

Password

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Details

- ❖ **Password**
- ❖ Deal with **Cracking**
- ❖ **Passive** Action
- ❖ Simulation
- ❖ Discussion



Password

- ❖ Why ?
- ❖ “Kata Kunci”
 - ❖ diansastro
 - ❖ 090382
 - ❖ mickey



Password

- ❖ Panjang Minimum 6 Karakter
- ❖ Tidak Ber-Makna (bukan nama pacar, bukan tanggal lahir)
- ❖ Kombinasi Huruf, Angka dan karakter lain
- ❖ Username ~~X~~ Password
- ❖ Perlu Pengamanan extra



Password

PassPhrase ?

- ❖ D1an545TR0
- ❖ 4m1nkExtravaganz4
- ❖ KaptenTSUBASA

Simulation

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Simulation !

- ❖ Cracking windows Password
 - ❖ via linux
 - ❖ via windows
- ❖ Cracking Linux Password
- ❖ Remote Cracking



Cracking windows Password

❖ Tools

❖ **Bkhive + sampdump2** (getting hash)

❖ **Pwdump2** (getting hash)

❖ **John the ripper** for cracking the hash

❖ Database password : SAM file , *system*

```
y3dips@heaven:~/windows-pass/winpass$ bkhive system saved-syskey.txt
Bkhive ncuomo@studenti.unina.it
```

```
Bootkey: 4fb1296aed69dc88c406f148567a833b
```

```
y3dips@heaven:~/windows-pass/winpass$ samdump
```

```
bash: samdump: command not found
```

```
y3dips@heaven:~/windows-pass/winpass$ samdump2
```

```
Samdump2 ncuomo@studenti.unina.it
```

```
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)
```

```
Usage:
```

```
samdump2 samhive keyfile
```

```
y3dips@heaven:~/windows-pass/winpass$ samdump2 SAM saved-syskey.txt >pass.
txt
```

```
Samdump2 ncuomo@studenti.unina.it
```

```
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)
```

```
No password for user Guest(501)
```

```
No password for user SUPPORT_388945a0(1002)
```

```
y3dips@heaven:~/windows-pass/winpass$ ls
```

```
key.txt pass.txt SAM saved-syskey.txt system
```

```
y3dips@heaven:~/windows-pass/winpass$ john pass.txt w:key.txt
```

```
Loaded 6 passwords with no different salts (NTLMv2 hashes)
```

```
ST022 (Administrator:1)
```

```
guesses: 1 time: 0:00:00:00 100% c/s: 18.00 trying: WLAHF - 163894
```

```
y3dips@heaven:~/windows-pass/winpass$ █
```

Simulation

Directory of D:\sploit\windows\syskey

```

01/26/2006  11:29 AM    <DIR>          .
01/26/2006  11:29 AM    <DIR>          ..
01/02/2004  01:45 AM             49,152 Bkhive.exe
01/02/2004  01:44 AM             45,056 Bkreg.exe
01/02/2004  01:45 AM             49,152 Sandump2.exe
01/26/2006  11:30 AM    <DIR>          bi
                3 File(s)      143,360 bytes
                3 Dir(s)      461,160,448 bytes free

```

```

D:\sploit\windows\syskey>hkhive bi\system syskey.txt
Bkhive ncuomo@studenti.unina.it

```

Bootkey: 7b2d921c4792b4c892c601f78299cd9e

```

D:\sploit\windows\syskey>Sandump2.exe bi\sam syskey.txt > password.txt
Sandump2 ncuomo@studenti.unina.it
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)

```

```

No password for user Guest(501)
No U value!

