IT3789 Cyber Security Attack & Defence

L11 - Gaining Access (2)

WITH KNOWLEDGE COMES RESPONSIBILITY

Gaining Access

Exploitation	Privilege Escalation	Understanding Shellcode
Remote & Local Shellcode	Sniffing	Password Attacks

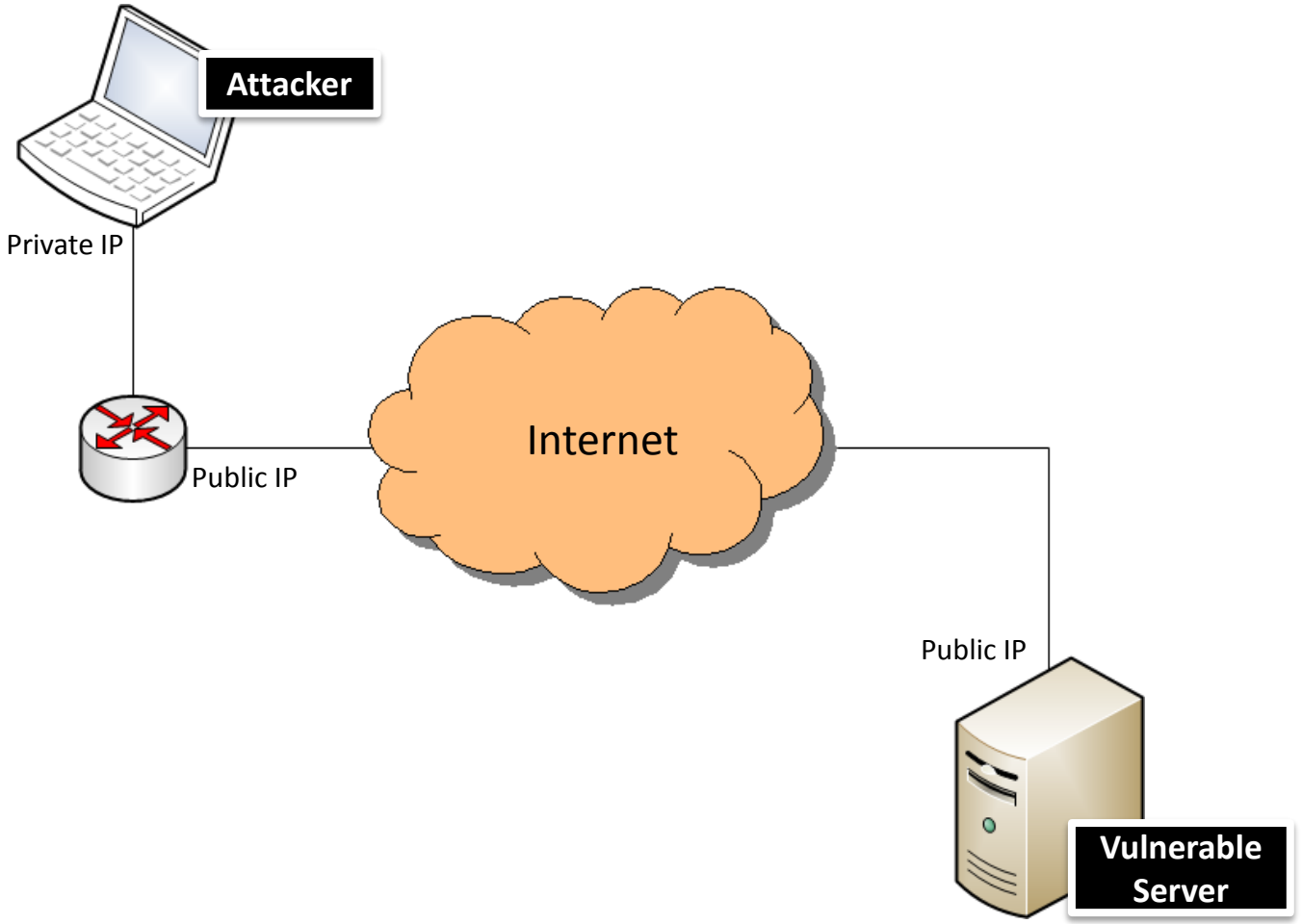
Remote Shellcode

- Remote shellcode allows attacker to gain access to a target machine remotely.
  - Examples:
    - Port-binding shellcode
    - Connect-back shellcode
    - Download and execute shellcode
- The target machine must have a vulnerability that enable the attacker to perform an arbitrary code execution.
- When a remote shellcode is executed, a remote shell may be spawned on the attacker machine enabling access remotely.

