Cyber Security Workshop 2015

"INTRODUCTION"

By

Ashish Belwase

KU SECURITY RESEARCHER

Disclaimer

- Any information disclosed in this series is provided for sole purpose of learning computer security. We do not take any responsibility for any misuse of any information we provide. We only suggest to audit the systems that you have permission on.

Cyber Security Workshop 2015

- Prereq: Basic programming,networking,Unix
- Enjoy playing with systems,network,analysing data
- Introduce core concepts in software/web/network security
- Making participants familiar with security tools
- Make participants able to make their software/network strong and defend against various attacks
- We'll learn many more technologies and you have to decide at the end in which you'll go more

Security Expert Career

- Network Security Engineer
- Information System Security
- Software Security Analyst
- Static Checker
- Bug Tester
- Penetration Tester

Training Contents

- Overview of Computer Security & Hacking
- Basic of Networking & Internet
- Basics of Ethical Hacking(5 steps)
- Cryptography & Phishing
- Browser Security Model
- SQL Injection
- XSS Attacks
- Network Security
- DDOS
- WiFi Cracking
- Metasploit
- Cryptography
- Wrap-up

Some Security Terms

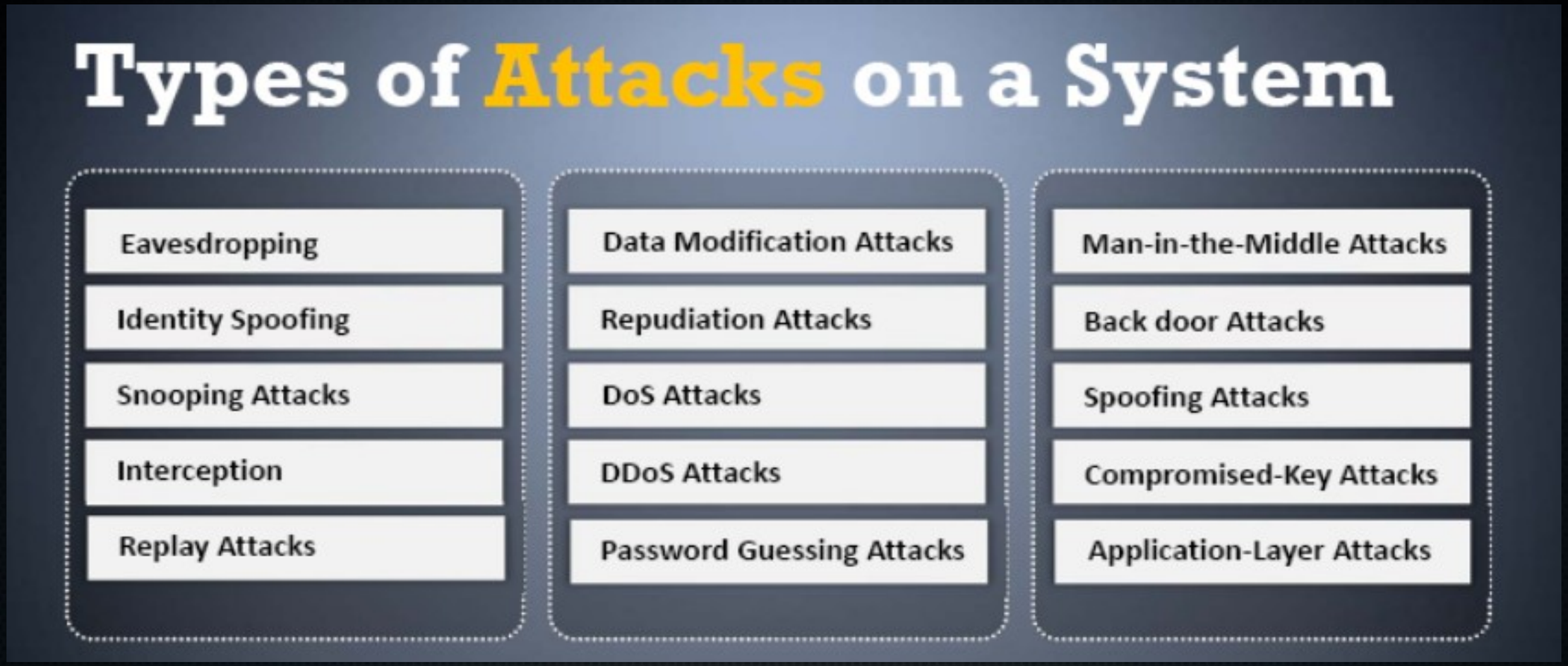
- Hacking[Forcing system to do thing for what it is not intended to do]
- Hacker [Black Hat,White Hat,Gray Hat]
- Black Box[hire penetration tester] & White Box Test[simple SQL]
- Vulnerability[Flaw or Loophole on the system,code]
- Exploit [Proof the vulnerability is valid]
- 0-Day [First time discovery of vulnerability]
- Penetration Test[Entering into the system]

