System and Network Security

Information System Security

Ing. Maroš Barabas

Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 2, 612 66 Brno
ibarabas@fit.vutbr.cz

BRNO
UNIVERSITY
OF TECHNOLOGY

FIT
FACULTY
OF INFORMATION
TECHNOLOGY

25.11.2015

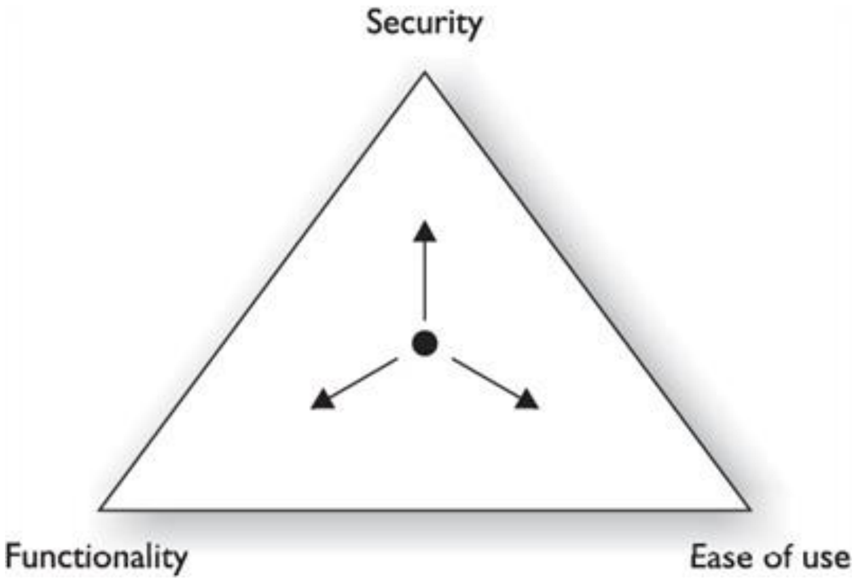
Security Basics

Security Basic Elements

- Confidentiality – measures taken to prevent **disclosure** of information or data to unauthorized individuals or systems
- Integrity – methods and actions taken to protect the information from unauthorized **alteration**
- Availability – ensures the data and resources **can be accessed** when legitimate users need them
- Non-repudiation, authentication, …

Security Basics

- Security, Functionality and Easy to Use Triangle
  - The more secure something is, the less usable and functional it becomes
  - The best security: Lock down, bury, without possibility to access



Defining Hacker

- White Hats
  - Ethical hackers, hired by a customer for testing, improving their security or other defensive purposes. Well respected and don’t use their skills and knowledge without prior consent.
- Black Hats
  - Using their skills illegally for either personal gain or malicious intent. Black Hats do not ask for permission or consent.
- Gray Hats
  - Neither good, nor bad. They are either curious about hacking or they feel like it’s their duty, with or without customer permission, to demonstrate security flaws in systems without permission.

- Hacktivist
  - hacker with political or ideological motivation
- Suicide Hacker
- Ethical Hacker

?
ANONYMOUS
We are Legion. We do not Forgive.
We do not Forget. Expect us.

Hacking Stages

- Reconnaissance
  - Gather evidence and information on the targets before attack.
  - Passive – gathering without the knowledge
  - Active – may or may not be discovered (more risk of discovery)
- Scanning and enumeration
  - Gather more in-depth information
- Gaining access
  - The main attack phase, bypassing security controls, abusing vulnerabilities, ..
- Escalation of privileges
  - Gaining more privileges within the system (from user to root)
- Maintaining access
  - Ensuring there is a way back to the system using backdoor
- Covering tracks
  - Hide before discovery

