UNIVERSITÄT SIEGEN

**Lehstuhl IT-Sicherheitsmanagment**
**Prof. Dr. Kesdogan**

# Exercise 2: Code Doctor

## Anglenna Imladris

Zusammen mit deinem Zertifikat erhältst du eine Konfigurationsdatei für OpenVPN. Eine kleine Anpassung und der Brandywein ist für dich überquert. Ein Freund wird dir den Namen deines Kontaktes im "Springenden Pony" nennen. Eine unruhige Nacht im "Springenden Pony" später befindest du dich schon wieder auf der Strasse.[1].

In dem Netz findet sich ein Server mit offenem Port 2342/TCP. Folge den Anweisungen des seltsamen Fremden. Und der Weg über die Lautwasser wird dir geöffnet werden und deine Verfolger werden abgeschüttelt.

Nimm dein Rivendel in Beschlag. Auf der Maschine findet sich ein rudimäres System. Wie auf jedem frisch übernommenen System wirst du dir jetzt erst einmal deinen Brückenkopf ausbauen müssen. (Siehe Aufgabe .

## Die Minen von Moria

Der Weg über die Berge war verschneit, Saurons Auge wachte über die Pässe, es gab keinen Weg nach Süden als durch die Tunnel von Moria. An einigen Stellen ist der Weg allerdings verschüttet und muss von neuem gebohrt werden.

Es gibt mehrere Varianten einen Tunnel von innen nach aussen zu graben, sinnvoller ist es aber den bestehenden Tunnel von aussen nach innen zu nutzen. Zeige deine Meisterschaft indem du Gleise in den Tunnel legst, über welches das Internet normal verwendet werden kann.

Genauer: sorge dafür, dass `apt-get update` und `apt-get upgrade` normal ablaufen.

## Die Schlacht um Rohan

Deine Maschine ist einsatzbereit, brennt vor Energie, aber der Feind ist nicht zu sehen. Zeit seine Späher auszuschicken und nach versprengten Ork-Truppen ausschau zu halten. Passworte die dir den Zugang zum feindlichen Feldlager öffenen sind natürlich gern gesehen.

## Der Stufenstapel zu Torech Ungol

Der spassige Teil der Hintergrundinformation findet sich hier: `http://phrack.com/issues.html?issue=49&id=14#article`. Etwas aktueller wird es unter `http://paulmakowski.wordpress.com/2011/01/25/smashing-the-stack-in-2011`.

[1] OpenVPN Server bei 141.99.96.200

Kontakt: `fischer@wiwi.uni-siegen.de`

```c
#include <stdio.h>

void manipulate(char *buffer) {
  char newbuffer[10];
  char *ptr = newbuffer;
  while ((*ptr++ = *buffer++) != NULL);
}

int main() {
  char ch, buffer[4096];
  int i=0;
  while ((buffer[i++] = getchar()) != '\n');
  i=1;
  manipulate(buffer);
  i=2;
  printf("The value of i is: %d\n",i);
  return 0;
}
```

Es gibt einen Punkt für einen DoS, fünf Punkte für einen Weg die Rücksprungadresse der `manipulate` Funktion und 15 Punkte für einen funktionierenden Shellcode. (Ausserdem geben wir 20 Punkte, wenn der Shellcode eine Verbindung zu einem externen Host aufbaut.) Ihr dürft für diese Aufgabe gerne etwaige Stack-Protection-Mechanismen abschalten.

## Bonus: Beutelsend Kaminfeuerrätsel

Hobbits am Kaminfeuer erzählen sich wilde Geschichten, Abenteuer vom heimischen Hackbrett und wackeln dabei am liebsten mit ihrem grossen 'C'. Verschachtelt sind ihre Höhlen allemal.

Welchen Wert gibt das folgende Programm zurück, und warum ist das nicht falsch?

```c
int (*getFunc(int b))(int)
{
  int test(int a)
  {
    return a + b;
  }
  return &test;
}

int main()
{
  int (*f)(int) = getFunc(4);
  getFunc(6);
  return f(3);
}
```