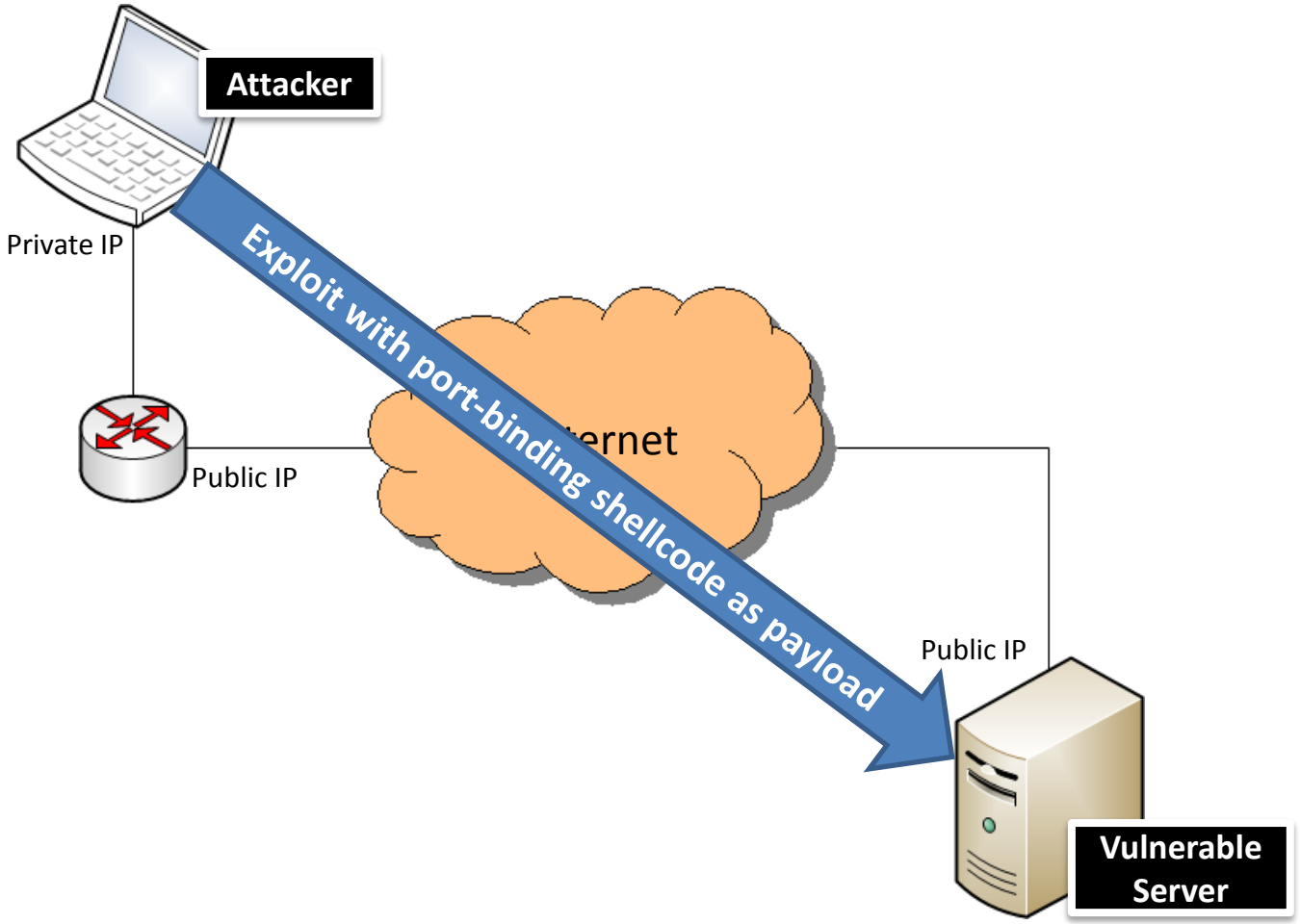
Port-binding Shellcode

- One of the commonest shellcode for remote vulnerabilities.
- Binds a shell to a port.
  - Allows attacker to create a **listening server** on **target machine**.
  - Spawn a shell on attacker's machine when attacker tries to connect to the port.
- A port-binding shellcode will not work if the target system has firewall up with deny policy in place.