Testing Types

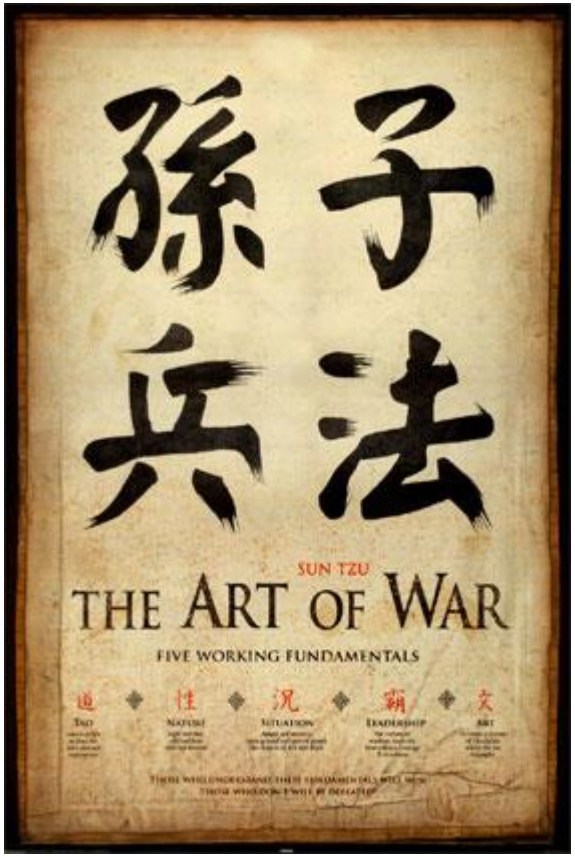
- Black Box
  - Method of software testing without knowledge of internal structure and code of the testing application. Usually used for purposes of testing from perspective of real attacker. Black box testing is designed to simulate the real unknown hacker from outside.
- White Box
  - Method of testing with access to internal structure of the application and/or code. It usually refers to a methodology where a tester has full knowledge of the testing application/system. . Designed to simulate internal threat – insider, disgruntled employee
- Grey Box
  - Combination of black-box and white-box testing, which benefits from straightforward technique of black-box testing and combines it with the knowledge base of code oriented white-box testing method.
  - Tester starts with some level of privileges targeting the escalation within the tested application, over network or system.

Reconnaissance - Vulnerabilities

- Vulnerability research
  - National Vulnerability Database (http://nvd.nist.gov)
  - Exploit Database (http://www.exploit-db.com)
  - CVE Details Database (http://ww.cvedetails.com)
  - Security Focus (http://www.securityfocus.com)

- Define victory before engaging in battle.
  - Sun Tzu – The Art of War

- ExploitKits, Exploit Tools
  - Metasploit



Reconnaissance - Stages

- Seven-Step Information-Gathering Process (CEH)
  - Information gathering
  - Determining the network range
  - Identifying active machines
  - Finding open ports and access points
  - OS fingerprinting
  - Fingerprinting services
  - Mapping the network attack surface

- Social networks
- Social engineering
- Tools: nmap

Footprinting

Looking for any information, no matter how big or small, that might give a better insight into the target

- Process of gathering information on systems, applications and network

- Active Footprinting
  - Require to take actions on the target
  - Scan against computers, banner grabbing
- Passive Footprinting
  - Without interacting or communicating with the target
  - Public information, web, DNS, Social Engineering, Competitive intelligence

- Anonymous vs. Pseudonymous

DNS Footprinting

- DNS – mapping service for names and IP addresses
- IANA – Internet Assigned Numbers Authority
- Full of information about internal structure, IP addresses, systems
- Record Types:

SRV	Service
SOA	Start of Authority
PTR	Pointer
NS	Name Server
MX	Mail Exchange
CNAME	Canonical Name
A	Address

- DNS poisoning and DNSSEC
- Tools: whois, nslookup, dig, tracert, traceroute

DNS Footprinting

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> kazi.fit.vutbr.cz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19080
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
;kazi.fit.vutbr.cz.              IN      A

;; ANSWER SECTION:
kazi.fit.vutbr.cz.       5       IN      A       147.229.8.12

;; AUTHORITY SECTION:
fit.vutbr.cz.            5       IN      NS      rhino.cis.vutbr.cz.
fit.vutbr.cz.            5       IN      NS      kazi.fit.vutbr.cz.
fit.vutbr.cz.            5       IN      NS      guta.fit.vutbr.cz.
fit.vutbr.cz.            5       IN      NS      gate.feec.vutbr.cz.

