Stockholm University

Network Attacking Techniques

Network Security (NETSEC)

Yuhong Li

Outline

- Attacking means and procedure

- Information collection
- Network hiding
- Port and vulnerability scanning
- Actualizing attacks
- Backdoor setting and log cleaning

Network Attacking Means and Procedure

Network attacking

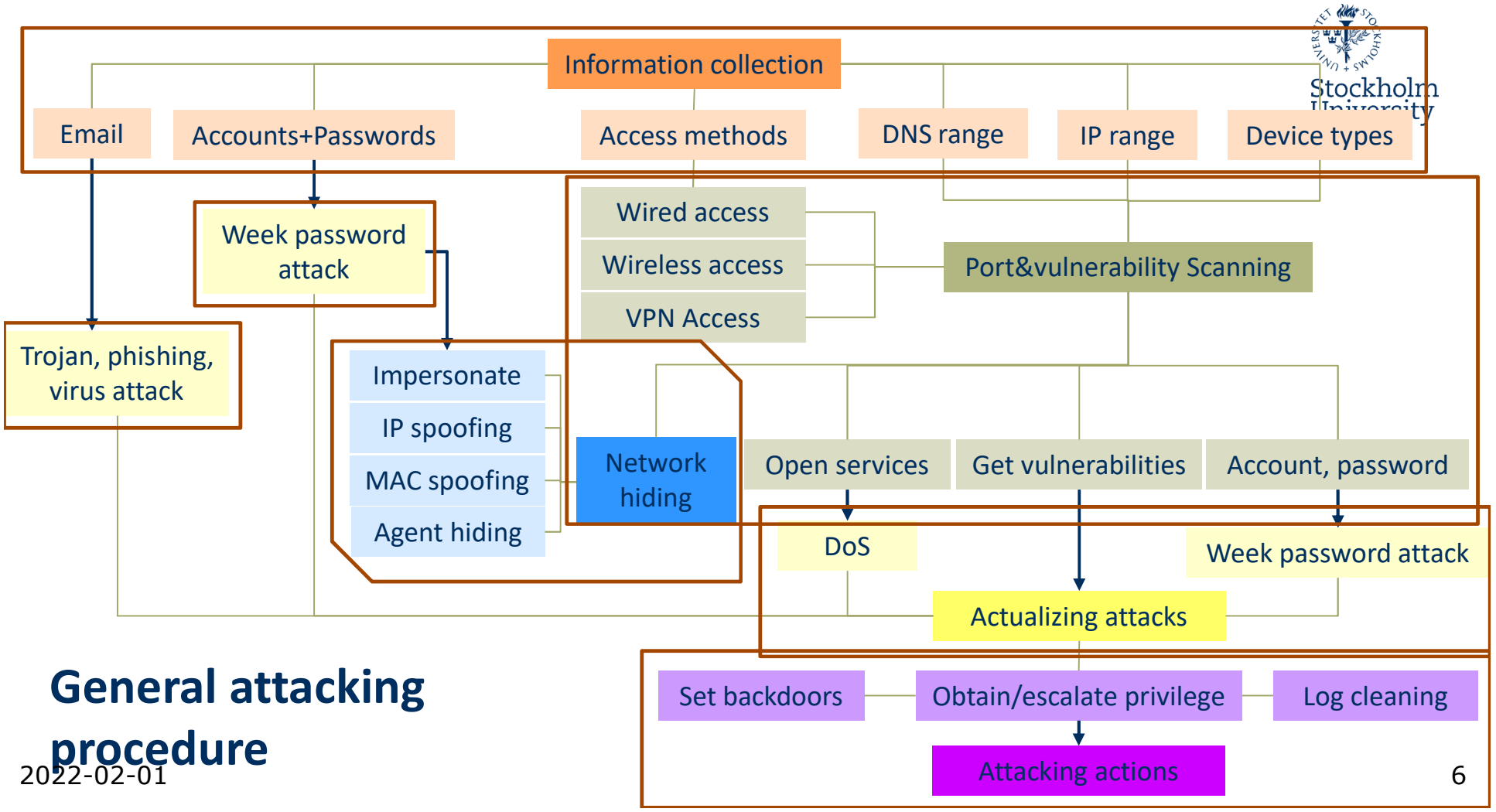
Stockholm University

- Network attacking
  - Actions that harm the networks
  - Disclose information, destroy integrity, deny services, non-authorized access …
- Basic features
  - Using certain tools
  - Having certain affects

Network attacking means

- Network scanning (reading, incl. interception)
- Operation (modification, fabrication)
- Masquerade/Spoofing: IP spoofing, ARP spoofing, DNS spoofing, phishing
- Flooding (exhausting the resources, interruption)
- Redirection (ARP redirect)
- Rootkits techniques

General attacking procedure



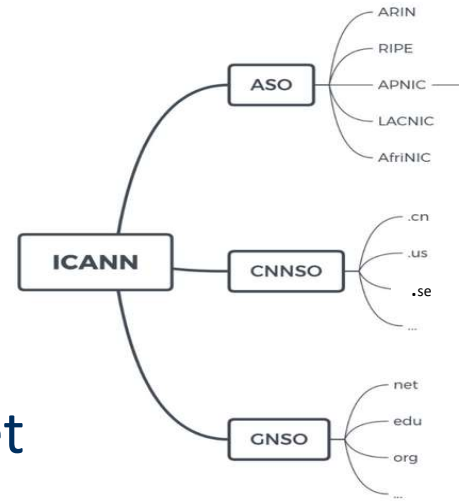
Information Collection

Information collection

Stockholm University

- Preparation for attacks: collecting various information of target hosts or networks
  - Network access methods: dial-in, wireless LAN, Ethernet, VPN etc.
  - Target network information： domain name, IP range, physical location etc.
  - Network topology： router/switch types, manufactures, transmission networks etc.
  - User information： email, user account, passwords etc.
  - Personal information: occupation, contact, …
- Approaches
  - Searching engine: google, bing, …
  - Tools: whois, netdiscover, dnsmap, dnswalk, dig, ….
  - Social engineering: social information