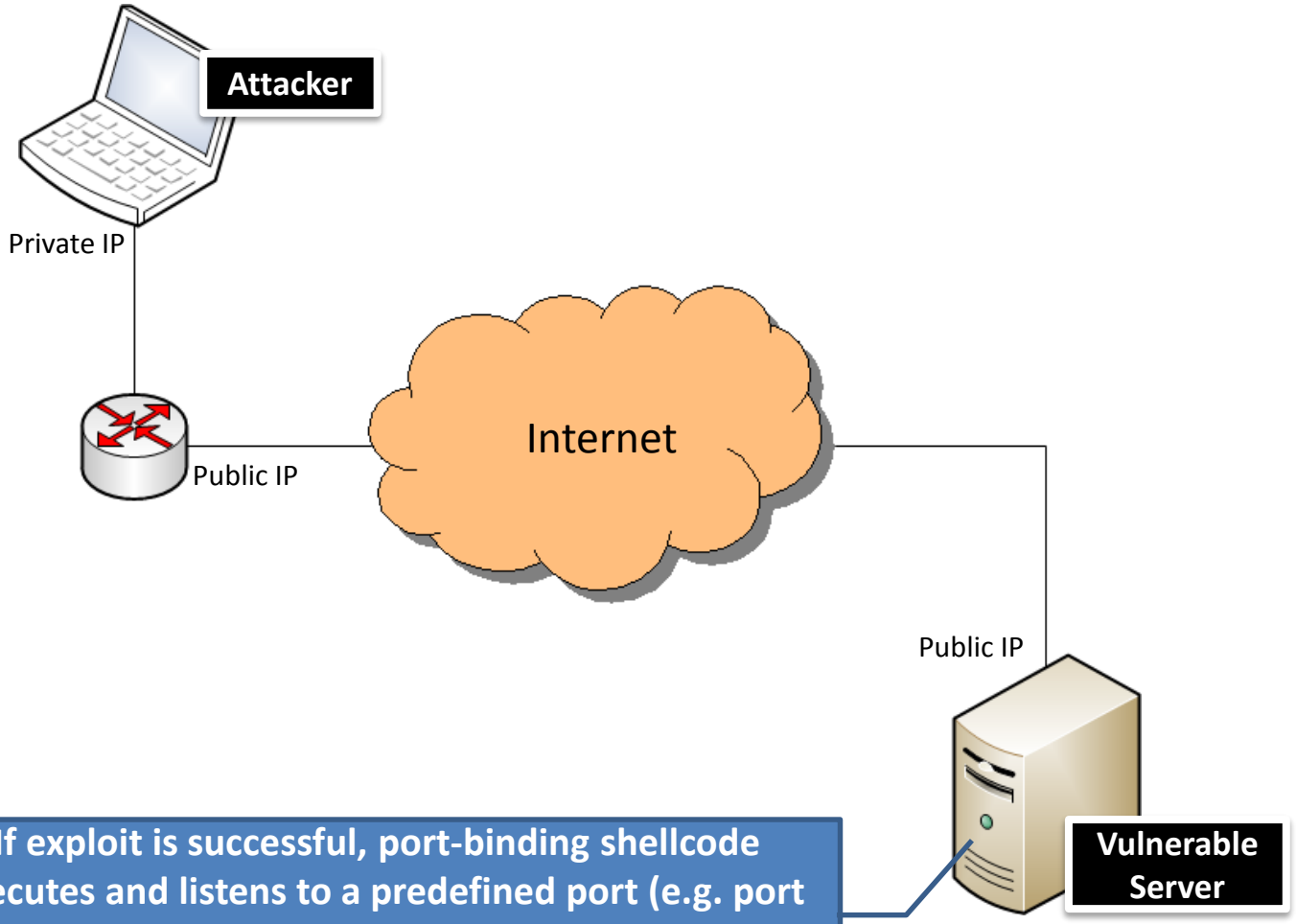
Port-binding Shellcode



Port-binding Shellcode

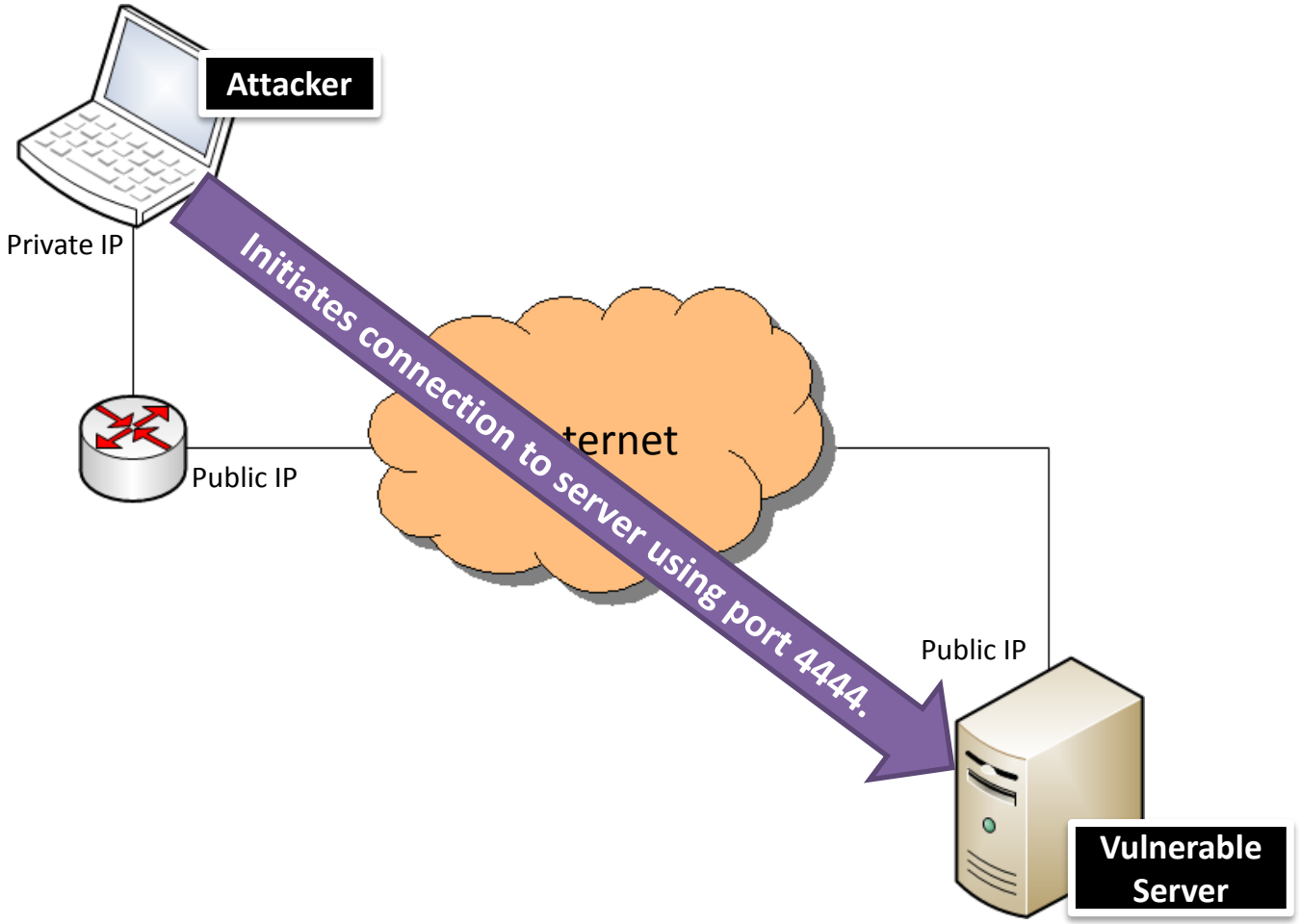


Port-binding Shellcode



If exploit is successful, port-binding shellcode executes and listens to a predefined port (e.g. port 4444).