;; ADDITIONAL SECTION:
gate.feec.vutbr.cz.      5       IN      A       147.229.71.10
guta.fit.vutbr.cz.       5       IN      A       147.229.9.11
guta.fit.vutbr.cz.       5       IN      AAAA    2001:67c:1220:809::93e5:90b
rhino.cis.vutbr.cz.      5       IN      A       147.229.3.10
rhino.cis.vutbr.cz.      5       IN      AAAA    2001:67c:1220:e000::93e5:30a

;; Query time: 31 msec
;; SERVER: 192.168.233.2#53(192.168.233.2)
;; WHEN: Wed Oct 30 13:52:33 2013
;; MSG SIZE  rcvd: 236
```

Google Hacking

- Vulnerabilities
  - "#-Frontpage-" inurl:administrators.pwd
  - cache:"access denied for user" "using password"

- Cameras
  - inurl:"ViewerFrame?Mode="
  - inurl:control/userimage

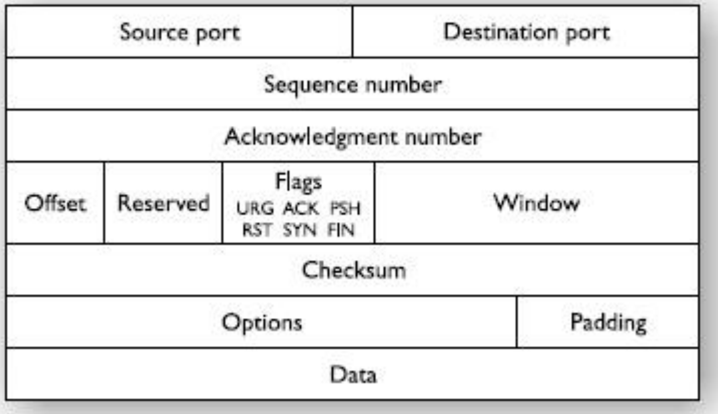
- Server files
  - intitle:index.of
  - cache:define inurl:/conf

- Anonymous googling:
  - Use cache, "&strip=1"

Scanning and Enumeration

Process of discovering systems on network and open ports and identifying applications

- Identify live systems
  - Ping each IP address of the subnet to see which IP is alive
  - Using ICMP protocol, TCP scanning
  - Could be blocked by FW, IDS/IPS systems
- Discover open ports
  - Scanning ports of the systems to identify listening services
  - Horizontal Scan – a scan of multiple hosts against one port
  - Vertical Scan – scan of one host and all port
  - Port range: 0 – 1023 – 49 151 – 65 535
- Nmap
  - Open-source network scanning tool



Source port | Destination port
Sequence number
Acknowledgment number
Offset | Reserved | Flags URG ACK PSH RST SYN FIN | Window
Checksum
Options | Padding
Data

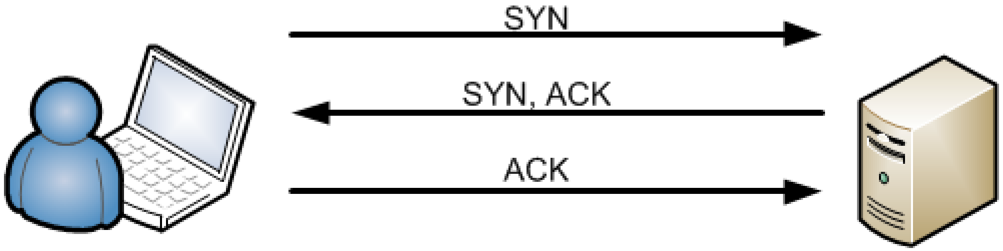
Scanning and Enumeration

- Identify operating system and services
  - Fingerprinting – analyze OS and service replies to identify operating system
  - Banner grabbing – analyzing the banner of the service to identify version, os, type of service and more

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-30 13:54 EDT
Nmap scan report for 192.168.233.1
Host is up (0.00059s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open     https
445/tcp   filtered microsoft-ds
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: general purpose
Running: Microsoft Windows 2008|7
```

