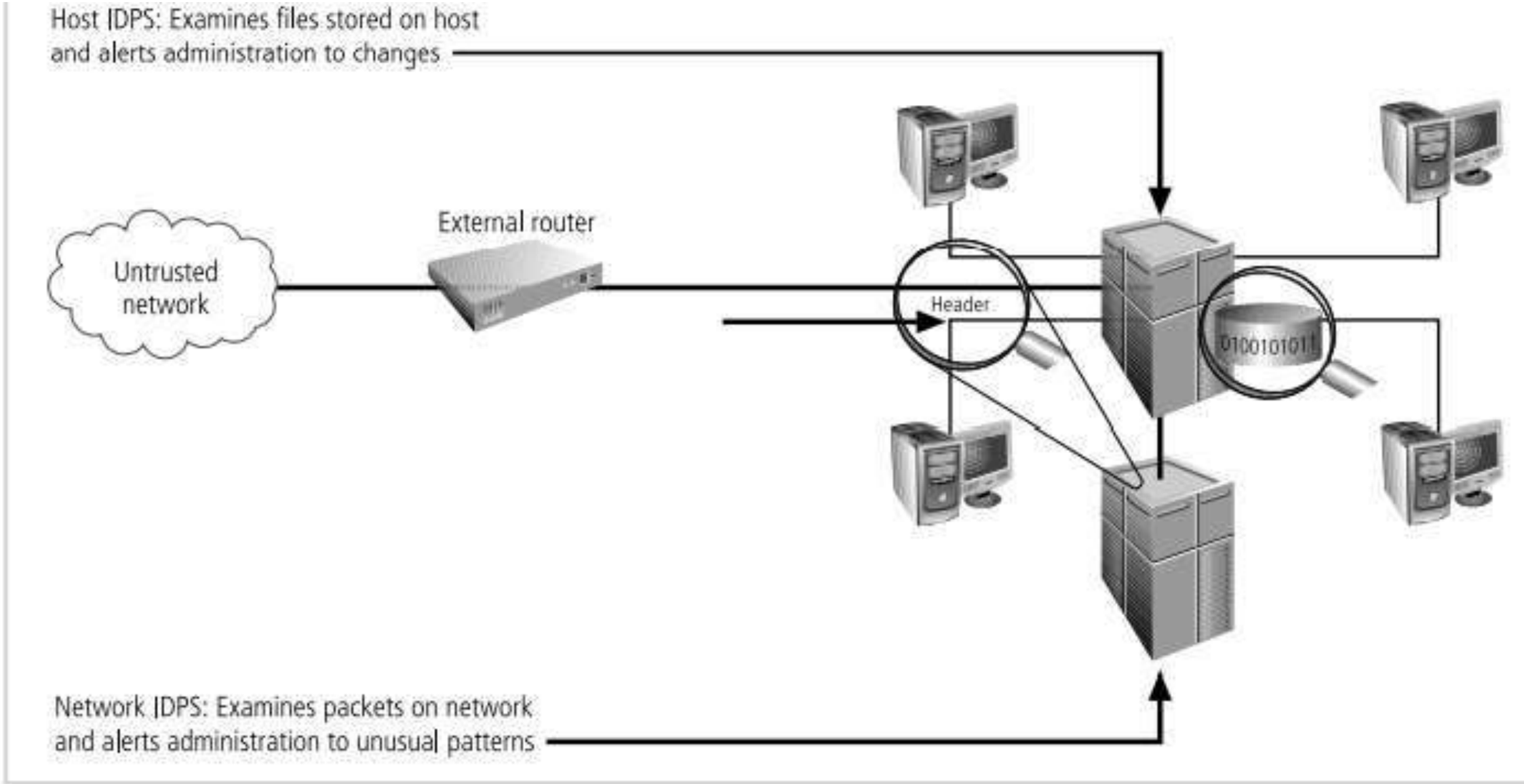


Figure 5-12 Intrusion Detection and Prevention Systems

HONEY POTS, HONEY NETS AND PADDED CELL SYSTEMS

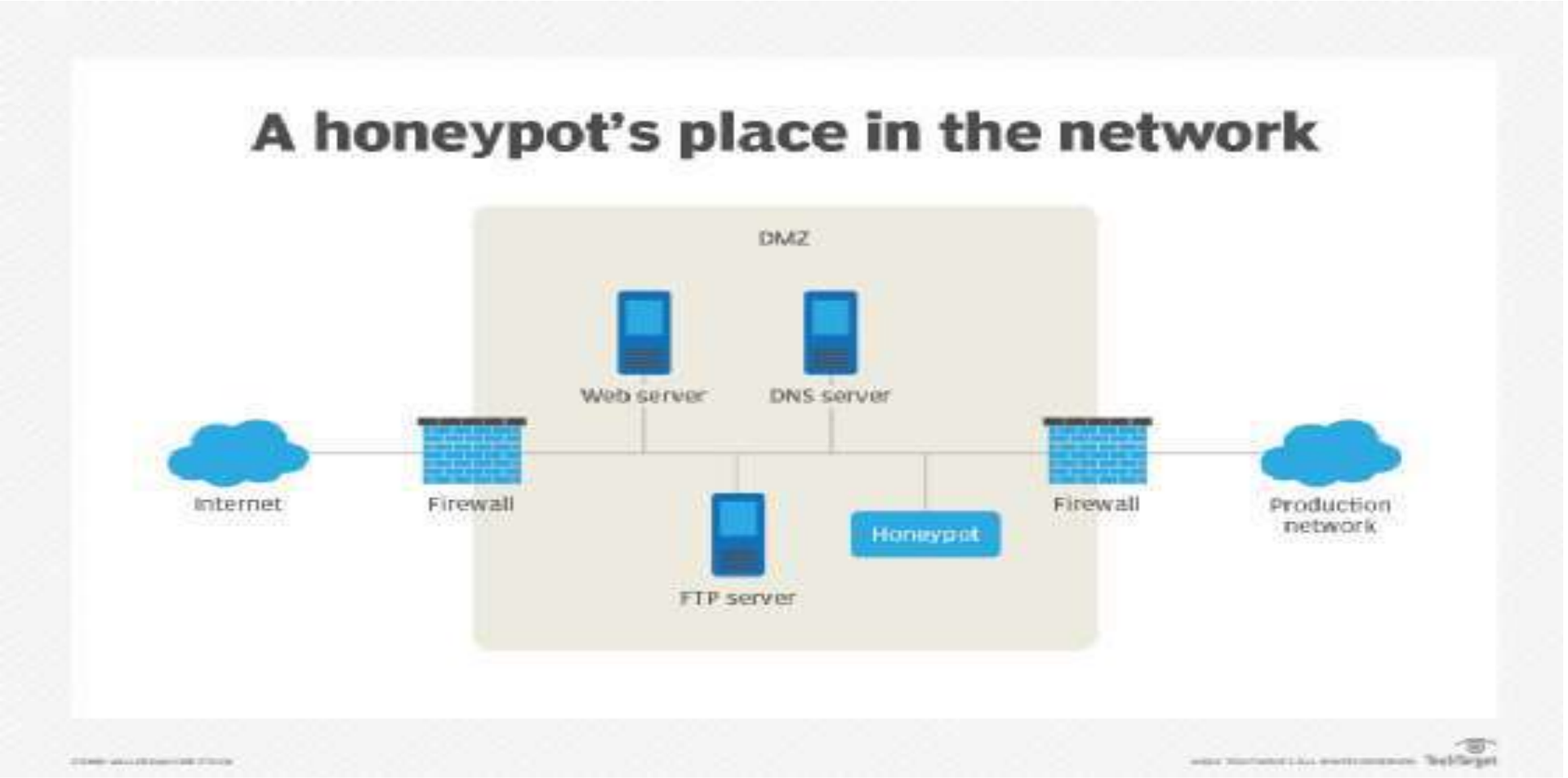
- ✓ Honeypots are instrumented with sensitive monitors and event loggers that detect attempts to access the system and collect information about the potential attacker's activities.
- ✓ Honeypots are decoy systems designed to lure potential attackers away from critical systems.
- ✓ In the industry, they are also known as decoys, lures, and fly-traps.
- ✓ When a collection of honeypots connects several honeypot systems on a subnet, it may be called a honeynet.
- ✓ A honeypot system (or in the case of a honeynet, an entire subnetwork) contains pseudo-services that emulate well-known services, but is configured in ways that make it look vulnerable to attacks.

Honeypots are designed to do the following:

- ✓ Divert an attacker from critical systems
- ✓ Collect information about the attacker's activity
- ✓ Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond.

HONEY POTS, HONEY NETS AND PADDED CELL SYSTEMS

- ✓ Because the information in a honeypot appears to be valuable, any unauthorized access to it constitutes suspicious activity.



PADDED CELL SYSTEMS

- ✓ A padded cell is **a simulated environment that may offer fake data to retain an intruder's interest**.
- ✓ **A padded cell is a honeypot that has been protected** so that it cannot be easily compromised—in other words, a hardened honeypot.
- ✓ In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS.
- ✓ When the IDPS detects attackers, it transfers them to a special simulated environment where they can cause no harm.

THE ADVANTAGES AND DISADVANTAGES OF USING THE HONEYPOT OR PADDED CELL APPROACH ARE SUMMARIZED BELOW:

Advantages:

- ✓ Attackers can be **diverted to targets** that they cannot damage.
- ✓ Administrators have **time to decide** how to respond to an attacker.
- ✓ Attackers' actions can be **easily and more extensively monitored**, and the records can be used to refine threat models and improve system protections.
- ✓ Honeypots may be **effective at catching insiders** who are snooping around a network.

Disadvantages:

- ✓ The **legal implications** of using such devices are not well understood.
- ✓ Honeypots and padded cells have not yet been shown to be generally useful security technologies.
- ✓ An expert attacker, **once diverted into a decoy system**, may become angry and launch a more aggressive attack against an organization's systems.
- ✓ Administrators and security managers need a **high level of expertise** to use these systems

SCANNING AND ANALYSIS TOOLS.