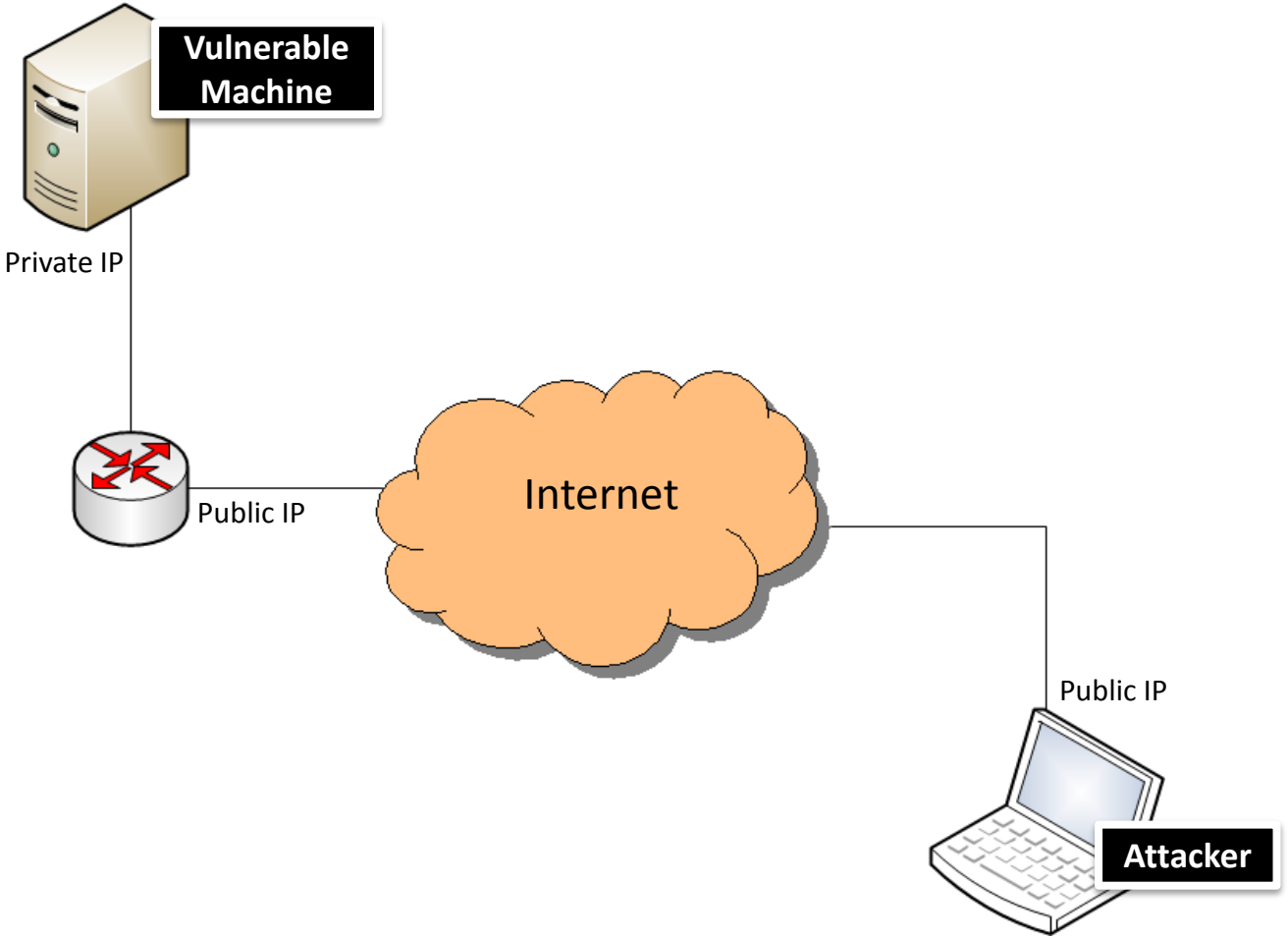
Port-binding Shellcode



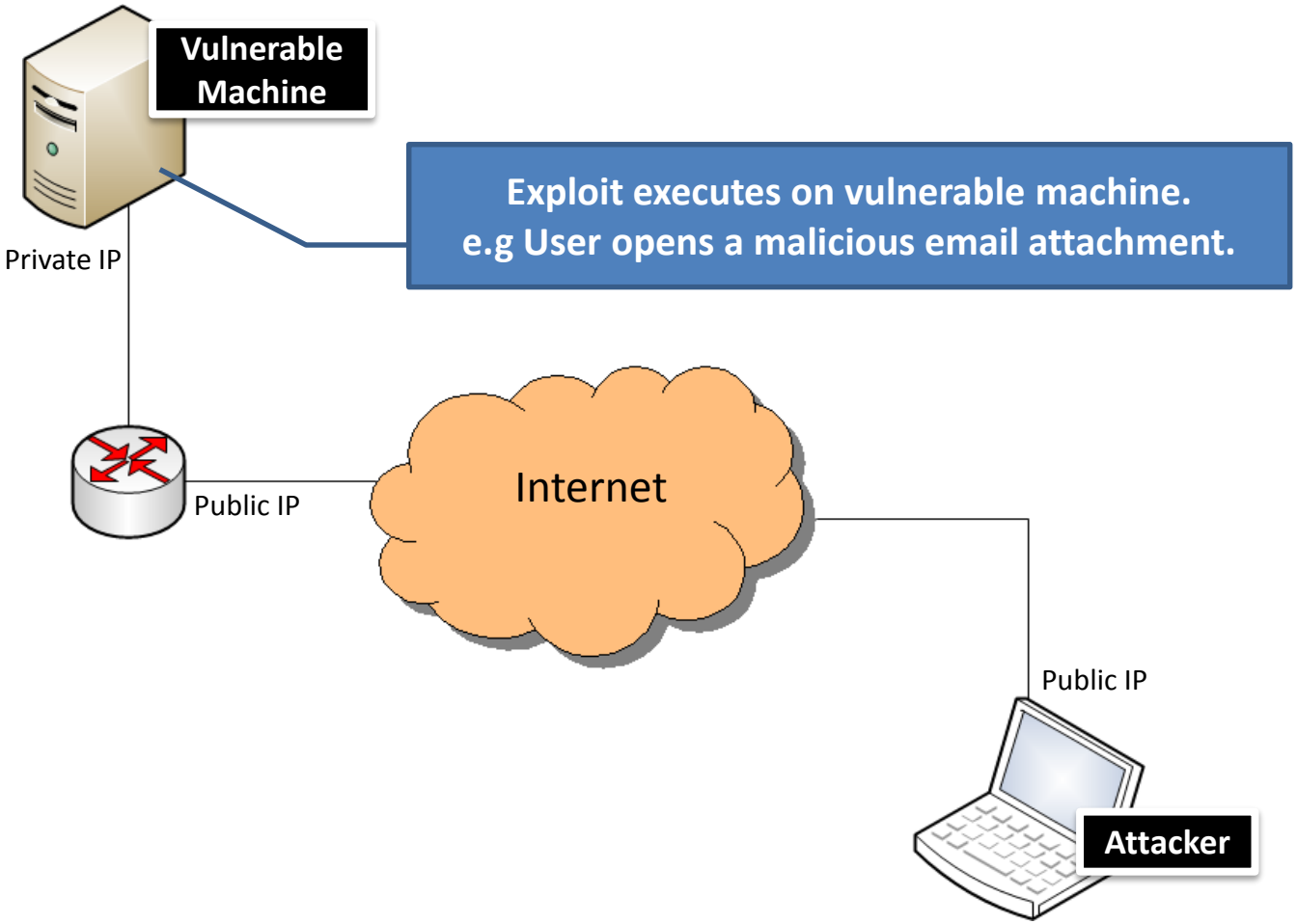
Connect-back Shellcode

- Connect-back shellcode makes connection from the compromised system to any machine indicated by the attacker.
- Once the compromised system connects to the intended machine, an interactive shell is spawned on this machine.
- Very useful when targeted system is behind a firewall.
  - Because outgoing traffic is usually not blocked by the firewall.