Example: whois enquiry



- Detail information about IP, DNS
- ICANN's ASO(Address Supporting Organization)
- Regional Internet Registry-RIR, National Internet Registry-NIR
  - IP addresses (address ranges) are kept in databases of NIR or RIR
  - Each RIR knows who manages the IP address ranges
- Select any whois server
  - http://www.whois365.com/

Other tools

Stockholm University

- Send query request to the target server
  - host, dig, nslookup dig domain +trace
- Network scanning
  - netdiscover
  - nmap
  - dnsmap
  - dnsdict6
- Brute force enumerate
  - dnsenum: recursive enumerate all the subdomains and hosts in the subdomain

    dnsenum [-r] [-f /usr/share/dnsenum/dns.txt] domain name
  - Dnsrecon: domain name collection tool
  - Fierce:scan target IP and hosts names, including find the domain names by inverse look up

netdiscover by using ARP

Stockholm University

```
root@kali:~# netdiscover --help
netdiscover: invalid option -- '-'

Netdiscover 0.3-pre-beta7 [Active/passive arp reconnais
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p
  -i device: your network device
  -r range: scan a given range instead of auto scan. 19
  -l file: scan the list of ranges contained into the g
  -p passive mode: do not send anything, only sniff
  -m file: scan the list of known MACs and host names
  -F filter: Customize pcap filter expression (default:
  -s time: time to sleep between each arp request (mil
  -n node: last ip octet used for scanning (from 2 to 2
  -c count: number of times to send each arp reques (fo
  -f enable fastmode scan, saves a lot of time, recomme
  -d ignore home config files for autoscan and fast mod
  -S enable sleep time supression between each request
  -P print results in a format suitable for parsing by
  -N Do not print header. Only valid when -P is enabled.
  -L in parsable output mode (-P), continue listening after

If -r, -l or -p are not enabled, netdiscover will scan for
```

```
Currently scanning: (passive)   |   Screen View: ARP Request

37915 Captured ARP Request packets, from 14387 hosts.   Total size: 2275188

  IP            At MAC Address     Requests IP      Count
-------------------------------------------------------------------------
192.168.1.232   9c:14:63:53:84:d9   192.168.1.1        181
192.168.2.156   fc:4d:d4:f8:84:f8   192.168.2.110      303
192.168.1.64    ac:cb:51:03:30:c0   192.168.1.1        187
192.168.2.156   fc:4d:d4:f8:84:f8   192.168.2.111      261
192.168.2.156   fc:4d:d4:f8:84:f8   169.254.169.254     10
192.168.101.4   d8:38:0d:cb:3d:dc   192.168.101.107     72
192.168.1.131   44:47:cc:99:bd:cc   192.168.1.1        187
10.72.38.4      00:50:ba:51:5f:57   10.11.248.51         2
10.72.38.5      00:50:ba:51:5f:58   10.11.248.52         3
10.72.38.6      00:50:ba:51:5f:59   10.11.248.53         3
10.72.38.7      00:50:ba:51:5f:5a   10.11.248.54         3
10.7
10.7
10.7
10.7
10.7
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
192.168.100.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.100.2   00:50:56:fa:d6:4e      1      60  VMware, Inc.
192.168.100.254 00:50:56:fc:4f:d5      1      60  VMware, Inc.

root@kali:~#
```