- ✓ Scanning tools are, as mentioned earlier, typically used as part of an **attack protocol** to collect information that an attacker would need to launch a successful attack.
- ✓ **The attack protocol is a series of steps or processes used by an attacker, in a logical sequence, to launch an attack against a target system or network.**
- ✓ One of the preparatory parts of the attack protocol is the collection of publicly available information about a potential target, a process known as foot printing.
- ✓ Foot printing is the **organized research of the Internet addresses owned or controlled by a target organization.**

TYPES OF SCANNING AND ANALYSIS TOOLS.

1. PORT SCANNERS

2. FIREWALL ANALYSIS TOOLS

3. OPERATING SYSTEM DETECTION TOOLS

4. VULNERABILITY SCANNERS

TYPES OF SCANNING AND ANALYSIS TOOLS.

1. PORT SCANNERS:

Port scanning utilities, or port scanners, are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.

- A port is a network channel or connection point in a data communications system.

- Within the TCP/IP networking protocol, TCP and User Datagram Protocol (UDP) port numbers differentiate the multiple communication channels that are used to connect to the network services being offered on the same network device.

- Each application within TCP/IP has a unique port number.

TYPES OF SCANNING AND ANALYSIS TOOLS.

2. FIREWALL ANALYSIS TOOLS :

- Understanding exactly **where an organization's firewall is located and what the existing rule sets on the firewall** do are very important steps for any security administrator.

- There are several tools that automate the remote discovery of firewall rules and assist the administrator (or attacker) in analyzing the rules to determine exactly what they allow and what they reject.

- In order to defend a computer or network well, it is necessary to understand the ways it can be attacked.
- Thus, a tool(TTL,NMAP,Firewalk,Hping) that can help close up an open or poorly configured firewall will help the network defender minimize the risk from attack.

TYPES OF SCANNING AND ANALYSIS TOOLS.

3. OPERATING SYSTEM DETECTION TOOLS :

- Detecting a target computer's operating system is very valuable to an attacker, because once the OS is known, all of the vulnerabilities to which it is susceptible can easily be determined
- There are many tools that use networking protocols to determine a remote computer's OS.
- One specific tool worth mentioning is XProbe, which uses ICMP(Internet Control Message Protocol) to determine the remote OS.
- When run, XProbe sends many different ICMP queries to the target host.
- As reply packets are received, XProbe matches these responses from the target's TCP/IP stack with its own internal database of known responses.
- Xprobe is very reliable in finding matches and thus detecting the operating systems of remote computers.

TYPES OF SCANNING AND ANALYSIS TOOLS.

4. VULNERABILITY SCANNERS：

Active vulnerability scanners scan networks for highly detailed information.

- An active scanner is one that initiates traffic on the network in order to determine security holes.
- This type of scanner identifies exposed usernames and groups, shows open network shares, and exposes configuration problems and other vulnerabilities in servers.
- Vulnerability scanners should be proficient at finding known, documented holes.
- There is a class of vulnerability scanners called blackbox scanners, or fuzzers.
- Fuzz testing is a straightforward testing technique that looks for vulnerabilities in a program or protocol by feeding random input to the program or a network running the protocol.

TYPES OF SCANNING AND ANALYSIS TOOLS.

Passive vulnerability

scanner is one that listens in on the network and determines vulnerable versions of both server and client software.

- Passive scanners are advantageous in that they do not require vulnerability analysts to get approval prior to testing.
- These tools simply monitor the network connections to and from a server to obtain a list of vulnerable applications.
- Furthermore, **passive vulnerability scanners have the ability to find client-side vulnerabilities that are typically not found by active scanners**

SUMMARY OF THE LECTURE

Introduction to Security Technology

Firewalls; Protecting Remote Connections

Intrusion Detection Systems (IDS), Honey Pots, Honey Nets, and Padded cell systems

Scanning and Analysis Tools.

DISCUSSION


discussion
students
group
questions
class
people
conversation
time
person
participants
minutes
comment
Discussion
way
question
think
one
comments
know
tolerance
ideas
new
another
groups
critical
good
responses
different
detectives
newspaint
others
Students
someone
discussions
things
course
made
like
quote
feel
really
assumptions
point
want
asked
help
repressive
speak
thinking
something
important
next
first
get
give
work
two
view
possible
team
power
also
ask
room
around
practice
contributions
storyteller
learning
make
just
talk
might
specific
small
perspective
words
John
use
see
rule
idea
allowed
Marcuse
large
whole
right
alternative
perspectives
best
response
ground
week
circle
DISCUSSION
Learning
White
written
mean
voices
saying
speaking
student
move
wish
One
members
arguments
process
three
open
station
end
start
already
interpretations
least
much
sheet
voice
choose
Make
need
else
Gary
topic
leader
exercise
minute
well
read
issue
going
democratic
everyone
must
drawn
MINUTES
used
adult
back
talking
participation
write
life
New
practices
Critical
take