```

```

D:\sploit\windows\syskey>dir
Volume in drive D is DATA
Volume Serial Number is 81BD-0B36

```

Directory of D:\sploit\windows\syskey

```

01/26/2006  11:29 AM    <DIR>          .
01/26/2006  11:29 AM    <DIR>          ..
01/02/2004  01:45 AM             49,152 Bkhive.exe
01/02/2004  01:44 AM             45,056 Bkreg.exe
01/02/2004  01:45 AM             49,152 Sandump2.exe
01/26/2006  11:30 AM    <DIR>          bi
01/26/2006  11:36 AM                16 syskey.txt
01/26/2006  11:36 AM                177 password.txt
                5 File(s)      143,553 bytes
                3 Dir(s)      461,156,352 bytes free

```

```

D:\sploit\windows\syskey>type password.txt
Administrator:500:d116ffffa7d12e90fc65a44ac7667bc80:e8eaa6c1327f7ba53db3239136339d7b:::
HelpAssistant:1000:db7fd173800ac94874fa2e7da53727b6:67571a0904ad122e6b40fd7d49cb71e7:::

```

```

D:\sploit\windows\syskey>type password.txt
Administrator:500:d116ffffa7d12e90fc65a44ac7667bc80:e8eaa6c1327f7ba53db3239136339d7b:::
HelpAssistant:1000:db7fd173800ac94874fa2e7da53727b6:67571a0904ad122e6b40fd7d49cb71e7:::

```

D:\sploit\windows\syskey>

Simulation

Windows Task Manager

File Options View Shut Down Help

Applications Processes Performance Networking Users

Image Name	User Name	CPU	Mem Usage
agentsvr.exe	amwk	00	912 K
COMOMC.exe	amwk	00	1,328 K
opera.exe	amwk	00	13,772 K
wmplayer.exe	amwk	30	6,672 K
taskmgr.exe	amwk	02	2,124 K
explorer.exe	amwk	00	13,080 K
wuauclt.exe	amwk	00	1,476 K
svchost.exe	SYSTEM	00	736 K
alg.exe	LOCAL SERVICE	00	1,588 K
cmd.exe	amwk	00	1,756 K
Fireworks.exe	amwk	00	20,836 K
UStorSrv.exe	SYSTEM	00	828 K
kavsvc.exe	SYSTEM	00	10,828 K
svchost.exe	LOCAL SERVICE	00	908 K
spoolsv.exe	SYSTEM	00	2,524 K
svchost.exe	LOCAL SERVICE	00	2,572 K
svchost.exe	NETWORK SERVICE	00	1,308 K
svchost.exe	SYSTEM	00	10,700 K
svchost.exe	NETWORK SERVICE	00	2,272 K
svchost.exe	SYSTEM	00	2,188 K
lsass.exe	SYSTEM	00	1,220 K
services.exe	SYSTEM	00	2,724 K
winlogon.exe	SYSTEM	00	752 K

Select Columns

Select the columns that will appear on the Process page of the Task Manager.

- Image Name
- PID (Process Identifier)
- CPU Usage
- CPU Time
- Memory Usage
- Memory Usage Delta
- Peak Memory Usage
- Page Faults
- USER Objects
- I/O Reads
- I/O Read Bytes
- Session ID
- User Name
- Page Faults Delta
- Virtual Memory Size
- Paged Pool
- Non-paged Pool
- Base Priority
- Handle Count
- Thread Count
- GDI Objects
- I/O Writes
- I/O Write Bytes
- I/O Other
- I/O Other Bytes

OK Cancel

```
D:\sploit\windows\pwdump2-orig>dir
Volume in drive D is DATA
Volume Serial Number is 81BD-0B36

Directory of D:\sploit\windows\pwdump2-orig

03/23/2005  11:11 AM    <DIR>          .
03/23/2005  11:11 AM    <DIR>          ..
08/23/1998  03:30 PM           9,472  pwdump2.c
06/08/1998  11:51 PM           3,431  pwdump2.dsp
08/23/1998  03:32 PM           1,619  pwdump2.h
08/23/1998  03:31 PM       11,001  sandump.c
06/07/1998  04:56 PM           3,634  sandump.dsp
08/23/1998  04:02 PM       46,080  pwdump2.exe
08/23/1998  04:02 PM       49,664  sandump.dll
09/03/1998  12:03 AM            800  readme.txt
            8 File(s)      125,701 bytes
            2 Dir(s)     460,820,480 bytes free
```

```
D:\sploit\windows\pwdump2-orig>pwdump2 552
Administrator:500:9a68c309fe4b6ac2aad3b435b51404ee:52008ee808983c65a34d4acc56016ec6:::
amwk:1003:d9807bb83a170cd1f7e62f36f8db5ae6:c8fca7c324e784c15a7440ffc49aca08:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:49823f929f91fca04dd0699a12e7facf:8ea03ea77cc1d60ed1906b347e610e0e:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:dc78539a3c85381c6b5f609d48d98efb:::
```