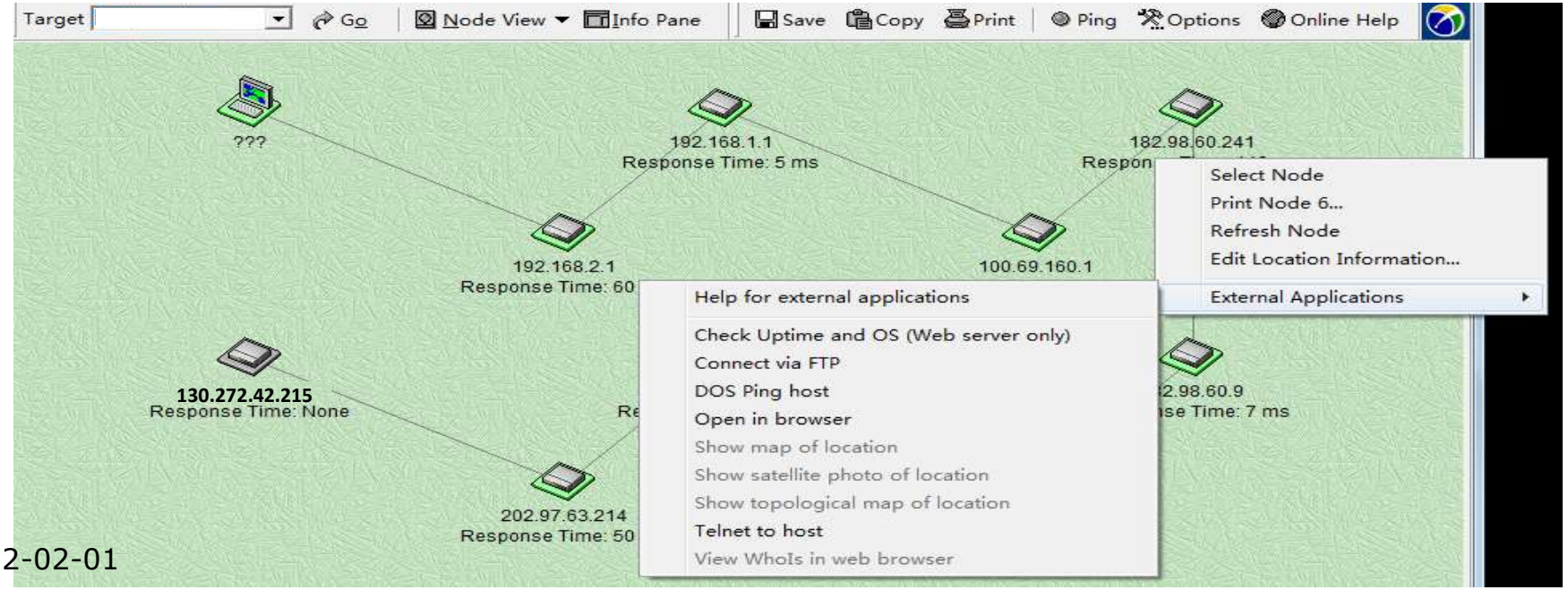
Social engineering

Stockholm University

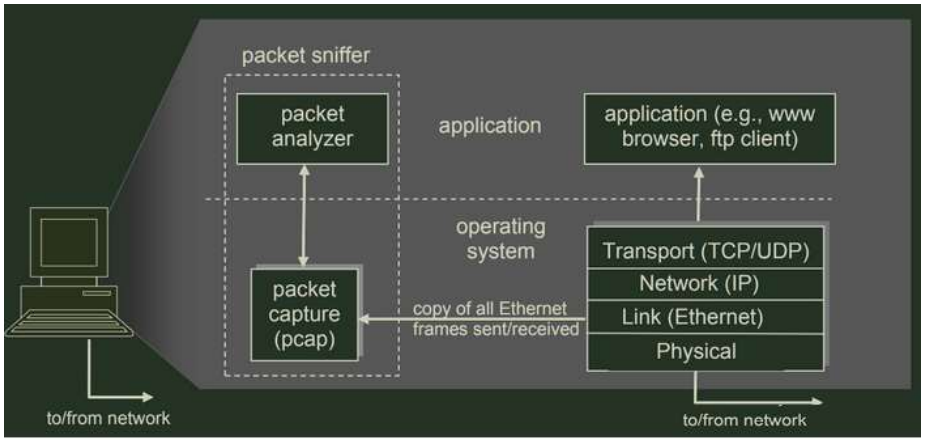
- Collecting information from people
- Information source
  - Professionist: information about an area
  - Staffs related to the target networks: analysis from other “unuseful” information
  - garbage collection: obsolete devices, media, files …
- Maltego
  - Highly automated information collecting tool
  - DNS severs, IP addresses, sub-domains, personal information
  - Cross platform
  - Graphical user interface (GUI)

Network topology determination

- Neotrace: graphical network path tracing tools, integrated IP address location, Whois and map



Eavesdropping/Snooping



- Intercept SMTP, HTTP, FTP, POP3, TELNET messages (not encrypted)
- Network listener/sniffer
  - Listen to drivers: intercept data streams, filter them and cache
  - Capture drivers: control the network card to receive data, and put in cache
  - Cache: store the captured data
  - decryption: decrypt the obtained data
  - Data analyzer: pattern matching and analysis to the obtained data
- Tools: Wireshark、IRIS、Tcpdump/Windump、Sniffer Pro
- More tools: Cain&Abel, p0f, driftnet, ferret
- Protection from eavesdropping and snooping
  - Check if a network card in network working in the promiscuous mode
  - Use encrypted protocols
  - Secure network topology

Summary

- Whois enquiry: IP Whois, DNS Whois, Whois reverse query, IP2Location, IP2Domain
- Collection based on DNS servers: host, dig, dnsenum, dnsrecon, fierce
- Searching IP addresses in internal networks: ICMP searching, ARP searching, UDP/TCP query
- Mining based on WEB
- Social engineering
- Determine the target network topology: traceroute, Zenmap, Neotrace
- Network sniffing: Cain&Abel, p0f, driftnet and ferret