- Scan for vulnerabilities
  - Versions of services and OS with known vulnerabilities
  - Specialized tools: Nessus

Scan Types



- Scan Types and TCP Flags with response

Scan Type	Initial Flags Set	Open Port Response	Closed Port Response
Full (TCP Connect)	SYN	SYN/ACK	RST
Half Open	SYN	SYN/ACK	RST
XMAS	FIN/URG/PSH	No response	RST/ACK
FIN	FIN	No response	RST/ACK
NULL	No flags set	No response	RST/ACK
ACK	ACK	RST	No response

Nmap

- Determine live systems

```
nmap -sP -v 192.168.1.0/24
```

- Use TCP sweep to evade ICMP blocking

```
nmap -PT 192.168.1.0/24
```

- SYN scan with identifying of operating system

```
nmap -sS -O 192.168.1.100
```

- UDP scan

```
nmap -sU 192.168.1.100
```

- TCP Full connect scan outputting the result into file

```
nmap -sT -oN results.txt 192.168.1.100
```

Banner grabbing

- Commonly by telnet, proxy for web applications, and other tools
- *telnet <IP address> <port>*

```
HTTP/1.1 302 Found
Date: Wed, 30 Oct 2013 18:03:03 GMT
Server: Apache/1.3.42 Ben-SSL/1.59 (Unix) PHP/5.2.17
X-Powered-By: PHP/5.2.17
Location: http://www.feec.vutbr.cz/fakulta/home.php.cz
Connection: close
Content-Type: text/html; charset=iso-8859-2
X-Pad: avoid browser bug
```

```
220 mailserver.domain.com Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329
```

```
220 192.168.1.1 FTP Server (version wu-2.6.2+Sun) ready.
```

```
SSH-2.0-OpenSSH_6.3p1-hpn14v2 FreeBSD-openssh-portable-6.3.p1,1
```

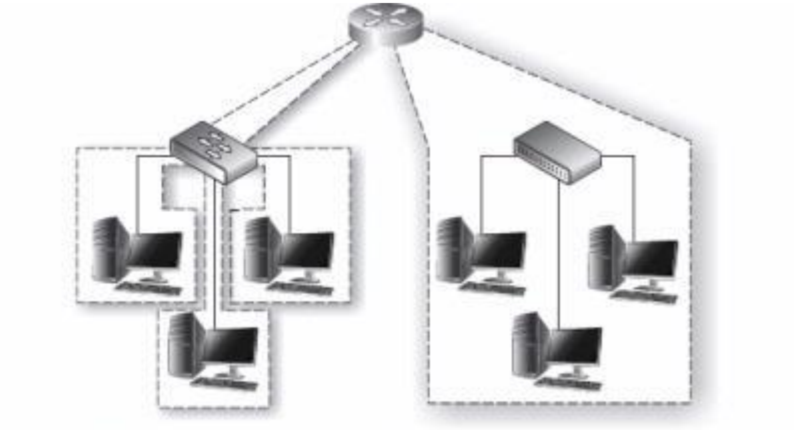
Scanning and Enumeration

- Proxy
  - Using specialized systems to hide IP address by replicating traffic through proxy
  - TOR – onion designed proxy service
- IP spoofing
  - Obscure the source IP address
  - Spoofing IP address may lead the packet never finds its way back
- Source routing
  - Specifying the route of a packet regardless of route tables
  - The attacker can use an IP address of another machine on the subnet and have all the return traffic sent back, regardless of which routers are in transit.
  - Most firewalls and routers detect and block source-routed packets
- Anonymizers
  - services to hide the identity, IP address, country of origin, etc.
  - http://www.anonymouse.org