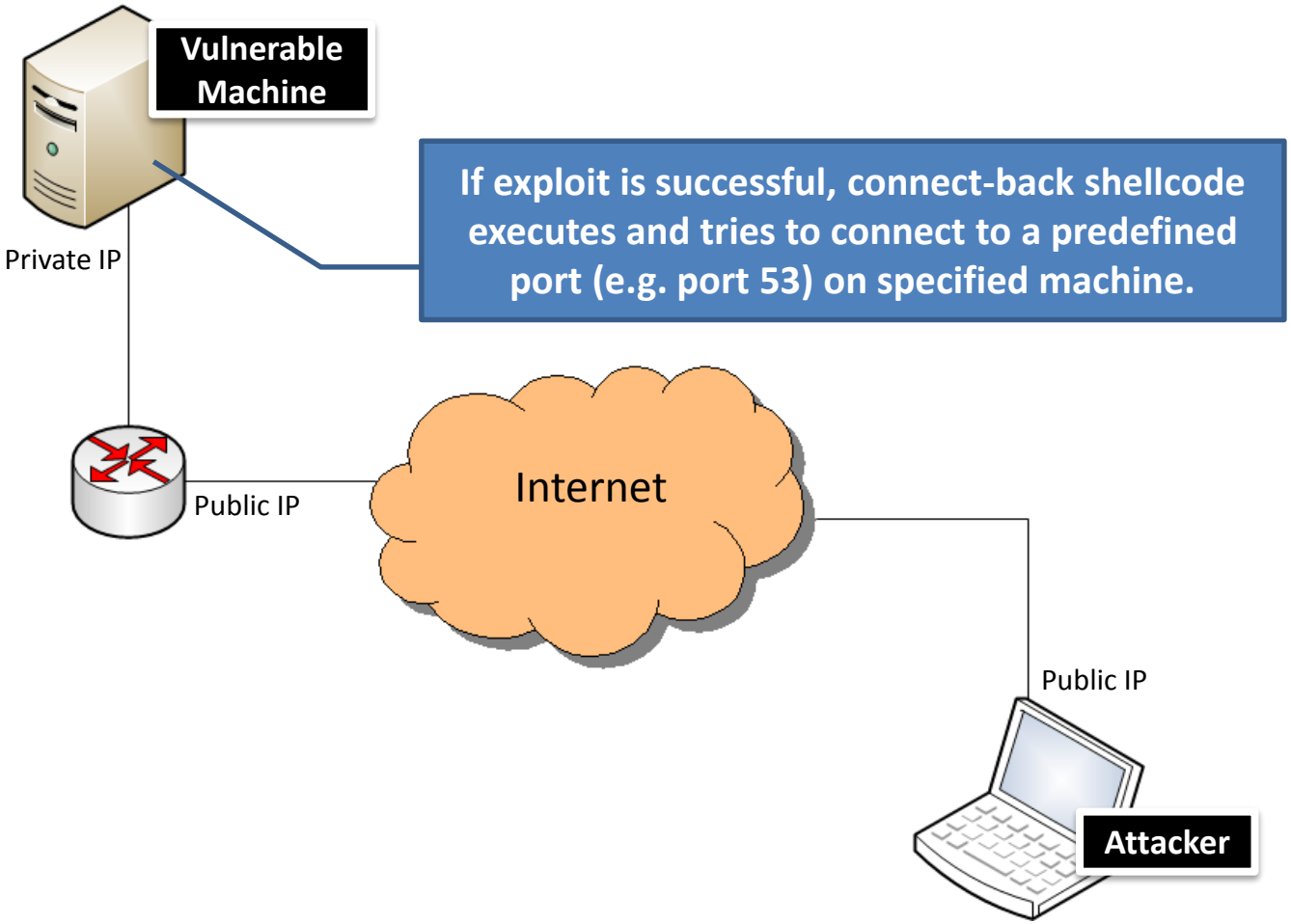
Connect-back Shellcode



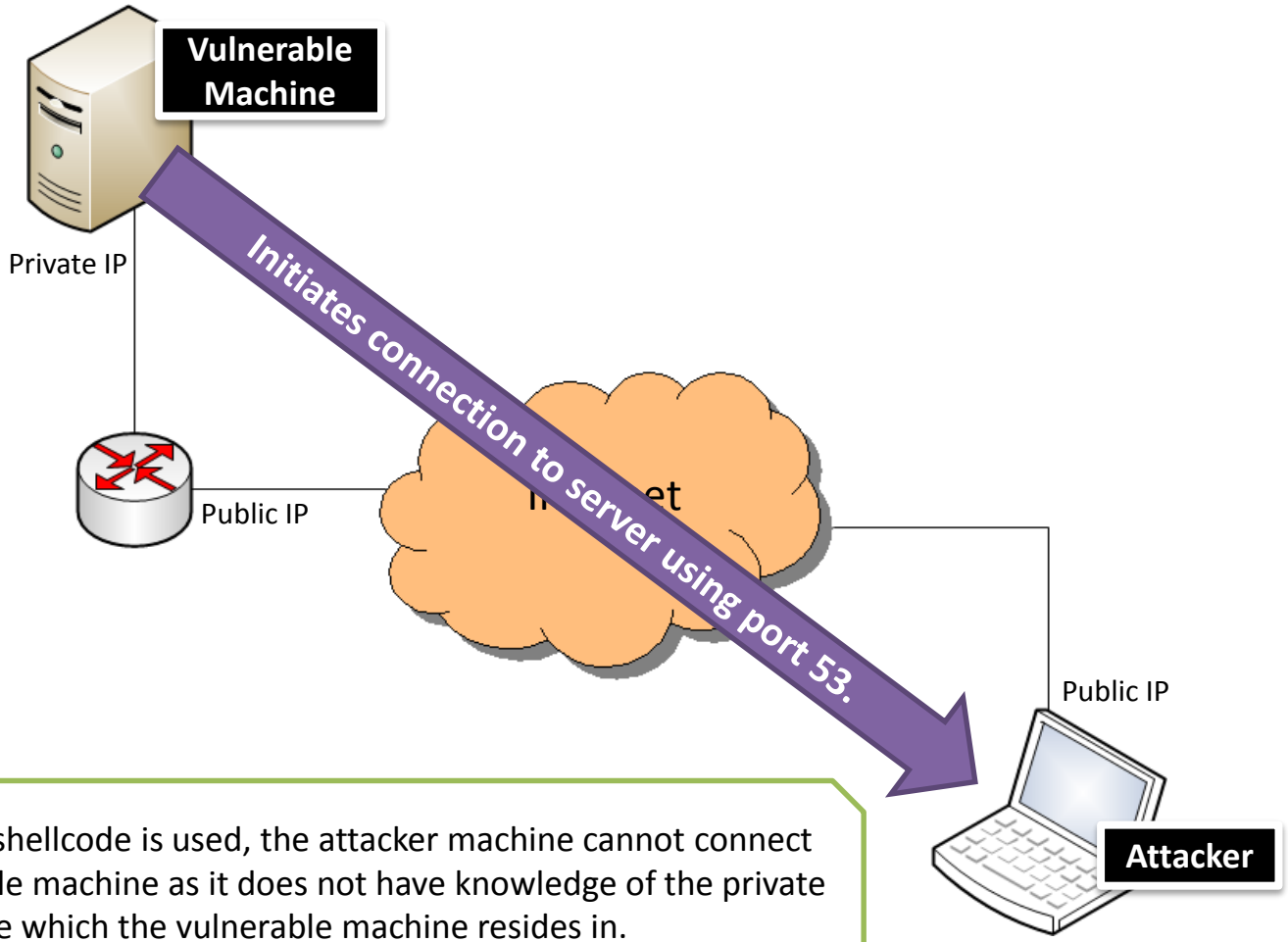
Connect-back Shellcode



Connect-back Shellcode



Connect-back Shellcode



If port-binding shellcode is used, the attacker machine cannot connect to the vulnerable machine as it does not have knowledge of the private IP address range which the vulnerable machine resides in.