Simulation



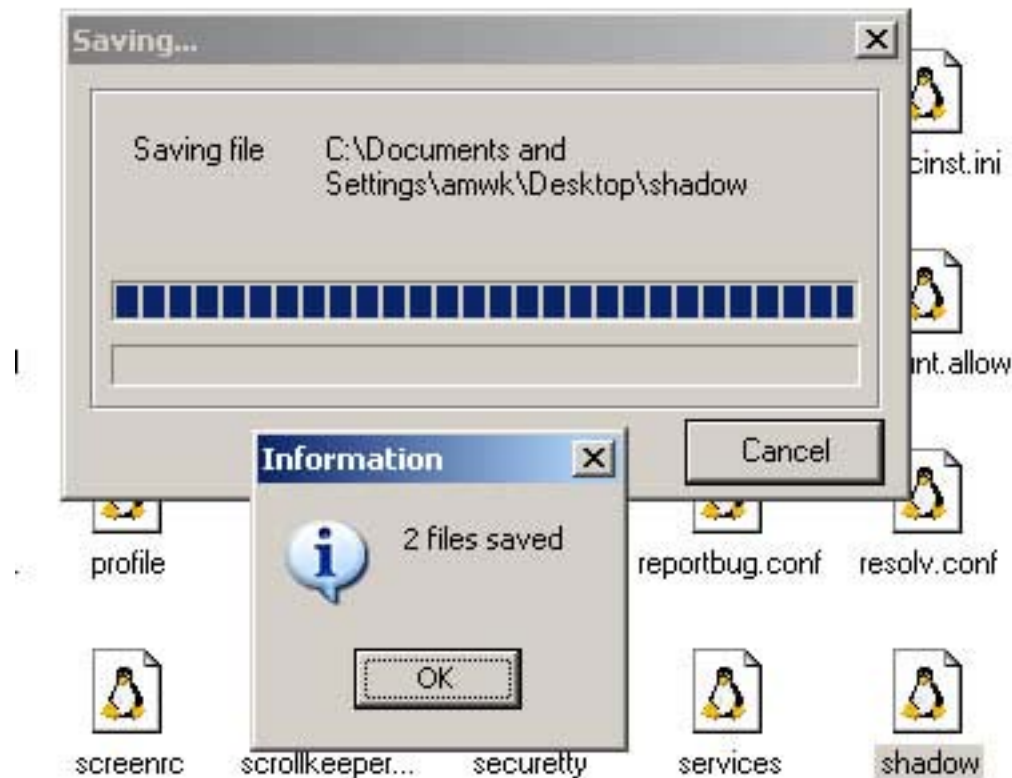
Cracking Linux Password

- ❖ Tools

 - ❖ **Unshadow**

 - ❖ **John the ripper** for cracking the hash

- ❖ Database password : passwd, *shadow*



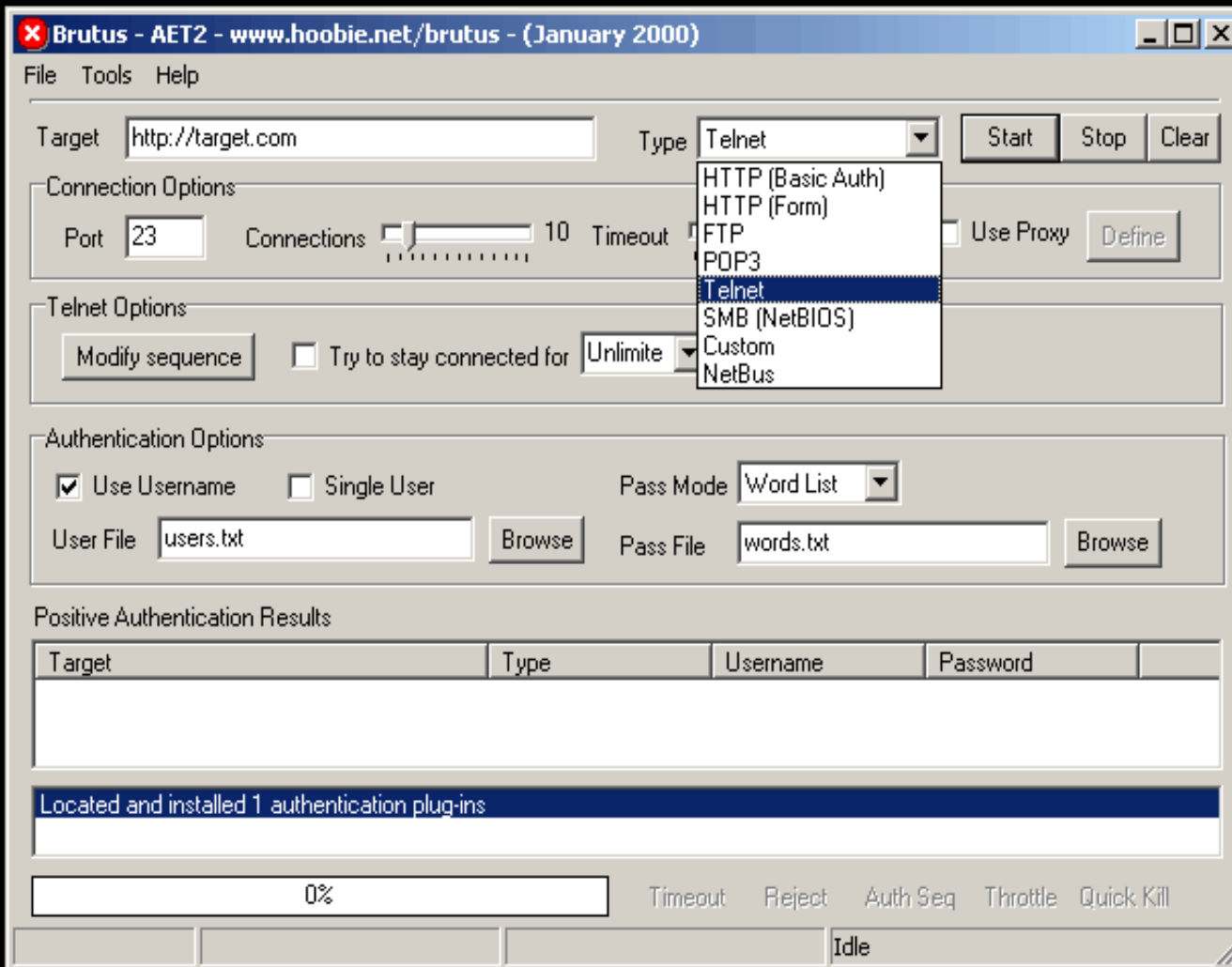
```
y3dips@hogwarts:~/linpass$ unshadow passwd shadow > pass.txt
y3dips@hogwarts:~/linpass$ john pass.txt -w:Wordlist.txt
Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/32])
dudul          (dudul)
asdfgh         (root)
guesses: 2   time: 0:00:00:06 100%  c/s: 3410  trying: asdfgh
```

Simulation



Remote Cracking

- ❖ Bruteforcing via network
- ❖ Slow speed
- ❖ Brutus, hydra, ssh crack, tftpd-bruteforce



Remote Cracking

Passive

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Passive Action?