Sniffing

Capturing packets from wire or air to analyze and find interesting information

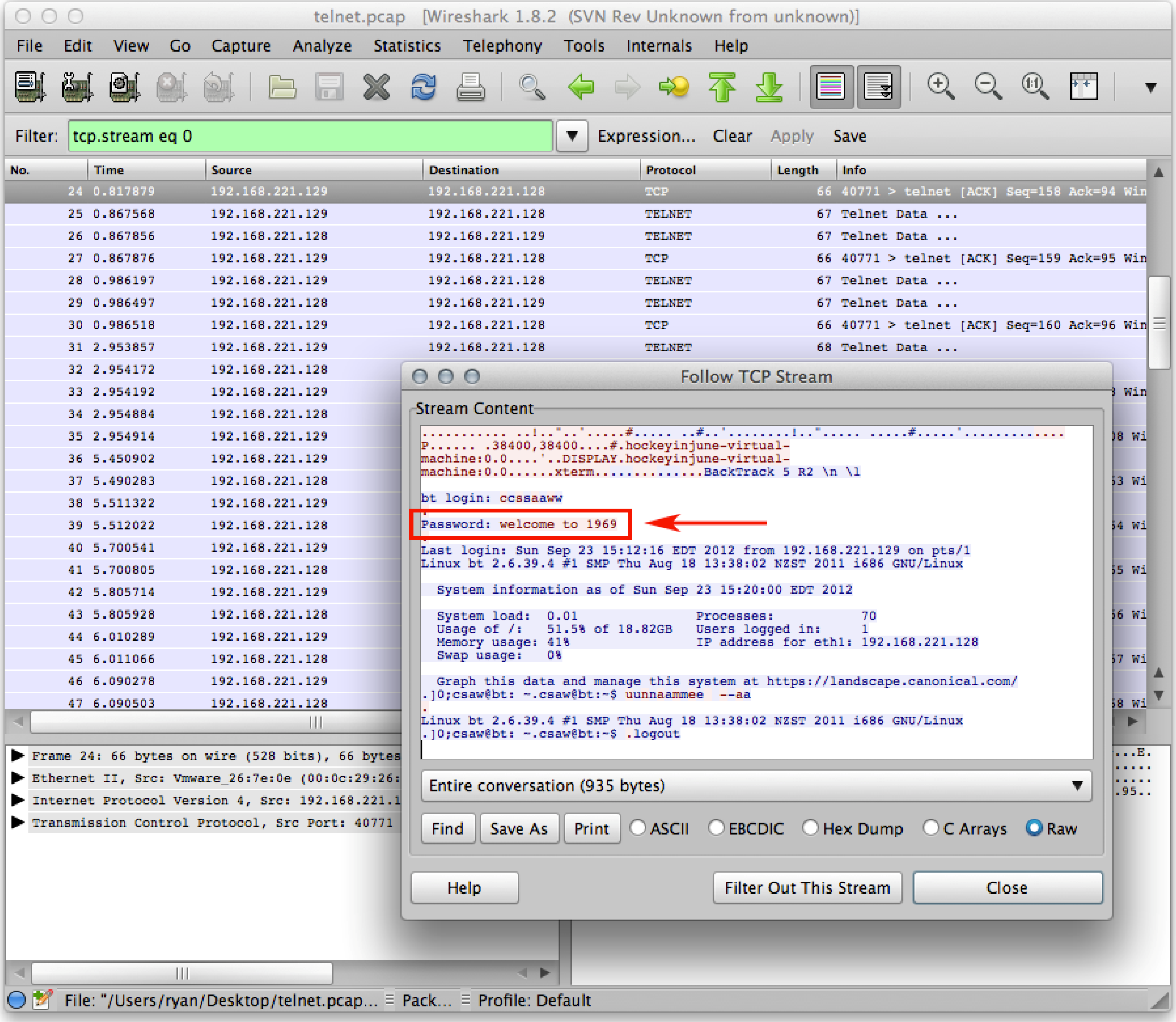
- Promiscuous mode of the network interface for capturing all packets regardless of source and destination IP address
  - Portable devices, phones, tablets?
- Collision domains
  - Sharing the transport medium
  - Switched network – how to sniff?
- Open protocols without encryption
  - All information available for sniffer
  - HTTP without SSL
  - Username / Passwords
- *tcpdump, wireshark, ettercap*