Virtualization

- Using multiple OS on same host
- Very useful for security testing
- Network isolation, security,portable,easy maintenance
- Vmware , Virtualbox
- Linux OS
- Kali, Backtrack
-

5 stages of Ethical Hacking

- Reconnaisance
  - Gathering maximum information[Network,System,Organization]
- Scanning
  - IP, OS, Services, Ports
- Gaining Access
  - Exploiting,Penetrating,System Hacking,Pw cracking,BO,DDOS
- Maintaining Access
  - Backdoors,Botnets,Trojans,Rootkits
- Covering Tracks
  - Log Clearance



- OS Attacks [Buffer overflow, Unpatched bugs]
- Mis-configuration attacks [invalid settings, permissions]
- Shrink wrap code attacks[additional script of a program]
- Application level attacks [BO,DDOS,SQL,Phishing]


Defense in Depth
Defense in Depth Layers
Policies, Procedures, and Awareness
Physical
Perimeter
Internal Network
Host
Application
Data
Defense in Depth Layers

Skills of an Ethical Hacker

Platform Knowledge

Has in-depth knowledge of target platforms, such as Windows, Unix, and Linux

Network Knowledge

Has exemplary knowledge of networking and related hardware and software

Computer Expert

Should be a computer expert adept at technical domains

Security Knowledge

Has knowledge of security areas and related issues

Technical knowledge

Has "high technical" knowledge to launch the sophisticated attacks

Skills needed

- Platform expert [Linux]
- Programming[Any language]
- Computer Networking
- **Security Knowledge [Focus of this Workshop]**
- Information Technology Expert

Tools & Platforms

- Virtualization [Vmware or VirtualBox]
- OS [Linux : Kali or any other]
- Reconnaissance Tools [whois, dig, traceroute, and nslookup]
- Network Scanning [Nmap,Nessus,eEye Retina,Wireshark]
- Exploitation [Metasploit,Armitage]
- Web[Webscrap,SQLMAP,Nikto]
- Testing [DVWA]

Networking Revision

- Network Administration Handsout

Information Gathering

- Who is our client/victim?
- What information they have ?
- ISP info
- Types of work there
- System,network,software info.
- **Tools**
  - Logic(your brain), google(dorking), social media,
  - Website(scanners,whois)
  - Social engineering

Enumeration

- Googling
- Netcraft
- Whois ntc.net.np
- Whois facebook -h whois.arin.net
- Nslookup,dig,host

Googling:Syntax : Operator : search_term

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject	yes	yes	like	like	yes	like intitle

Googling:Syntax : Operator : search_term

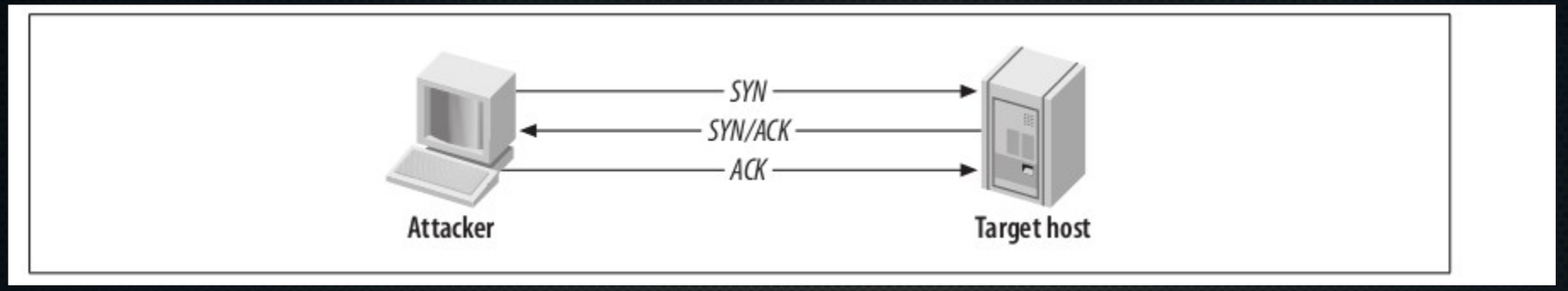
- allintitle:“index of /data“ site:.nasa.gov
-
-

