

How to Hack a System

John Green
Rodney Tillotson
JANET-CERT



Why?

- Target ac.uk because
 - Large Bandwidth
 - Some fast, large systems
 - Liberal filters
- Why?
 - Exchange of copyright/illegal material
 - Bandwidth allows powerful DoS



Who?

- Espionage
- Professional Hackers
- Script kiddies
- The “threat from within”
- Warez groups



How?

- Two scenarios
 - **Exploit chosen**
Task: find exploitable targets <- more likely in ac.uk
 - **Target chosen**
Task: find exploit to gain entry



Recon (non-invasive)

- Websearch
 - google.com for target.ac.uk
 - google.com for exploitable XYZ (e.g perl.exe)
 - groups.google.com for postings from @target.ac.uk
 - groups.google.com for exploitable XYZ product
- Network (whois)
 - Find netblocks for target organisation
 - Find other netblock (linked to same handle)



Recon (non-invasive)

- DNS
 - Check NS, MX records (dig)
 - Names often reveal information
 - Eg exchange.target.ac.uk, cisco.target.ac.uk
 - Zone transfers. Alternatively one-by-one
 - Version/type of nameserver using chaos
 - Eg BIND: “8.3.3-REL” or “[FORMERR] Guess: djbdns' tinydns”
 - TXT or HINFO records sometimes reveal extra



Recon (Invasive)

- Scanning
 - Ping sweep. Quickly tells what machines are up
 - Nmap -sP -PI 192.168.0.0/16 (also use different -P?)
 - Traceroute. Identifies node along packets path.
 - TCP scanning
 - Nmap -sT 192.168.0.0/16 (basic connect)
 - -sS offers half-open scanning
 - -sF, -sX, -sN, -sI, -sA enable more advanced methods
 - Optimised scanning methods increase performance (distributed, asynchronous)



Nmap examples

```
$ nmap epia.target.ac.uk
```

Starting nmap V. 3.00 (www.insecure.org/nmap/)

Interesting ports on epia.target.ac.uk (172.16.1.1):

(The 1598 ports scanned but not shown below are in state: filtered)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http

Nmap run completed -- 1 IP address (1 host up)
scanned in 171 seconds



Recon (Invasive)

- UDP scanning
 - More unreliable than TCP scanning
 - ICMP port unreachable if closed, no reply if open.
 - Firewalls can easily confuse results.
- OS fingerprinting
 - Different IP stacks behave in different ways.
 - Either, fire packets at target and see how it responds
 - Or, use service legitimately and just watch
 - Can also be used to identify attacker



Recon (Invasive)

- Banner grabbing
 - Program, OS, version, build date, current date, hostname, patch level,
 - 220 exchange.target.ac.uk ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2656.59) ready
 - HTTP/1.1 400 Bad Request
Date: Sun, 02 Mar 2003 21:10:49 GMT
Server: Apache Connection: close
Content-Type: text/html; charset=iso-8859-1