A switch splits the collision domain: 4 domains.
An attacker on A can only see traffic intended for A.

Shared media using a hub: 1 collision domain
An attacker on A can see all traffic for B and C.

Capturing by Wireshark



telnet.pcap [Wireshark 1.8.2 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp.stream eq 0

```
No.  Time      Source           Destination      Protocol  Length Info
  24 0.817879  192.168.221.129  192.168.221.128  TCP           66 40771 > telnet [ACK] Seq=158 Ack=94 Win
  25 0.867568  192.168.221.129  192.168.221.128  TELNET        67 Telnet Data ...
  26 0.867856  192.168.221.128  192.168.221.129  TELNET        67 Telnet Data ...
  27 0.867876  192.168.221.129  192.168.221.128  TCP           66 40771 > telnet [ACK] Seq=159 Ack=95 Win
  28 0.986197  192.168.221.129  192.168.221.128  TELNET        67 Telnet Data ...
  29 0.986497  192.168.221.128  192.168.221.129  TELNET        67 Telnet Data ...
  30 0.986518  192.168.221.129  192.168.221.128  TCP           66 40771 > telnet [ACK] Seq=160 Ack=96 Win
  31 2.953857  192.168.221.129  192.168.221.128  TELNET        68 Telnet Data ...
  32 2.954172  192.168.221.128
  33 2.954192  192.168.221.129
  34 2.954884  192.168.221.128
  35 2.954914  192.168.221.129
  36 5.450902  192.168.221.129
  37 5.490283  192.168.221.128
  38 5.511322  192.168.221.129
  39 5.512022  192.168.221.128
  40 5.700541  192.168.221.129
  41 5.700805  192.168.221.128
  42 5.805714  192.168.221.129
  43 5.805928  192.168.221.128
  44 6.010289  192.168.221.129
  45 6.011066  192.168.221.128
  46 6.090278  192.168.221.129
  47 6.090503  192.168.221.128
```

```
▶ Frame 24: 66 bytes on wire (528 bits), 66 bytes
▶ Ethernet II, Src: Vmware_26:7e:0e (00:0c:29:26:
▶ Internet Protocol Version 4, Src: 192.168.221.1
▶ Transmission Control Protocol, Src Port: 40771
```

Follow TCP Stream

Stream Content

```
........... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'............
P...... .38400,38400....#.hockeyinjune-virtual-
machine:0.0....'..DISPLAY.hockeyinjune-virtual-
machine:0.0......xterm.............BackTrack 5 R2 \n \l

bt login: ccssaaww
.
Password: welcome to 1969
.
Last login: Sun Sep 23 15:12:16 EDT 2012 from 192.168.221.129 on pts/1
Linux bt 2.6.39.4 #1 SMP Thu Aug 18 13:38:02 NZST 2011 i686 GNU/Linux

  System information as of Sun Sep 23 15:20:00 EDT 2012

  System load:  0.01               Processes:           70
  Usage of /:   51.5% of 18.82GB   Users logged in:     1
  Memory usage: 41%                IP address for eth1: 192.168.221.128
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/
.]0;csaw@bt: ~.csaw@bt:~$ uunnaammee  --aa
.
Linux bt 2.6.39.4 #1 SMP Thu Aug 18 13:38:02 NZST 2011 i686 GNU/Linux
.]0;csaw@bt: ~.csaw@bt:~$ .logout
```