- ❖ Browser Ability?
- ❖ Keylogger
- ❖ Application/Engine Hole
- ❖ Insecure protocol/line

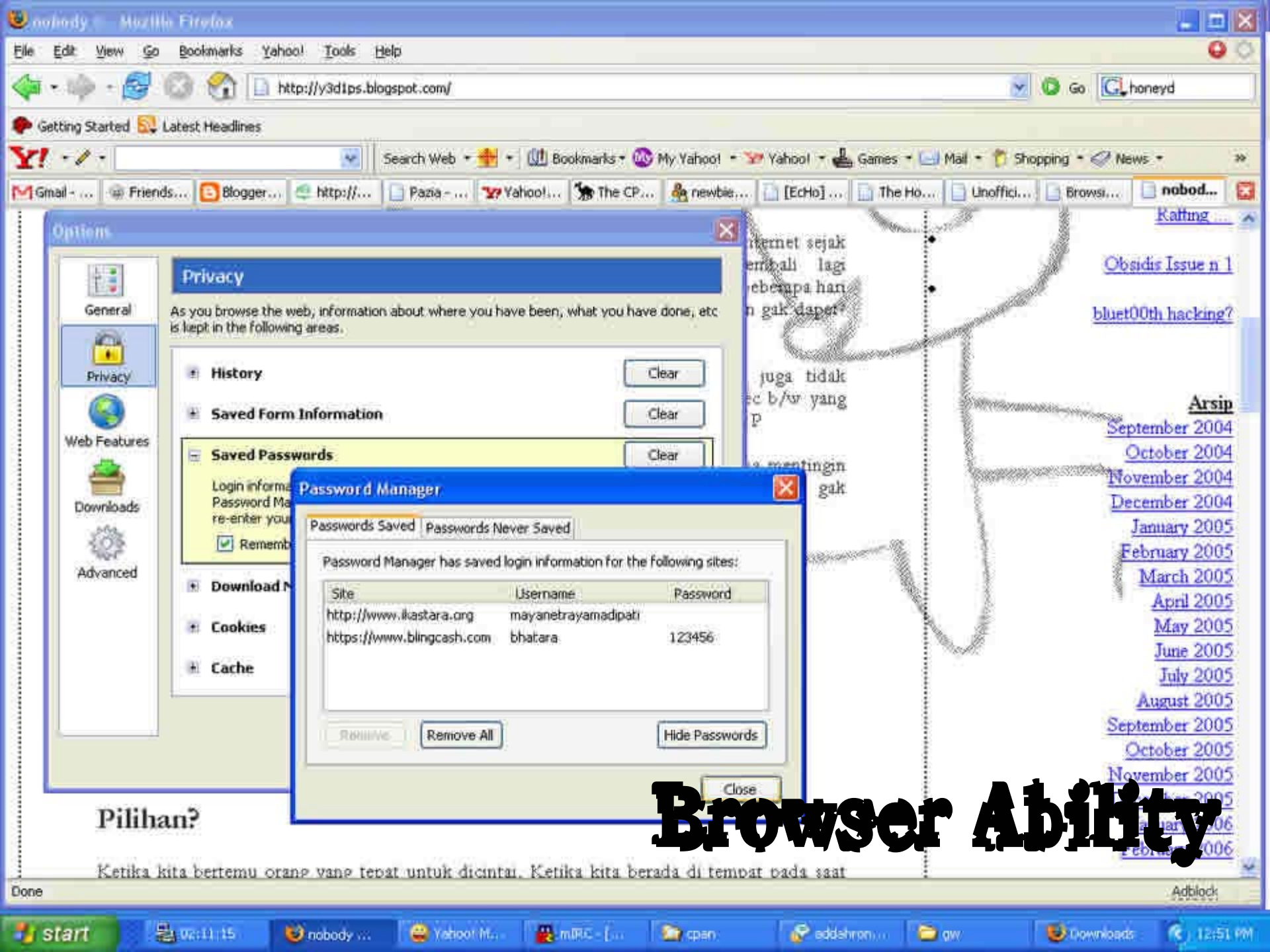
Browser Ability

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Browser Ability

- ❖ Wand/Remember Password
- ❖ History
- ❖ Cache ability
- ❖ etc



Privacy
As you browse the web, information about where you have been, what you have done, etc is kept in the following areas.