Stockholm University

Network Hiding

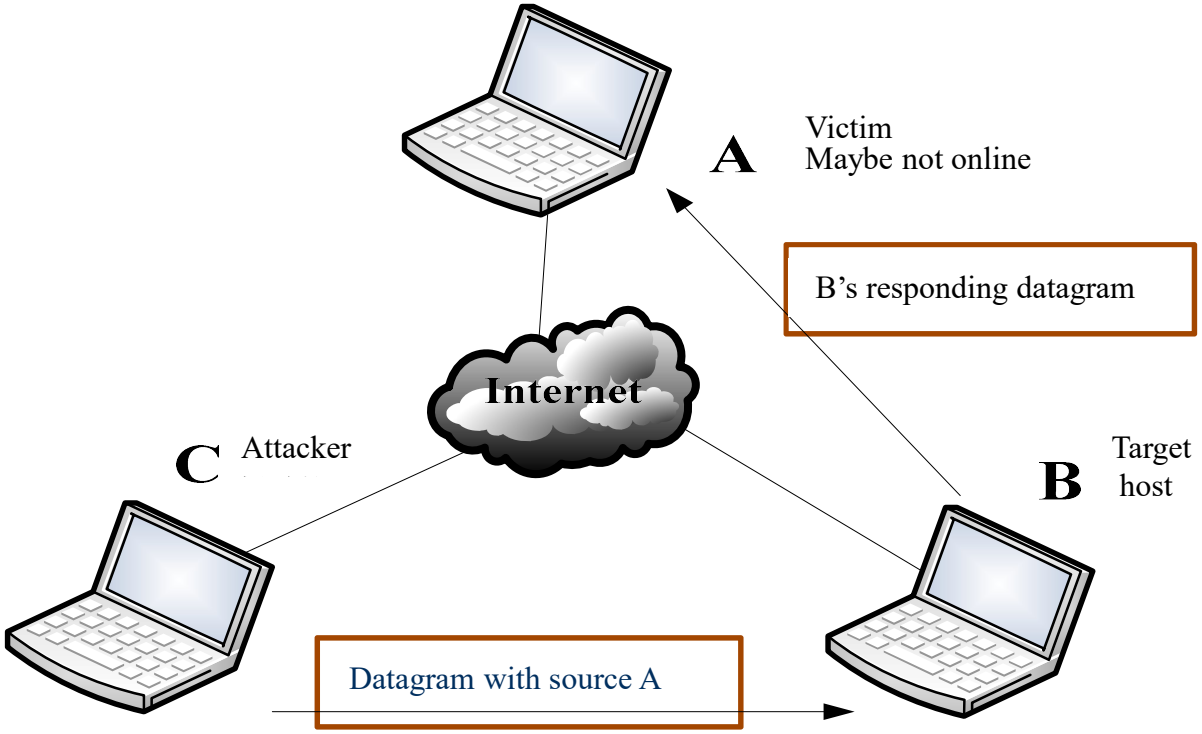
Network hiding

- Hide own IP address -> cannot be traced after attacking

- IP spoofing
  - TCP/IP does not check source IP address; bypass the blacklist in ACL
- MAC spoofing
  - Change the MAC address to permissible ones
- Using agents
  - Visiting or collecting data through (multiple) agents,
- Impersonate a user
  - Eavesdropping or break account or password of users
- zombies
  - Control zombies to attack other machines

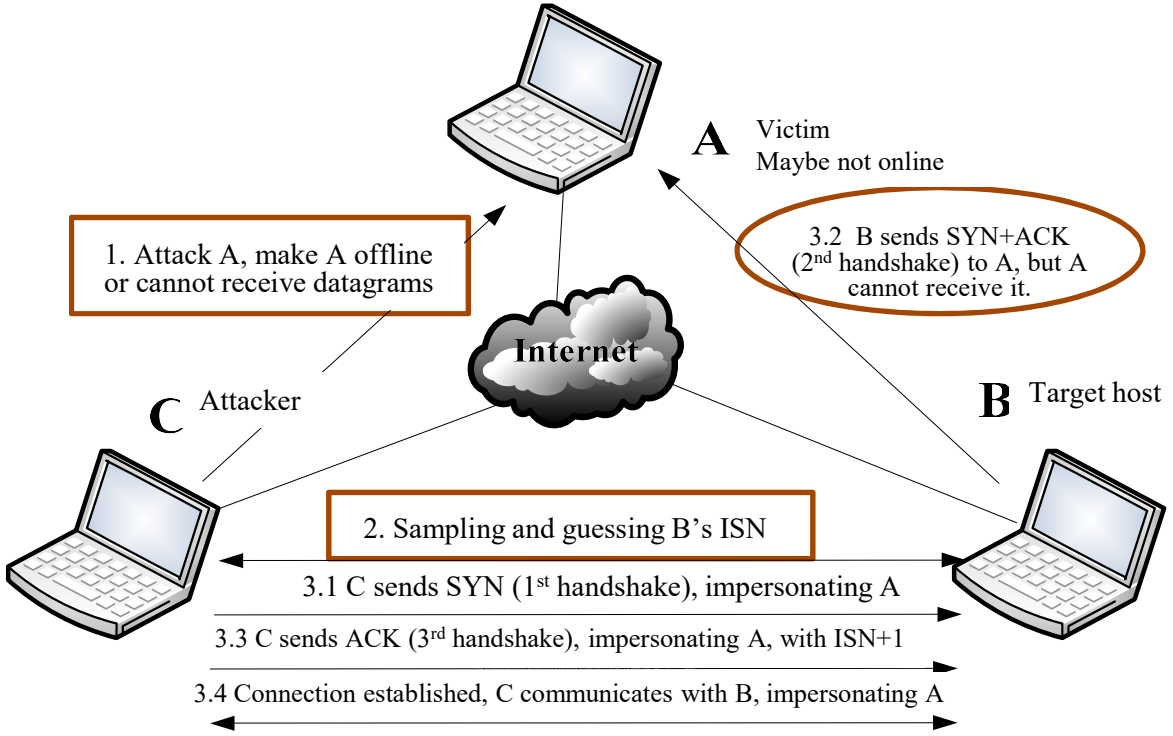
IP spoofing -1

- TCP/IP only check the validity of destination IP: change IP and bypass the host's or network's access control
- Relative easy when C and A are in the same LAN
- When C and A are not in the same LAN， UDP spoofing is relatively easy



IP spoofing -2

- If A and B use TCP, a little complex for the attacker C
- Procedure
  - Stop A's receiving data
  - Guess the ISN (initiating sequence number)
    - Time-dependent
    - Random
    - Fixed
  - Established a deceiving connection to B



Countermeasures

Stockholm University

- Prerequisite: identify a host by its IP address + successfully guess the ISN
- Countermeasures
  - Use encryption-based protocols, e.g., IPSec, SSH
  - Use password or certificate for authentication
  - Use random ISN
  - Use packet filtering on routers: make sure source IP addresses is accordant to the network topology
  - Don’t use trust policies based on IP addresses

MAC spoofing

Stockholm University

- Access control based on MAC
- Access control based on IP and MAC
- Soft modification
  - Card driver reads MAC address from the system and writes it to the hardware's memory
- Hard modification
  - Change the original MAC address stored in ROM

Network address translation (NAT)