Entire conversation (935 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

File: "/Users/ryan/Desktop/telnet.pcap... Pack... Profile: Default

Evade Security Controls

- ARP protocol
  - ARP is broadcast protocol for communication within collision domain
  - IP address translated to MAC address
  - CAM table – content addressable memory, all MAC addresses
- ARP Flooding
  - Generating ARP packets to fill CAM table. When CAM table is full and switch receives a message with no entry in CAM table, it will broadcast the message to all ports turning itself into a hub.
  - In case of multiple entries in CAM table, the last record is used.
  - Port security – manually assign MAC address to a specific port
- MAC spoofing
  - Valid user with MAC *0A-1B-2C-3D-4E-6F* is connected to port 2. An attacker connects to port 3 and spoof *0a-1B-2C-3D-4E-5F* MAC address. The switch will notice that the MAC address of valid user, formally on port 2, seems to have moved to port 3 and updates CAM table. The attacker will see all communication to valid user as long as this is kept up.

Intrusion Detection Systems

Tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity

- Network system for monitoring and detection network activities of malicious or unwanted behavior
- Alert administrator or other security mechanisms
- Capture and analyze communication on the network interface
- Detect malicious code
- Provides information about illegal acivity
- Passive mechanism (does not prevent the malicious behavior)

- Host, Network based IDS and IPS systems
- Evasion: IP fragmentation, Unicode characters, Slow actions

Firewalls and Honeypots

- Firewalls
  - Rule-based packet filters. First rule matched executes.
  - Stateful inspection firewalls – tracks the entire status of the connection
  - ICMP blocked with error code Type 3 Code 13
  - Firewalking – determine what is opened on Firewall
  - WAF – Web Application Firewall
  - HTTP Tunneling – evasion technique tunneling protocols over HTTP
  - ACK Tunnel – communicating with ACK messages

- Honeypots
  - Honey pot – Invitation for attackers as easy meat, often vulnerable to various types of attacks, full of services
  - Capability of obtaining lot of information about attack, malware
  - Can record the attack vector, characteristics and behavior, used tools, methods, exploits
  - Best way to get new type of attacks, zero-day vulnerabilities, codes, programs to further analysis

Password cracking

- Bad Passwords
  - Short, blank, usernames, common dictionary, default values
  - Dictionary words: `password`, `Heslo123`, `qwerty`, `asdasdasd`, `test`, …
- Password attacks
  - Dictionary attack – enumerate commonly used passwords
  - Bruteforce attack – all possible combinations
  - Hybrid attack – dictionary attack with variable upper/lower case, numbers
  - Replay attack – Don’t break hash, replay the packet/message
- Kerberos
- Keyloggers
  - Software, Hardware
  - AV software can detect?

Windows Essentials

- Patch Management
  - Most problematic security threat is out-of-date windows machine
  - 0-day (zero-day) vulnerabilities and exploits – Microsoft has zero day to patch the vulnerability

- Passwords
  - Stored in SAM file, located in *c:\windows\system32\config* directory.
  - LAN Manager, NTLM, NTLMv2 – MD5
  - Rainbow Tables

- Escalating Privileges
  1. Obtain administrator password
  2. Take advantage of found vulnerability
  3. Use Metasploit
  4. Social Engineering

Linux Security

- File-system security
  - Access control through users permissions

```
chmod 777 file
```

  - Dangerous SUID bits

```
-rwsr-xr-x 1 root    root      937532 Jan  2  2013 exim4
-rwsr-xr-- 1 root    dip       302176 Jun 22  2012 pppdt
```

- Passwords
  - Located in clear-text in /etc/passwd, if shadowed in /etc/shadow

```
root:x:0:0:root:/root:/bin/bash
user:x:500:500:Maros Barabas:/home/user:/bin/bash
```

```
user:$1$fnfffc$pGteyHdicpGOfffXX4ow#5:13064:0:9999:7:::
```

Buffer Overflow

```
#include <string.h>

void f(char* s) {
    char buffer[10];
    strcpy(buffer, s);
}
```

- The faulty code does not check that the source buffer is too large to fit in the destination buffer.
- When the function returns, the CPU unwinds the stack frame and pops the (now modified) return address from the stack.
- Control does not return to the function as it should. Instead, arbitrary code (chosen by the attacker when crafting the initial input) is executed.