Local Shellcode

- Shellcodes that are used for local vulnerabilities.
- Local shellcodes does not perform any network operation unlike remote shellcode.
  - Typically used for privilege escalation.
- execve shellcode is used to execute commands on a compromised system.
  - Most basic type of shellcode.
  - e.g. execute /bin/sh
- Execve is a system call provided by the kernel for command execution.
- Many exploits are a variant of this shellcode.

Gaining Access

Exploitation	Privilege Escalation	Understanding Shellcode
Remote & Local Shellcode	Sniffing	Password Attacks

Sniffing

- A sniffer is a tool that is used to capture traffic that are transmitting between systems.
- Most sniffers display both Layer 2 (Frame) and Layer 3 (packet) headers and data payload.
- A sniffer will be able to capture confidential information depending on how it is used and the measures in place.
  - e.g. Usernames and passwords may be obtained if Secure Socket Layer (SSL) is not used in client/server application.

How a Sniffer Works?

- Sniffers capture packets that are not intended for the system's Media Access Control (MAC) address.
  - Known as promiscuous mode.
- In promiscuous mode, the system Network Interface Controller (NIC) reads all traffic and direct them to the sniffer.
  - Network card must be in promiscuous mode.
- Protocols that do not encrypt data are subjected to sniffing.
- Attacker can gather valuable information such as usernames and passwords by capturing the traffic.

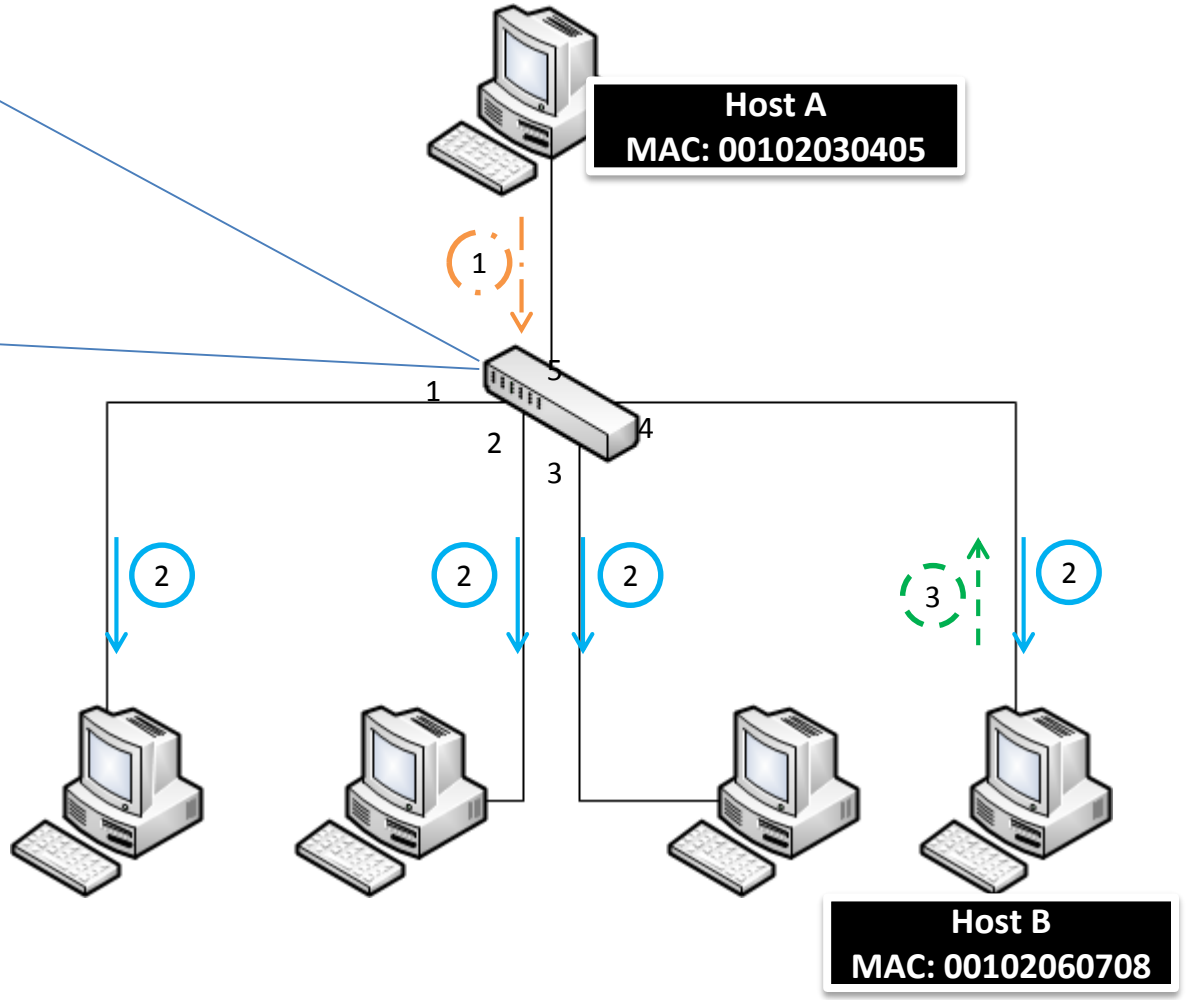
Address Resolution Protocol (ARP)

- ARP translates IP addresses into MAC addresses (hardware addresses).
- A MAC address a unique identifier assigned to network interfaces for communications on the physical network segment.
- How ARP works?
  - Host A tries to contact Host B using TCP/IP on a LAN, it needs the MAC address of Host B.
  - Host A first looks at its ARP cache to see if it has the MAC address of Host B.
  - If Host A does not have the MAC address, it will broadcast an ARP request to find out what is the MAC address associated with Host B's IP address.
  - The host with the IP address (Host B) will reply with its MAC address.
  - Host A will update its ARP cache with Host B's MAC address.

How ARP works in Switch?

Switch Routing Table

Port	MAC Address
5	00102030405
4	00102060708



1
- Host A send packet to Host B.
- Switch update Host A's MAC address in its routing table if the table does not contain Host's A MAC address.