- History [Clear]
- Saved Form Information [Clear]
- Saved Passwords [Clear]

Password Manager

Passwords Saved | Passwords Never Saved

Password Manager has saved login information for the following sites:

Site	Username	Password
http://www.ikastara.org	mayanetrayamadipati	
https://www.blingcash.com	bhatara	123456

[Remove] [Remove All] [Hide Passwords] [Close]

Browser Ability

Pilihan?

Ketika kita bertemu orang yang tepat untuk dicintai. Ketika kita berada di tempat pada saat

Keylogger

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Keylogger

- ❖ Malicious Program
- ❖ Key stroke
- ❖ Passive tools

C:\Documents and Settings\amwk\Desktop\keylogger>dir

Volume in drive C has no label.
Volume Serial Number is 8864-CAF8

Directory of C:\Documents and Settings\amwk\Desktop\keylogger

02/09/2006	09:10 PM	<DIR>	.
02/09/2006	09:10 PM	<DIR>	..
02/09/2006	09:03 PM		23,552 klogger.exe
	1 File(s)		23,552 bytes
	2 Dir(s)		504,598,528 bytes free

C:\Documents and Settings\amwk\Desktop\keylogger>klogger.exe

C:\Documents and Settings\amwk\Desktop\keylogger>type klogger.txt

http://192.168.1.1
admindudulx
192.168.1.1
type kl.t

C:\Documents and Settings\amwk\Desktop\keylogger>

Keylogger

Bug in Application

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Bugs in Application

- ❖ Application/Engine Vulnerability
- ❖ Information disclosure
- ❖ e.g: phpnuke, postnuke, mambo

`$param{sql} = 'localhost'; $param{sqlusername} = 'root'; $param{sqlpassword} = 'k10r2c'; 1;`

Bug in Application

Insecure Line

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Insecure Line

- ❖ Plaintext protocol (http, tcp, smtp)
- ❖ Plaintext Data
- ❖ Sniff it & collect it (ethereal, ettercap, dsniff, etc)

http:// ← clear text

Mail helps me stay in touch.



New to Yahoo!?

Get a free **Yahoo! Mail** account – it's a breeze to stay connected and manage your busy life.

- ◆ **1GB of email storage**
Keep more of what's important to you
- ◆ **Powerful spam protection**
Read only the mail you really want
- ◆ **Get your mail anywhere**
All you need is a web connection

[Learn More](#) [Take a Tour](#)



[Sign Up Now](#)

Need more? Get **Yahoo! Mail Plus**.

Mail Plus offers personalized spam protection, a virtually unlimited 2GB of storage, POP access, and more for only **\$19.99/year**.

[Learn more](#)

Already have a Yahoo! ID?
Please sign in to read or send mail

Enter your ID and password

Yahoo! ID:

Password:

Remember my ID on this computer

[Sign In](#)

MODE: Standard | [Secure](#)

[Sign-in help](#)
[Forgot your ID or password?](#)

Insecure Line

y3d1ps

Conversation Options

y3d1ps x

(13:44:59) ammar_wk: woi, gw tau sekarang siapa yang ngebobol www.quabangget.com sama bug yang dia gunakan , kalo lo mau tau coba aja lo email gw secepatnya , nanti gw kirim hasil trace gw , btw untuk login ke private site gw coba pake user : elotau password : eloPASTIk4g4ktau; hehehhehehe 😄

(13:48:29) Requesting key...

(13:48:59) ammar_wk: woi, gw tau sekarang siapa yang ngebobol www.quabangget.com sama bug yang dia gunakan , kalo lo mau tau coba aja lo email gw secepatnya , nanti gw kirim hasil trace gw , btw untuk login ke private site gw coba pake