- Defense:
    - Code auditing
    - Non-executable stacks
    - Randomize virtual address space

- http://insecure.org/stf/smashstack.html

Security Hardening

- Least Privileges
  - Grant only those privileges that are necessary
  - Run services with non-privileged users
  - Restrict remote access to privileged accounts

- Minimalize attack surface
  - Stop and remove all unnecessary services
  - Remove all not used personal and non-personal accounts
  - Remove all unused libraries, tools, packages

- Keep security high
  - Set policy for password strength (8 length, characters, numbers, special chars, not dictionary)
  - Set firewall with least privilege rules policy

Rootkits

Collection of software put in place by an attacker that is designed to obscure system compromise

- Application level
  - Works within the application, change application’s behavior, user rights level, and actions
- Kernel level
  - Attacks boot sectors and kernel level of the operating system, most dangerous and difficult to detect
- Library level
  - Uses system-level calls to hide its existence

Human Based

- Dumper Diving
  - Rifling through the dumpsters, paper-recycling bins, and office trashcans
- Impersonation
  - Pretending to be employee, a valid user, executive (VIP)
- Technical Support
  - Form of impersonation aimed at technical support to solve problems such forgot password
- Shoulder Surfing
  - Look over the shoulder to watch them log in or access sensitive data even from long distance
- Tailgating and Piggybacking
  - Follow authorized person through open door
  - Piggybacking – ask for help, convincing lost or forget badge

Computer Based

- Social networks
  - Facebook, Google+, Linkedin, Twitter, …
  - Plenty of personal or professional information for attack
  - Friend of a friend

- Phishing
  - Crafting an e-mail that appears legitimate, but in fact contains malware, links to fake websites or to download malicious content
  - No security technology is able to detect

- Rogue security software
  - Modern implementation of malware
  - Fake AV programs carrying malware

- Disgruntled employee
  - Easy to convince, lot of sensitive information
  - Biggest threat to company

Other Attacks

- Reflected / Spoofed attack
  - Spoofing target IP address and sending huge amount of SYN, SYN/ACK packets to list of zombies. They reply with RST to the target.
- Ping of Death
  - RFC unspecified behavior with large ping payload crashing target operating system
- Smurf attack
  - Sent large number of ICMP packets with source IP address of target to broadcast, all machines will reply to target use all bandwidth preventing legitimate traffic to reach the destination.
- SYN flood
  - Large number of SYN packets sent to target "half-open" the target connection saturating the number of connections. The client is not able to receive more connections denying legitimate ones.
- Teardrop attack
  - Using IP fragmentation with over-sized payloads. After re-assembling the packets on the target machine, crashing due to vulnerability in the re-assembling code.

Conclusion

- Practice
  - Only on localhost, local virtual network. Never attack anyone!
  - Not even with prior consent – illegal!
  - Use Kali Linux (www.kali.org)
  - Get familiar with vulnerabilities, tools, sec. technologies

- Professional Penetration Testing, 2nd edition, T. Wilhelm, 2013, ISBN: 9780124046184

- https://www.google.cz/search?q=penetration+testing+how+to
- RTFM, Google, Ask

- Do projects, alone!

Pokračovanie

- **2. 12. 2015**
  - Bezpečnosť bezdrôtových sietí (Matej Kačic)
- **9. 12. 2015**
  - ?
- **16. 12. 2015**
  - ?

ĎAKUJEM!