



BURSA ULUDAĞ ÜNİVERSİTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

ROOTKİT SALDIRISI TESPİTİ VE ÖNLEM
YÖNTEMLERİ

HAZIRLAYANLAR:
ECE JILTA
HATİCE FEYZA BENAL

Rootkit Tespiti ve Önlem Yöntemleri

Rootkit, bilgisayar korsanlarının hedef cihaza erişmesini ve bu cihazı kontrol etmesini sağlamak için tasarlanmış bir kötü amaçlı yazılım türüdür. Çoğu rootkit, yazılımları ve işletim sistemlerini etkiler. Ancak bazıları bilgisayarınızın donanımını ve aygıt yazılımını da etkileyebilir. Rootkit'ler varlıklarını gizlemede uzmandır ancak gizli kaldıkları süre boyunca etkinliklerine devam ederler.

Bilgisayar korsanları hedef makinelere rootkit'ler yüklemek için çeşitli yöntemler kullanır:

1. En sık kullanılan yöntem kimlik avı veya başka bir sosyal mühendislik saldırısı türü aracılığıyla saldırı gerçekleştirmektir. Kurbanlar, makinelerinde çalışan diğer işlemlerde gizlenen ve korsanlara neredeyse tüm işletim sistemi özelliklerinin kontrolünü veren kötü amaçlı yazılımları farkında olmadan indirip yükleyebilir.
2. Bir diğer yöntemi de yazılımdaki veya güncelleştirilmemiş bir işletim sistemindeki bir güvenlik açığından yararlanarak rootkit'i bilgisayara sızdırmaktır.
3. Kötü amaçlı yazılımlar ayrıca virüslü PDF'ler, korsan medya dosyaları veya şüpheli üçüncü taraf mağazalardan alınan uygulamalar gibi dosyaların içinde de gelebilir.

Rootkit Tespit Simülasyonu

Projemiz, rootkit tespiti ve önlemeye ilişkin bir simülasyonu temsil etmektedir. Gerçek bir rootkit tespit ve önleme mekanizması değildir, sadece konuya ilişkin bir örnektir. Sanal sürücü üzerinden projeyi yürüttük ve Windows Form uygulaması olarak tasarladık. Form üzerindeki "Rootkitleri Tespit Et" düğmesine tıklandığında, tarama işlemi başlar. Tarama işlemi, işletim sisteminde çalışan işlemleri kontrol eder ve potansiyel rootkitleri bulmaya çalışır. Potansiyel rootkitler tespit edildiğinde, bu bilgiler metin kutusunda görüntülenir. Her potansiyel rootkit için işlem adı ve dosya yolu gösterilir. Simülasyon potansiyel rootkit tespit ederse etkisiz hale getirebilir ya da karantinaya alabilir. Tarama işlemi tamamlandıktan sonra da simülasyonun bir mesajla tamamlandığı ve sonuçların görüntülendiği bildirilir.

Simülasyon Kodu:

```
using System;
using System.Diagnostics;
using System.Threading;
using System.Windows.Forms;

namespace RootkitDetectionSimulation
{
    public class Program
    {
        [STAThread]
        static void Main()
        {
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(new FormRootkitDetection());
        }
    }

    public partial class FormRootkitDetection : Form
    {
        private TextBox txtResults;
        private Button btnDetectRootkits;

        public FormRootkitDetection()
        {
            InitializeComponent();
        }

        private void InitializeComponent()
        {
            this.txtResults = new TextBox();
            this.btnDetectRootkits = new Button();

            this.SuspendLayout();

            // txtResults TextBox kontrolünün özelliklerini ayarla
            this.txtResults.Location = new System.Drawing.Point(12, 12);
            this.txtResults.Multiline = true;
            this.txtResults.ScrollBars = ScrollBars.Vertical;
            this.txtResults.Size = new System.Drawing.Size(400, 200);
            this.txtResults.Name = "txtResults";

            // btnDetectRootkits Button kontrolünün özelliklerini ayarla
            this.btnDetectRootkits.Location = new System.Drawing.Point(12, 218);
            this.btnDetectRootkits.Size = new System.Drawing.Size(150, 30);
            this.btnDetectRootkits.Text = "Rootkitleri Tespit Et";
            this.btnDetectRootkits.Click += new
System.EventHandler(this.btnDetectRootkits_Click);

            // Form özelliklerini ayarla
            this.ClientSize = new System.Drawing.Size(424, 260);
            this.Controls.Add(this.btnDetectRootkits);
            this.Controls.Add(this.txtResults);
            this.Name = "FormRootkitDetection";
            this.Text = "Rootkit Detection Simulation";

            this.ResumeLayout(false);
            this.PerformLayout();

            this.KeyPreview = true; // Klavye olaylarını formda işlemek için KeyPreview'ı true
olarak ayarla
            this.KeyDown += new KeyEventHandler(FormRootkitDetection_KeyDown); // KeyDown
olayını formda yakala
        }

        private void btnDetectRootkits_Click(object sender, EventArgs e)
        {
            // Rootkit tespitini gerçekleştir
            CheckRootkit();
        }

        private void CheckRootkit()
        {