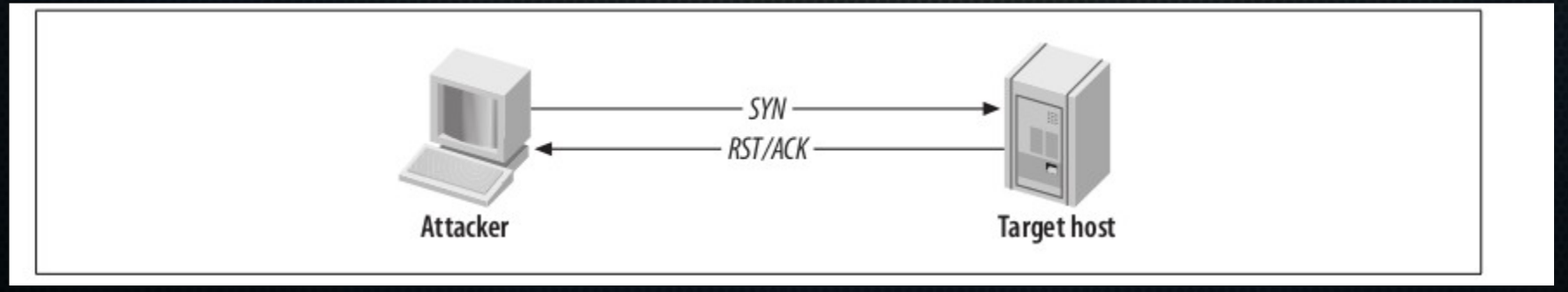
Enumeration Countermeasures

- Prevent traversing of directory in web servers
- Configure all name servers to disallow DNS zone transfers to untrusted hosts,
- Configure SMTP servers either to ignore email messages to unknown recipients
-
-
-

Network Scanning

- Vanilla Connect Scanning Method





A vanilla TCP scan result when a port is open(fig1) and closed(fig2)

Scanning Tools

- Port Scanning : nmap,hping3,netcat
- Vulnerability Scanners : OpenVAS,nessus, Metasploit+Armitage,web scanners
- Telnet / Banner Grabbing / Verification
- Port Checking
-

Reconnaisance(scanning)

- first check the ip address : ifconfig
- netbios scan : nbtscan -r 192.168.5.1/24 > nb_file
- Lets find the open port on 192.168.5.12 : nmap -A 192.168.5.1-30 -p 21,22
  - -A(host discovery) or -p21-30 , -oX nmap.xml
- convert the nmap result to webpage => xsltproc nmap.xml -o /var/www/nmap.html
- now check the open ports for any vulnerability.=> openvas,nessus,msf

Network Scanning

- NMAP [perform ICMP ping sweep scans of target IPblocks]
  - Syntax : #nmap [ScanType] [Options] {targets}
  - Basic scanning
  - Discovery Options
  - Firwall Evasion
  - Version Detection
-

Network Scanning

- Enumerating subnet network and broadcast addresses with Nmap
  - nmap -sP 192.168.0.1/24
- Operating system fingerprinting using Xprobe 2
  - Xprobe2 -v 192.168.0.43
-
  -
  -

Prevent Scanning

- Close unnecessary services
  - /etc/inetd.conf
  - Runlevels
- Limit the amount of information given to port scans is to utilize PortSentry offered by Psionic. PortSentry detects connection requests on a number of selected ports.
- Employ TCP Wrappers
  - give the administrator the flexibility to permit or deny access to the services based upon IP addresses or domain names.

Vulnerability Assestment

- Acunetix
- Vega
- Uniscan [uniscan -u 'site' -qweds]
- OpenVAS

Web Server Scanning

- Using the HTTP HEAD method against Apache
  - Telnet ntc.net.np 80 : HEAD / HTTP/1.0
  -
-