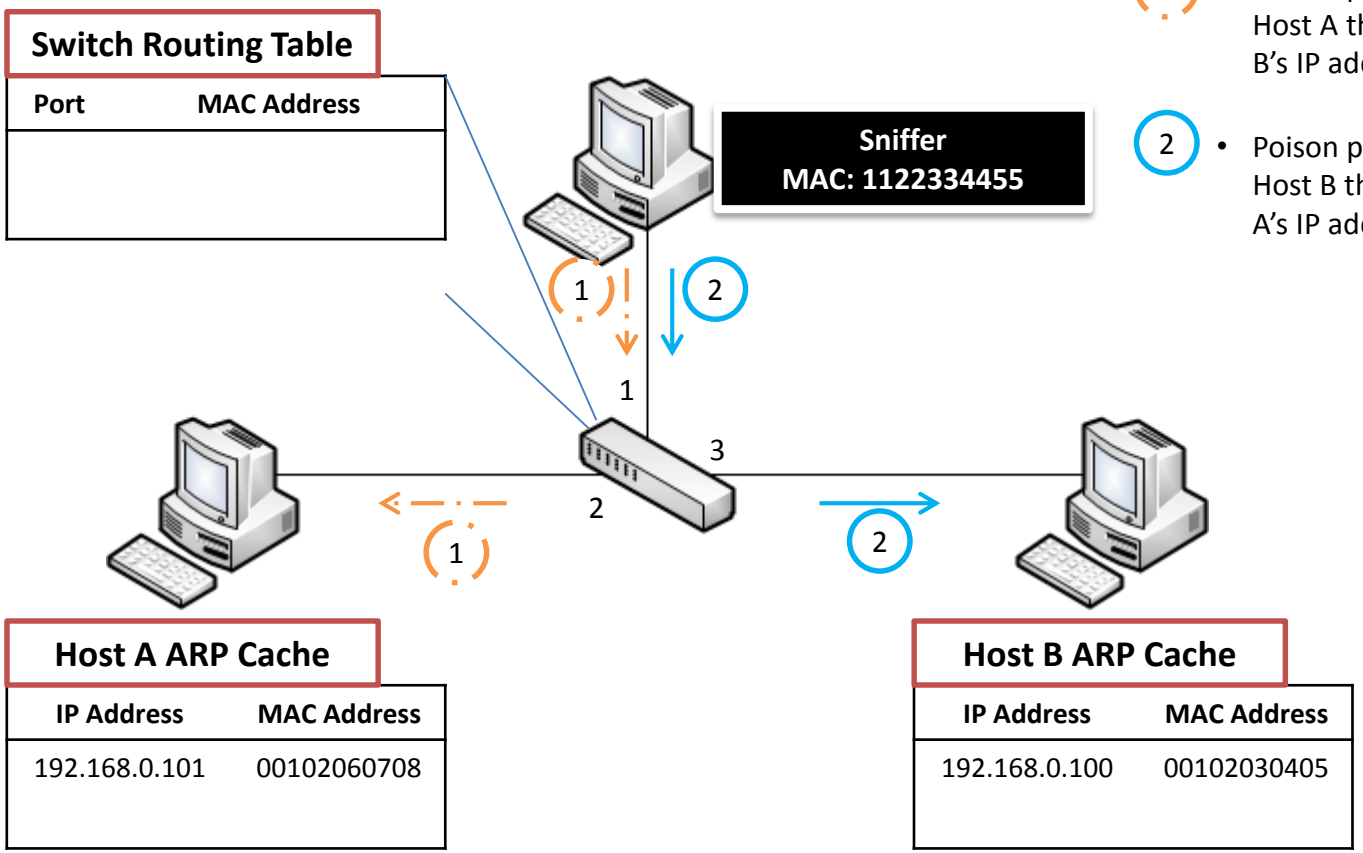
2
- If the switch does not have Host B's MAC address, a ARP request will be broadcasted.

3
- Host B will send a ARP reply and switch will update its routing table.
- Once mapping is learnt, only the relevant ports will be used.

ARP Poisoning

- By sending spoofed ARP reply to a target machine which will poison its ARP cache.
- Give an attacker the ability to redirect traffic from a target machine in a switched environment at will.
- ARP Poisoning will slow down network performance as the sniffer must process the packets.
- Points to Note
  - ARP Poisoning will only work within the same subnet.
  - The IP and MAC address of the target hosts are required for ARP Poisoning.
  - The mapping between target hosts must be present in their ARP cache in order to manipulate it.

ARP Poisoning



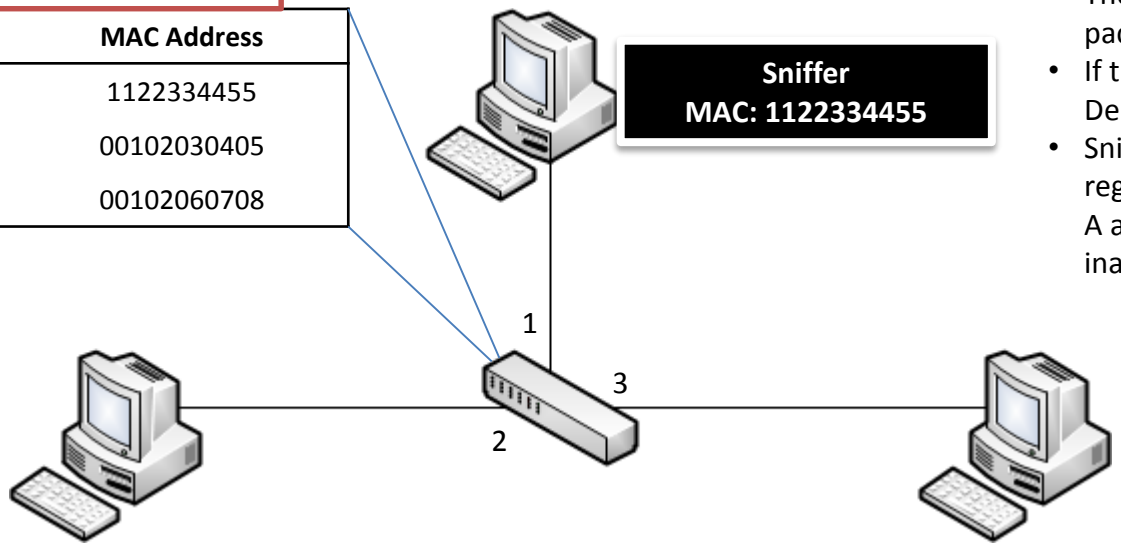
1 • Poison packet from Sniffer machine inform Host A that it can find 192.168.0.101 (Host B's IP address) at 1122334455.