Stockholm University

- Private address <-> public address, transparent to end users

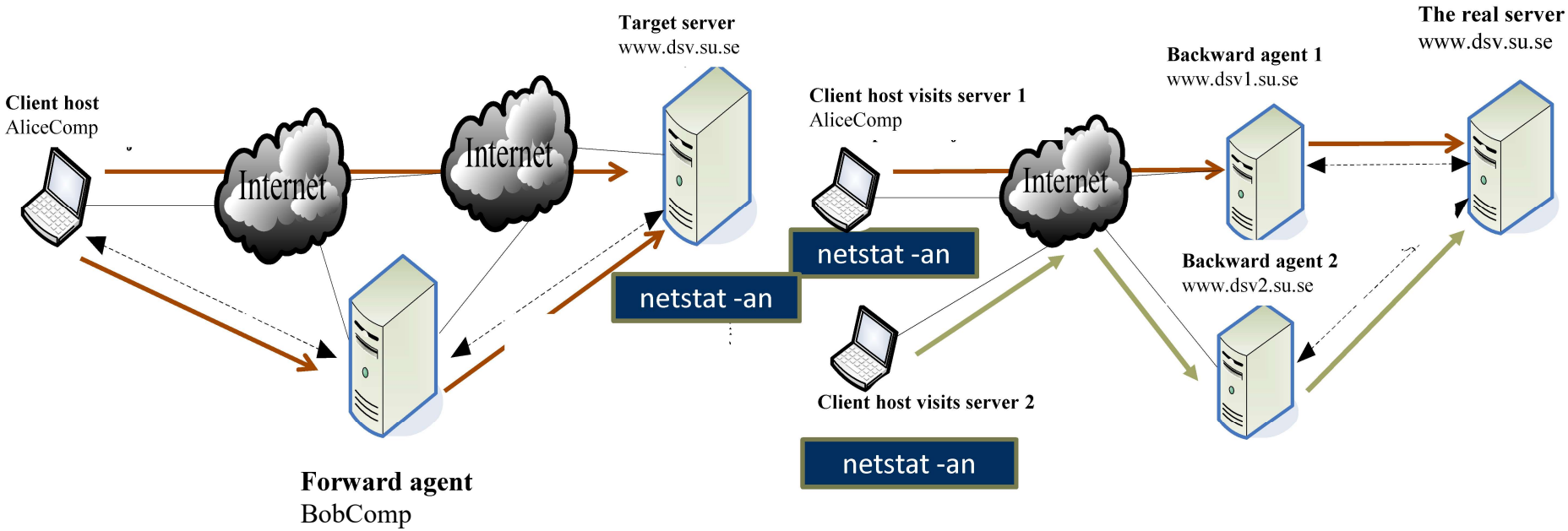
  netstat –an
- Static: one to one, fixed
  - Mapping between internal and external networks
- Dynamic: select from an address pool randomly
  - Can be used e.g., for OSPF
- Port address translation (PAT): mapping both IP address and port number
  - Sharing the same IP address, for TCP and UDP communications
  - Address translating table: setup an entry recording the mapping when a communication begins, delate the entry when ends
  - Each entry: bind a session

Hiding through agents

Stockholm University

- Agent: “act” on behalf of hosts -> communicate with target hosts indirectly through an agent
  - Separate the direct communication into two segments/processes
  - isolate internal network and external network
  - What will happen if the agent is vulnerable?
- Forward agent
  - Send request to the agent, the agent answers and forwards the request to the destination host
  - Must know the IP address of the agent and the port
- Backward agent
  - Can be seen as the front-end of a server, can be used to protect the sever.
  - The client does not know the exist of the agent

Working procedure



Frequently used proxies

Stockholm University

- HTTP agent, normally port 80, 8080
- SSL agent, standard port 443
- HTTP CONNECT agent
- HTTP TUNNEL agent
- FTP agent, normally port 21, 2121
- POP3 agent, normally port 110
- Telnet agent, normally port 23
- Socks agent, standard port 1080

- Tools
  - Burpsuite, ZAP, Sockcaps64, Proxychains, Squid, Subgraph Vega …

Summary

- TCP-based IP Spoofing: need to guess TCP ISN, relatively difficult
- MAC Spoofing: used in LAN, break the ACL-based access control
- NAT: trace each message based on address translation (static and dynamic)
- Agent: attackers can attack the target machine indirectly
- Multiple agents + zombies: very difficult to trace

Port and Vulnerability Scanning

Network scanning -1

- Technique based on remote service discovery and system vulnerabilities scanning.
  - The open services on the target host (i.e., the ports)
  - The developer of the services and versions
  - OS type and version
  - Vulnerabilities of the services that can be utilized
  - Vulnerabilities of the OS
  - Sensitive information like accounts and passwords
- General steps of network scanning
  - Scan service connections as many as possible -> open services
  - Scan the services -> type and version
  - Scan vulnerability -> attack

Network scanning -2

Stockholm University

- Host-based scanning
  - Run on the scanned host
  - Detect the wrong configurations, weak passwords, configurations violating security policies…
  - Need access right to the scanned host: system security scanning based on passive policy
- Network-based scanning
  - Send probing packets to the remote hosts, collect the responses, decoding and analyzing the data
  - System security scanning based on active policy
- According to the purpose of network scanning
  - Port scanning, type and version scanning, vulnerability scanning, weak password scanning, Web vulnerability scanning, configuration scanning.