(13:48:59) ammar_wk: user : elotau password : eloPASTIk4g4ktau; hehehhehehe 😄

(13:53:35) y3d1ps: oke dech

Wz Bl Se Re In Tx se Ir

Insecure Line

root@heaven: /root

y3dips@heaven: /home/y3dips/egg

y3dips@heaven: ~/egg\$

Conversation Options

ammar_wk x

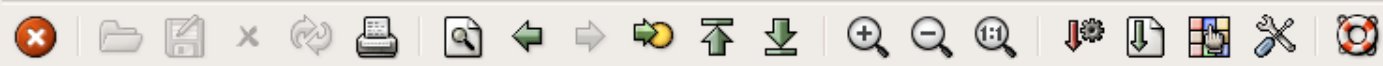
(13:45:27) ammar_wk: woi, gw tau sekarang siapa yang ngebobol <http://www.guabanget.com> sama bug yang dia gunakan , kalo lo mau tau coba aja lo email gw secepatnya , nanti gw kirim hasil trace gw , btw untuk login ke private site gw coba pake user : elotau password : eloPASTik4g4ktau; hehehhehehe 😄

(13:49:29) ammar_wk: woi, gw tau sekarang siapa yang ngebobol www.guabanget.com sama bug yang dia gunakan , kalo lo mau tau coba aja lo email gw secepatnya , nanti gw kirim hasil trace gw , btw untuk login ke private site gw coba pake

(13:49:29) ammar_wk: user : elotau password : eloPASTik4g4ktau; hehehhehehe 😄

War Bloc Sen Ren Info Tx: secure Rx: secure Send

Insecure Line



Filter: (ip.addr eq 216.155.193.167 and ip.addr eq 192.168.1.9) a + Expression... Clear Apply

Follow TCP stream

Stream Content

```

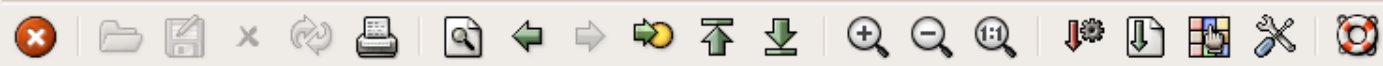
0 01 65 00 06 5a 55 aa 56 YMSG.... .e..ZU.V
1 6d 6d 61 72 5f 77 6b c0 ....1..a mmar_wk.
1 70 73 c0 80 39 37 c0 80 .5..y3dl ps..97..
7 6f 69 2c 20 67 77 20 74 1..14..w oi, gw t
2 61 6e 67 20 73 69 61 70 au sekar ang siap
e 67 65 62 6f 62 6f 6c 20 a yang n gebobol
0 3a 2f 2f 77 77 77 2e 67 .[lmhttp ://www.g
4 2e 63 6f 6d 1b 5b 78 6c uabanget .com.[xl
2 75 67 20 79 61 6e 67 20 m sama b ug yang
1 6b 61 6e 20 2c 20 6b 61 dia guna kan , ka
1 75 20 74 61 75 20 63 6f lo lo ma u tau co
c 6f 20 65 6d 61 69 6c 20 ba aja l o email
0 61 74 6e 79 61 20 2c 20 gw secep atnya ,
7 20 6b 69 72 69 6d 20 68 nanti gw kirim h
1 63 65 20 67 77 20 2c 20 asil tra ce gw ,
5 6b 20 6c 6f 67 69 6e 20 btw untu k login
1 74 65 20 73 69 74 65 20 ke priva te site
0 70 61 6b 65 20 75 73 65 gw coba pake use
4 61 75 20 70 61 73 73 77 r : elot au passw
c 6f 50 41 53 54 49 6b 34 ord : el oPASTIk4
0 20 68 65 68 65 68 68 65 g4ktau; hehehe
0 80 36 33 c0 80 3b 30 c0 hehe :P. .63..;0.
0 31 30 30 32 c0 80 31 c0 .64..0.. 1002..1.
0 80 .206..0. .
0 00 3b 00 4b 00 00 00 16 YMSG.... ;.K....
0 54 59 50 49 4e 47 c0 80 ....49.. TYPING..
0 5f 77 6b c0 80 31 34 c0 1 ammar_wk 14

```

Insecure Line

Save As Print Entire conversation (2189 bytes)