2 • Poison packet from Sniffer machine inform Host B that it can find 192.168.0.100 (Host A's IP address) at 1122334455.

ARP Poisoning

Switch Routing Table

Port	MAC Address
1	1122334455
2	00102030405
3	00102060708



- Traffic between Host A and Host B will be redirected to the Sniffer machine.
- The Sniffer will decide whether to re-route the packets to the correct destination.
- If the Sniffer did not re-route the packets, a Denial of Service (DOS) occurs.
- Sniffer need to continue poisoning the hosts at regular intervals, or else the ARP cache of Host A and Host B will be cleared after a period of inactivity.

Host A ARP Cache

IP Address	MAC Address
192.168.0.101	1122334455

Host B ARP Cache

IP Address	MAC Address
192.168.0.100	1122334455

Gaining Access

Exploitation	Privilege Escalation	Understanding Shellcode
Remote & Local Shellcode	Sniffing	Password Attacks

Passwords

- Passwords can be formed by any of the following character sets.
  - Alphabets only
  - Numbers only
  - Special characters only
  - Alphanumeric
  - Alphabets and special characters
  - Numbers and special characters
  - Alphanumeric and special characters

Popular Passwords

123456

Despite Internet security breaches, this is world's most popular password

NEW YORK

BACK at the dawn of the Web, the most popular account password was "12345". Today, it's one digit longer but hardly safer: 123456.

Despite all the reports of Internet security breaches over the years, including the recent attacks on Google's e-mail service, many people have reacted to electronic break-ins with a shrug.

According to a new analysis, one out of five Web users is still leaving the digital equivalent of a key under the doormat. They choose simple, easily-guessed passwords like "abc123", "iloveyou" or even "password" to protect their data.

"I guess it's just a genetic flaw in humans," said Mr Amichai Shulman, the chief technology officer at Imperva, which makes software for blocking hackers. "We've been following the same patterns since the 1990s."

Mr Shulman and his company examined a list of 32 million passwords that an unknown hacker stole last month from RockYou, a Californian company that makes software for users of social-networking sites like Facebook and MySpace.

The list was briefly posted on the Web, and hackers and security researchers downloaded it.

RockYou, which had already been widely criticised for lax privacy practices, has advised its customers to change their passwords, as the hacker gained information about customers' e-mail accounts as well.

The trove provided an unusually detailed window into computer users' password habits. Typically, only government agencies, like the Federal Bureau of Investigation or the National Security Agency, have had access to such a large password list.

Said Mr Matt Weir, a doctoral candidate in the e-crimes and investigation technology lab at Florida State University, where researchers are also examining the data: "This was the mother lode."

Imperva found that nearly 1 per cent of the 32 million people it studied had used "123456" as a password.

The second-most-popular password was "12345". Others in the top 20 included "qwerty", "abc123" and "princess".

More disturbing, said Mr Shulman, was that about 20 per cent of people on the RockYou list picked from the same, relatively small pool of 5,000 passwords.

This suggests that hackers could easily break into many accounts just by trying the most common passwords. Due to the prevalence of fast computers and speedy networks, hackers can fire off thousands of password guesses per minute.

Said Mr Shulman: "We tend to think of password guessing as a very time-consuming attack, in which hackers take each account and try a large number of

CONTINUED ON TECHNOLOGY A14

'ILOVEYOU' IS HOT TOO

One million RockYou users chose these passwords:

1. 123456	11. nicole	21. iloveu
2. 12345	12. daniel	22. michelle
3. 123456789	13. babygirl	23. 111111
4. password	14. monkey	24. 0
5. iloveyou	15. jessica	25. tigger
6. princess	16. lovely	26. password1
7. rockyou	17. michael	27. sunshine
8. 1234567	18. ashley	28. chocolate
9. 12345678	19. 654321	29. anthony
10. abc123	20. qwerty	30. angel
		31. FRIENDS
		32. soccer

SOURCE: IMPERVA PHOTO: ISTOCKPHOTO

"Nearly 1 percent of the 32 million people studied had used '123456' as a password."

*"**Hackers could easily break into many accounts** just by trying the most common passwords.*

*Because of the prevalence of fast computers and speedy networks, hackers can **fire off thousands of password guesses per minute**."*

Published: NYTimes, 20 Jan 2010

Weak Passwords

- Weak passwords are one of the security concern especially for internal networks.
- Common problems related to passwords.
  - Blank password
  - Password identical to username
  - Password reuse on different accounts
  - Writing passwords on post-it notes
  - Password management tools
  - Password saved in browsers

Passwords in Operating Systems

- Where are passwords stored?
  - Windows: Security Accounts Manager (SAM)
    - Use tools like fgdump.exe to perform a hash dump of the SAM file that is held in the registry.
    - A backup copy of the SAM can usually be found in %SYSTEMROOT%\repair
  - Linux: /etc/shadow file
    - A copy of the shadow file can be copied with root privileges.

Password Attacks

Passive Online Attacks

- Eavesdropping on network for password exchange.
- Data may be hashed or encrypted.
- e.g. Sniffing, man-in-the-middle, replay attacks.

Active Online Attacks

- Any network service that requires a user to log on is vulnerable to password guessing.
- Involves the automation of password guessing process which improves speed and success rate.
- Using word list that has been collected or generated.
- e.g. Hydra and Medusa which are login brute forcing tool.

Offline Attacks

- Perform from another location other than the actual target machine where the passwords reside.
- Dictionary, hybrid and brute force attacks.
- Examples
  - Rainbow Crack: Use pre-computed hashes (Rainbow table) of common strings to speed up the password discovery and cracking.
  - John-the-Ripper: Fast password cracker which main purpose is to detect weak passwords.

Non-electronic Attacks

- Attacks that do not employ any technical knowledge.
- Shoulder surfing, keyboard sniffing and social engineering.

Offline Attacks

Dictionary Attacks

- Using list of words from dictionary to identify a password.

Hybrid Attacks

- Starts with words in a dictionary and then substituting characters with numbers or symbols.
- e.g. @dm1n1str@t0r

Brute Force Attacks

- Trying all combinations of alphabets (uppercase/lowercase), numbers and symbols.
- Slowest of the 3 types of offline attacks.

Gaining Access (2)

Remote Shellcode

- Remote Shellcode
- Local Shellcode

Sniffing

- How a Sniffer Works?
- ARP Poisoning

Password Attacks

- Passive Online Attacks
- Active Online Attacks
- Offline Attacks
- Non-electronic Attacks