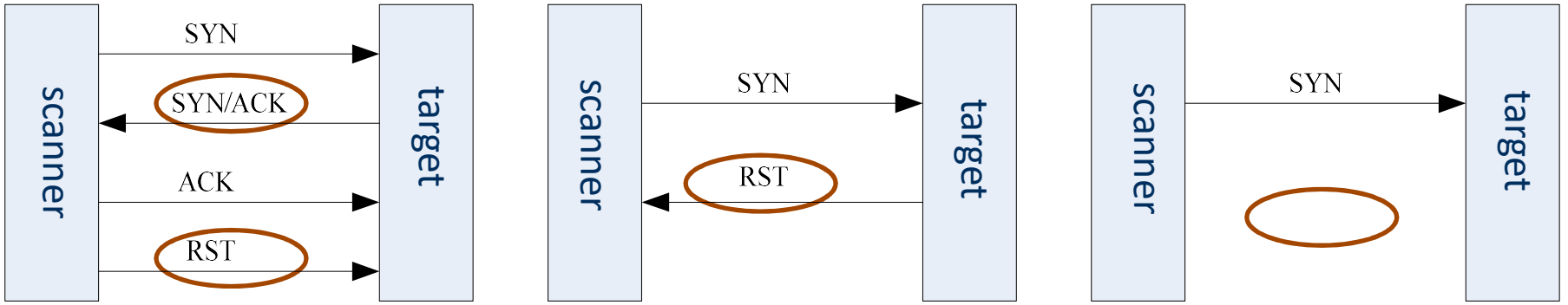
Port scanning

Stockholm University

- To find the open ports and services on the target devices -> preparing for the attacks
- Slow-scanning: irregular and long interval scanning on discrete ports
- Out-of-order scanning: short interval scanning on continuous ports
- TCP-port scanning: connection scanning, SYN scanning, FIN scanning, ACK scanning, NULL scanning, XMAS scanning, TCP window scanning, self-defined scanning
  - System log can only record the connection scanning
- UDP-port scanning

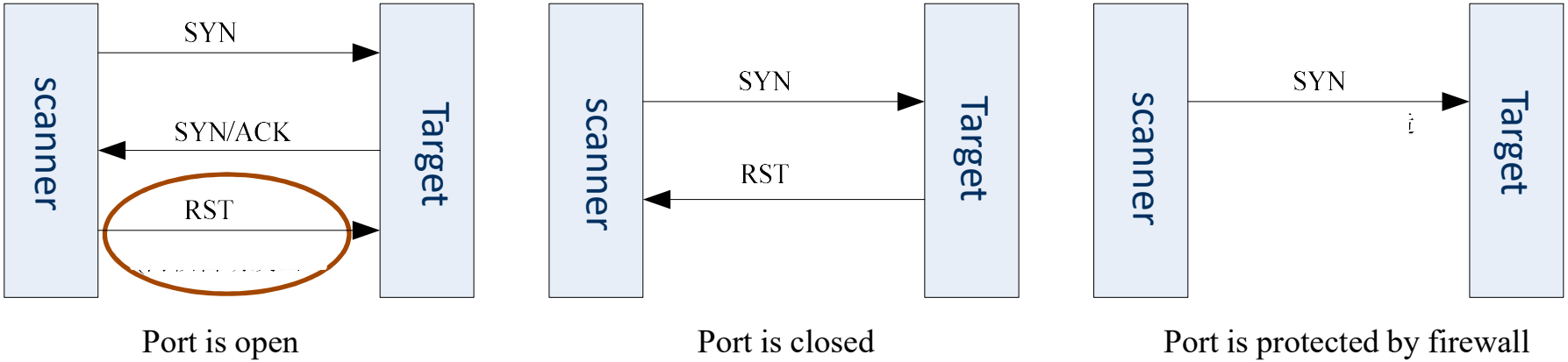
Connection Scanning

- Attempt to setup a TCP connection with the target device by invoking the transport layer API



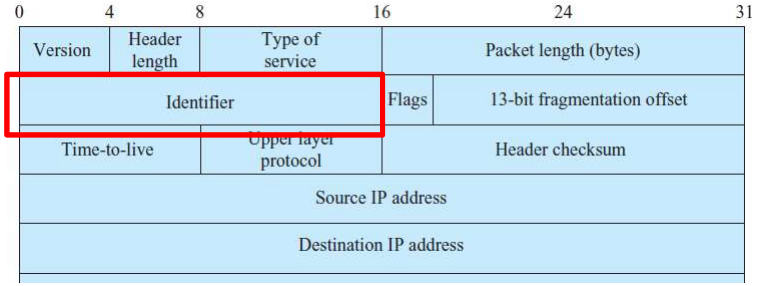
SYN scanning

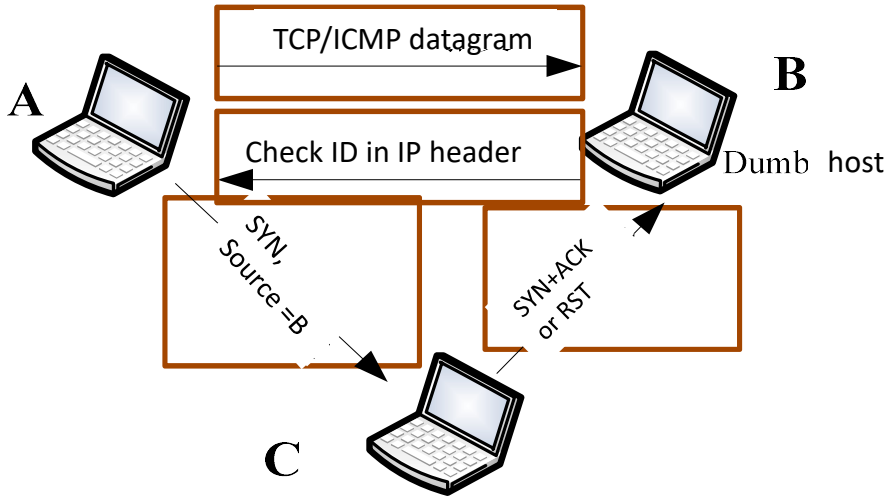
- To finish two handshakes when attempting to setup a TCP connection with the target port, no record is made in logs



Dumb scanning

- Need cooperation by a third device with less traffic
- Dumb scanning of IP header
  - A sends consecutive ICMP requests to B, then analyze the ID in the IP header
  - A send connection request (SYN) to the specified port of C, impersonating B
    - If the port is open, C responses B with SYN+ACK.
    - If the port is closed, C responses B with RST.
  - From B's response, i.e., ID in the IP header
    - If the port at C is open, ID increases by a big value, not 1
    - If the port at C is closed, ID increases by 1 regularly





The accuracy is dependent on B, B should have no connection with other devices.