Filter out this stream Close



Filter: (ip.addr eq 192.168.1.9 and ip.addr eq 216.155.193.167) + Expression... Clear Apply

Time Source Destination Protocol Info

Follow TCP stream

Stream Content

```

00000E6E 59 4d 53 47 00 0c 00 00 01 6a 00 06 5a 55 aa 56 YMSG.... .j..ZU.V
00000E7E 00 00 00 00 31 c0 80 61 6d 6d 61 72 5f 77 6b c0 ....1..a mmar_wk.
00000E8E 80 35 c0 80 79 33 64 31 70 73 c0 80 39 37 c0 80 .5..y3d1 ps..97..
00000E9E 31 c0 80 31 34 c0 80 2a 2a 2a 20 45 6e 63 72 79 1..14..* ** Encry
00000EAE 70 74 65 64 20 3a 3a 20 4b 65 79 3a 20 50 72 6f pted :: Key: Pro
00000EBE 74 20 4e 53 53 20 31 2e 30 3a 20 4c 65 6e 20 32 t NSS 1. 0: Len 2
00000ECE 34 39 3a 69 70 47 6a 6d 51 56 41 57 47 54 4e 62 49:ipGjm QVAWGTNb
00000EDE 45 67 53 79 57 34 55 6e 39 64 39 64 51 65 6d 56 EgSyw4Un 9d9dQemV
00000EEE 46 67 78 2c 4d 49 47 66 4d 41 30 47 43 53 71 47 Fgx,MIGf MAOGCSqG
00000EFE 53 49 62 33 44 51 45 42 41 51 55 41 41 34 47 4e SIb3DQEB AQUAA4GN
00000F0E 41 44 43 42 69 51 4b 42 67 51 44 6a 52 2b 38 63 ADCBiQKB gQDjR+8c
00000F1E 64 67 6a 37 77 51 44 56 57 38 72 57 49 4b 45 62 dgj7wQDV W8rWIKEb
00000F2E 65 70 48 6a 47 31 7a 71 2b 2b 4b 2b 61 71 7a 69 epHjG1zq ++K+aqzi
00000F3E 33 50 53 62 2b 39 49 49 57 6d 58 54 38 4a 34 6b 3PSb+9II WmXT8J4k
00000F4E 74 58 47 30 46 65 35 37 2f 4d 53 34 59 34 6c 6e tXG0Fe57 /MS4Y4ln
00000F5E 33 34 76 75 38 38 7a 62 48 59 4c 79 69 69 73 66 34vu88zb HLYiisf
00000F6E 38 72 6d 4d 62 58 2b 6f 4f 76 78 43 75 6b 62 4e 8rmMbx+o OvxCukbN
00000F7E 4e 62 61 47 79 63 76 45 71 4d 46 59 61 38 37 74 NbaGycvE qMFYa87t
00000F8E 4a 42 4c 45 51 5a 41 69 2b 72 55 65 48 58 4b 35 JBLEQZAI +rUeHXK5
00000F9E 45 32 55 34 65 5a 6a 46 77 52 34 51 6e 72 4f 48 E2U4eZjF wR4Qnr0H
00000FAE 31 64 2b 75 71 72 67 79 6b 38 72 75 62 2f 30 55 1d+uqrgy k8rub/0U
00000FBE 75 34 35 4c 30 51 49 44 41 51 41 42 c0 80 36 33 u45L0QID AQAB..63
00000FCE c0 80 3b 30 c0 80 36 34 c0 80 30 c0 80 31 30 30 ..;0..64 ..0..100
00000FDE 32 c0 80 31 c0 80 32 30 36 c0 80 30 c0 80 2..1..0 6..0..

```

Insecure Line

Save As Print Entire conversation (5975 bytes)

Filter out this stream Close



Survive

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>



Survive

- ❖ Using a better pass phrase
- ❖ Using secure line/protocol
- ❖ **Encryption**
- ❖ Securing tools (**firewall, antivirus**)
- ❖ Update info
- ❖ E.t.c

Discussion

Ahmad Muammar W. K.
<http://google.com/search?q=y3dips>