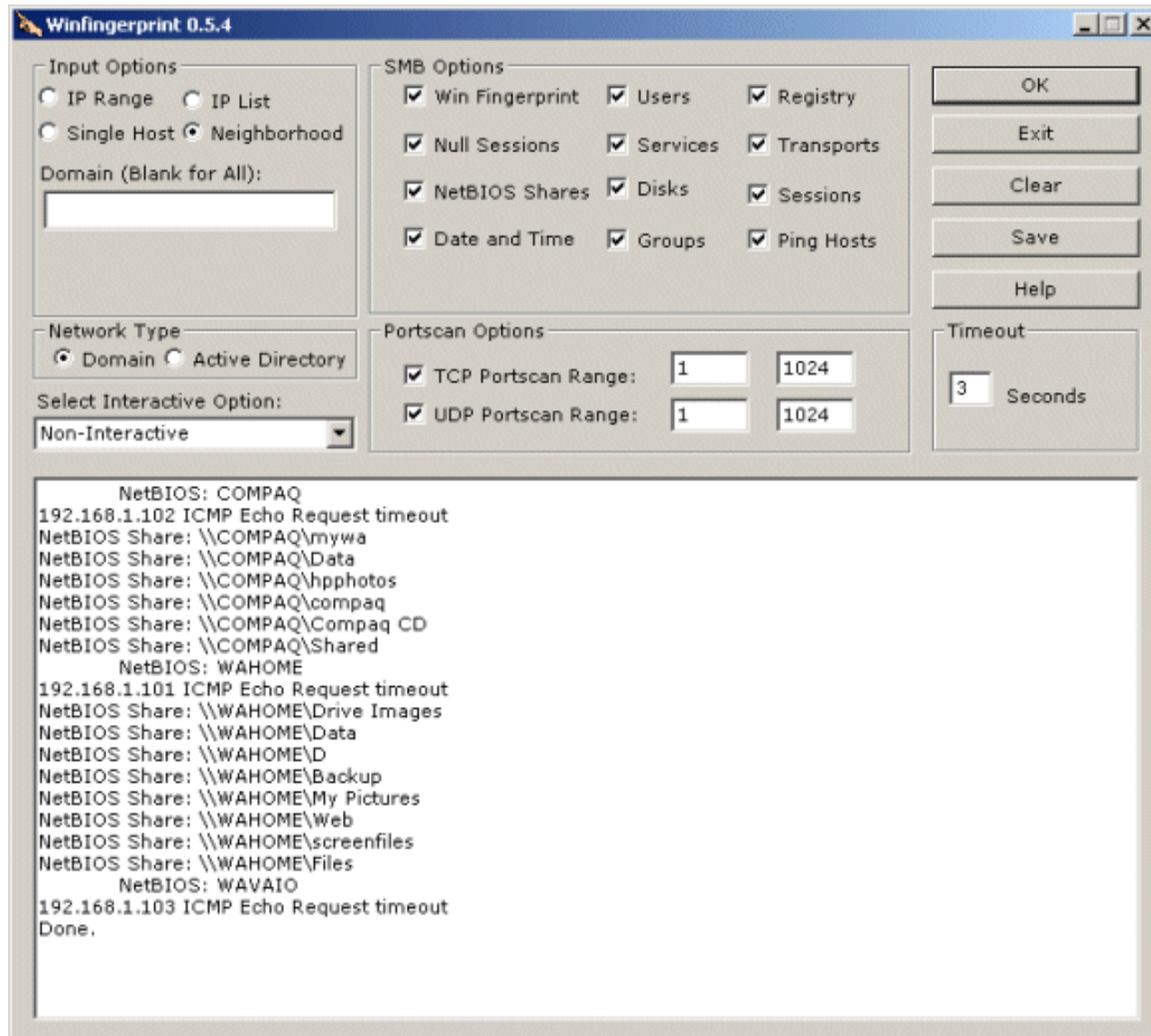


Enumeration

- NT/XP
 - ResKits
 - Winfingerprint
 - Xscan
 - Sid2user, user2sid
- UNIX
 - Finger, rpcinfo, showmount, snmp, ident



Winfingerprint



Hacking Computers – How?

- Inject code into running process
 - **Buffer Overflows**
User sends more data than buffer can hold, overwriting memory
 - **Format String**
Missing format string in printf allows use of %n and %x to manipulate stack
- Privilege escalation
 - Race conditions
 - Kernel exploit



Examples – Windows

- Internet Information Services (IIS)
- Microsoft Data Access Components (MDAC)
- Microsoft SQL Server
- NETBIOS -- Unprotected Windows Shares
- Anonymous Logon -- Null Sessions
- LAN Manager Authentication -- Weak LM Hashing
- General Windows Authentication -- Weak Passwords
- Internet Explorer
- Remote Registry Access
- Windows Scripting Host



Examples – Unix

- Remote Procedure Calls (RPC)
- Apache Web Server
- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- File Transfer Protocol (FTP)
- R-Services -- Trust Relationships
- Line Printer Daemon (LPD)
- Sendmail
- BIND/DNS
- General Unix Authentication –Weak Passwords



Post Compromise

- Hide presence (rootkit)
- Secure machine from further attack
- Ensure easy access in future
- Remove evidence of activity
- Look for further information on machine/network

Hacking Network devices

- Number of services enabled by default
 - SNMP, telnet, web, tftp
- Same problems as “Hacking Computers”
- Network devices are often fire and forget, designed to work straight out the box
 - Default passwords
 - Backdoors
 - Often missed from upgrade schedule



Hacking Firewalls

- Detection
 - Traceroute
Identify intermediate network infrastructure
 - Hping2
Can use other protocols
 - Firewalk
Similar, designed specifically to test firewall rules
 - Proxies
Open proxies give anonymity and internal access



Hacking People

- Trojaned code
 - Email, p2p, website “Please run me - mp3.exe”
- Information disclosure
 - Web “Remote access is available via....”
- IRC
- Email forgery
 - Email “Please send your username/password to..”



Summary

- .ac.uk rarely a specific target
- Often opportunists looking for a specific vulnerability
- Sites frequently scanned for specific services and versions
- Once a machine has been compromised attackers can exploit trust relationships
- Machines put to quite mundane use



?