Vulnerability scanning

Stockholm University

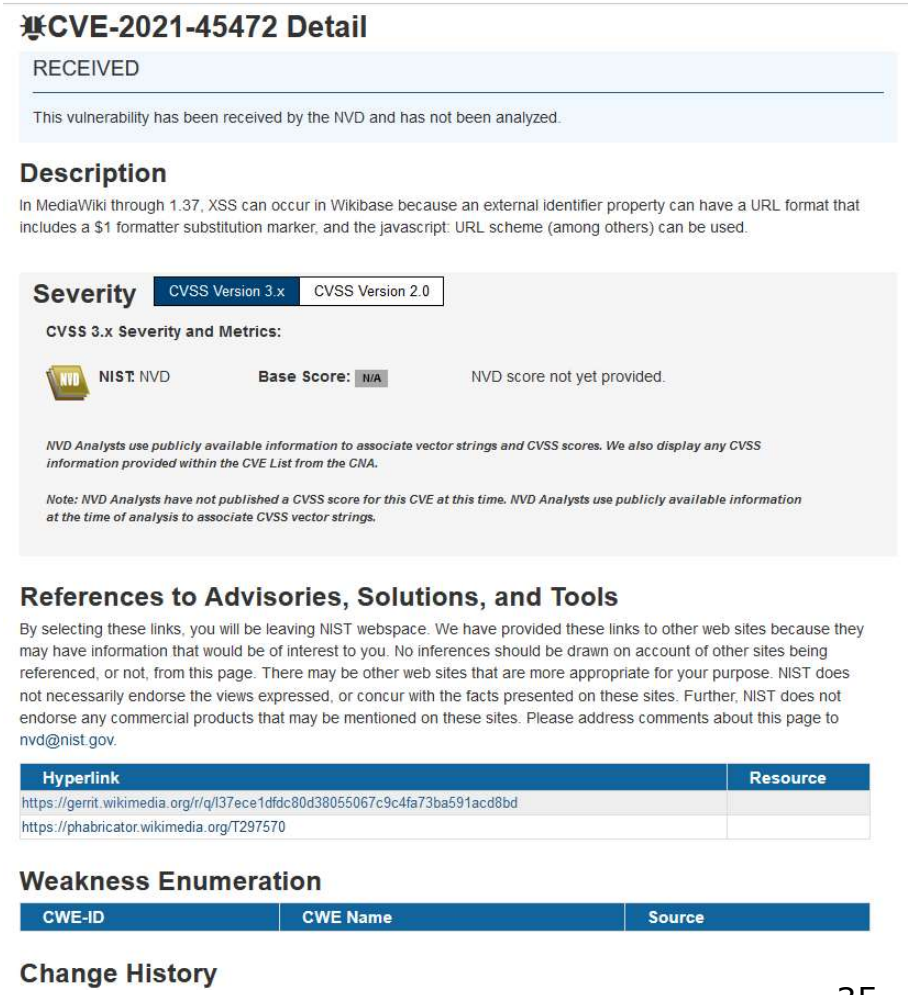
- To find the security holes in the applications and services in target networks -> key for conducting attacks!
- Vulnerabilities
  - OS: Windows, Linux, Mac OS, Unix
  - Applications and services: types, applications/services, and versions
  - Configurations: systems, applications/services, versions
- Approaches
  - Match the scanning results with known bases
  - Tentative attacks: probe if a security hole exists according to the known features or certain configurations
- Techniques
  - Vulnerability databases
  - Add-ons

Vulnerability databases

- CVE program and platform： https://www.cve.org/ (http://cve.mitre.org/)
  - Common Vulnerabilities and Exposures
  - Unique name to each vulnerability
- American National Vulnerability Database: https://nvd.nist.gov/

- https://vuldb.com/
- https://bugtraq.securityfocus.com/archive
- http://cvescan.com
- https://www.exploit-db.com/
- https://ics-cert.us-cert.gov/advisories

- National Computer Emergency Response Teams (CERTs) around the world (e.g., JP-CERT, CERT-US, and CERT-SE) usually publishes information about the latest critical vulnerabilities.
  - e.g. https://nvd.nist.gov/vuln/detail/CVE-2021-45472



CVE-2021-45472 Detail

RECEIVED

This vulnerability has been received by the NVD and has not been analyzed.

Description

In MediaWiki through 1.37, XSS can occur in Wikibase because an external identifier property can have a URL format that includes a $1 formatter substitution marker, and the javascript: URL scheme (among others) can be used.

Severity | CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: N/A NVD score not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://gerrit.wikimedia.org/r/q/I37ece1dfdc80d38055067c9c4fa73ba591acd8bd	
https://phabricator.wikimedia.org/T297570	

Weakness Enumeration

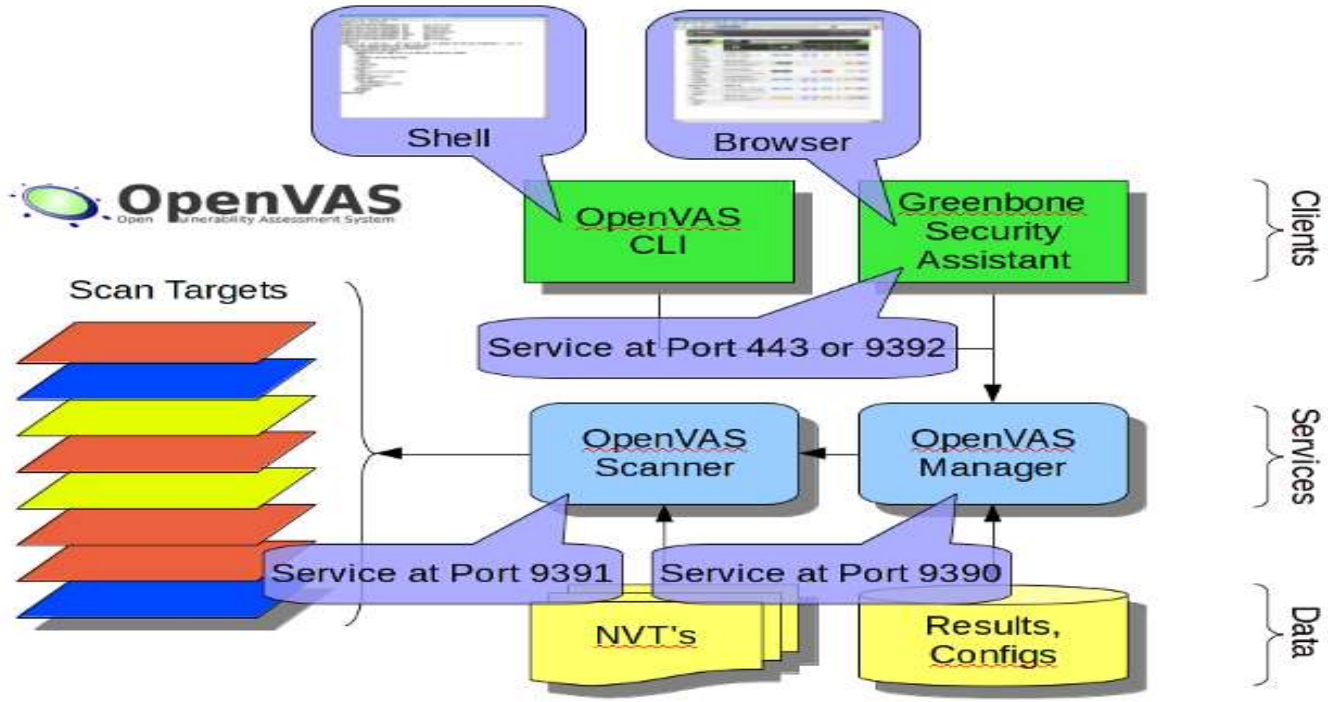
CWE-ID	CWE Name	Source

Change History

Tools

- Shadow Security Scanner: from Russia
- Nessus： system vulnerability scanning and analysis software
  - C/S, graphical interface
  - The server returns scanning results to the client
  - Add-ons: NASL(NESSUS Attack Scripting Language)
- OpenVAS： open vulnerability evaluation system

OpenVAS


Shell
Browser
OpenVAS
OpenVAS CLI
Greenbone Security Assistant
Clients
Scan Targets
Service at Port 443 or 9392
OpenVAS Scanner
OpenVAS Manager
Services
Service at Port 9391
Service at Port 9390
NVT's
Results, Configs
Data

Web vulnerability scanning

Stockholm University

- Security holes published by OWASP 2013
  - Injection flaw: e.g., SQL, OS, LDAP injection.
  - Wrong authentication and session management: bypass the authentication based on passwords, keys or tokens etc.
  - Cross-site vulnerability: e.g., session-hijacking
  - Insecure, direct object access: download password files, sensitive directories and databases
  - Mistakes in security configuration
  - Sensitive data leak: credit card information
  - Mistakes in access control
  - Fabricated cross-site request: log into the victim's browser (remotely), visit a web site, obtaining the session cookie and ID and other authentication information
  - Using components with known vulnerabilities
  - Unverified redirection: phishing

Tools for web vulnerability scanning -paid

Stockholm University

- Accunetix
  - Provide Online scanning
  - Good at SQL injection and XSS
- Appscan, IBM
  - Scan e.g., XSS, HTTP response splitting, falsified parameters, hidden fields processing, buffer overflow
- N-STALKER (originally N-Stealth) https://www.nstalker.com/alliance/
  - WebApp Security Scan to search for vulnerabilities such as SQL Injection, XSS, and known attacks.
  - 39,000 Web Attack Signature database along with a patent-pending Component-oriented Web Application Security Assessment technology

Tools for web vulnerability scanning – free

Stockholm University

- Nikto: scanning the known vulnerabilities on web server
- Golismero: Framework for web vulnerability scanning written in Python, integrated tools like Nikto, theharvester, sqlmap, OpenVAS
- VEGA: from Subgraph, Web program security test platform, effective for SQL injection, XSS, sensitive information leak and others
- Skipfish: from google, Web program evaluation tool, fast & low CPU occupation
- Sqlmap: written in Python, specialized for scanning and making use of SQL injection
- W3af: web attacking and evaluating tool written in Python

Summary

Stockholm University

- Network scanning: port, vulnerability (web vulnerability)
- Port scanning: full connection, half connection, dump
- Vulnerability scanning: approaches, techniques
- Web scanning

Expected learning outcomes

Stockholm University

- Describe the general procedure for performing network attacks
- Understand and explain the basic principles for information collection, network hiding and port and vulnerability scanning
- Acquaint yourself with some tools (the names and their major functions)

Thank you!