```

```

txtResults.Clear();

// İşlem kontrolü
Process[] processes = Process.GetProcesses();
int maxProcessesToScan = 1000; // Taramak için en fazla işlem sayısı
int scannedProcessCount = 0; // Taranan işlem sayısı
int maxDurationSeconds = 60; // Maksimum işlem süresi (saniye cinsinden)
bool rootkitDetected = false; // Rootkit tespit edilip edilmediğini takip etmek
için bir bayrak

Stopwatch stopwatch = new Stopwatch();
stopwatch.Start();

foreach (Process process in processes)
{
    if (scannedProcessCount >= maxProcessesToScan ||
stopwatch.Elapsed.TotalSeconds >= maxDurationSeconds)
        break;

    try
    {
        string processName = process.ProcessName;
        string processPath = process.MainModule.FileName;

        if (processName.ToLower().Contains("rootkit") ||
processPath.ToLower().Contains("rootkit"))
        {
            string result = "Potansiyel bir rootkit tespit edildi:\n";
            result += "İşlem Adı: " + processName + "\n";
            result += "İşlem Yolu: " + processPath + "\n";
            result += "----\n";

            txtResults.AppendText(result);

            rootkitDetected = true;

            // Rootkit'i etkisiz hale getirmek veya kaldırmak için burada ilgili
            kodu ekleyebilirsiniz.
            RemoveRootkit(process);

            // Rootkit'i karantinaya almak için burada ilgili kodu
            ekleyebilirsiniz.
            // Örneğin:
            // QuarantineRootkit(process);
        }

        scannedProcessCount++;
    }
    catch (Exception)
    {
        // İşlem alınamazsa veya yoksa devam et
    }
}

stopwatch.Stop();

if (!rootkitDetected)
{
    txtResults.AppendText("Rootkit bulunamadı. \n");
}
else
{
    txtResults.AppendText("Rootkit tespit edildi.\n");

    // Alınan önlemlerle ilgili bir mesajı burada ekle
    txtResults.AppendText("Rootkit etkisiz hale getirildi veya kaldırıldı.\n");
}

txtResults.AppendText("Rootkit taraması tamamlandı.\n");
}

```

ROOTKİT BULUNAMADIĞINDA

The screenshot displays the Visual Studio IDE with a Windows Forms application named 'WinFormsApp2' in the 'Debug' configuration. The code in 'Form1.cs' shows a method 'CheckRootkit()' that simulates a rootkit detection process. The method logs the process path, checks for rootkit presence, and updates the 'txtResults' label. A 'Rootkit Detection Simulation' dialog box is open, displaying the message 'Rootkit bulunamadı. Rootkit taraması tamamlandı.' (Rootkit not found. Rootkit scan completed.) and a 'Rootkitleri Tespit Et' button. The Visual Studio interface includes the Solution Explorer, Code Editor, and Output Window. The Output Window shows the execution log of the application.

```
117 result += "İşlem Yolu: " + processPath + "\n";
118 result += "----\n";
119
120 txtResults.AppendText(result);
121
122 rootkitDetected = true;
123
124 // Rootkit'i etkisiz hale getirmek veya kaldırmak için burada ilgili kodu ekleyebilirsiniz.
125 RemoveRootkit(process);
126
127 // Rootkit'i karantinaya almak için burada ilgili kodu ekleyebilirsiniz.
128 // QuarantineRootkit(process);
129
130 }
131
132 scannedProcessCount++;
133
134 catch (Exception)
135 {
136     // İşlem alınmazsa veya yoksa devam et
137 }
138
139 stopwatch.Stop();
140
141 if (!rootkitDetected)
142 {
143     txtResults.AppendText("Rootkit bulunamadı\n");
144 }
145 else
146 {
147     txtResults.AppendText("Rootkit tespit edildi.\n");
148
149     // Alınan önlemlerle ilgili bir mesajı burada ekle
150     // Örneğin:
151     // txtResults.AppendText("Rootkit etkisiz hale getirildi veya kaldırıldı.\n");
152 }
153
```

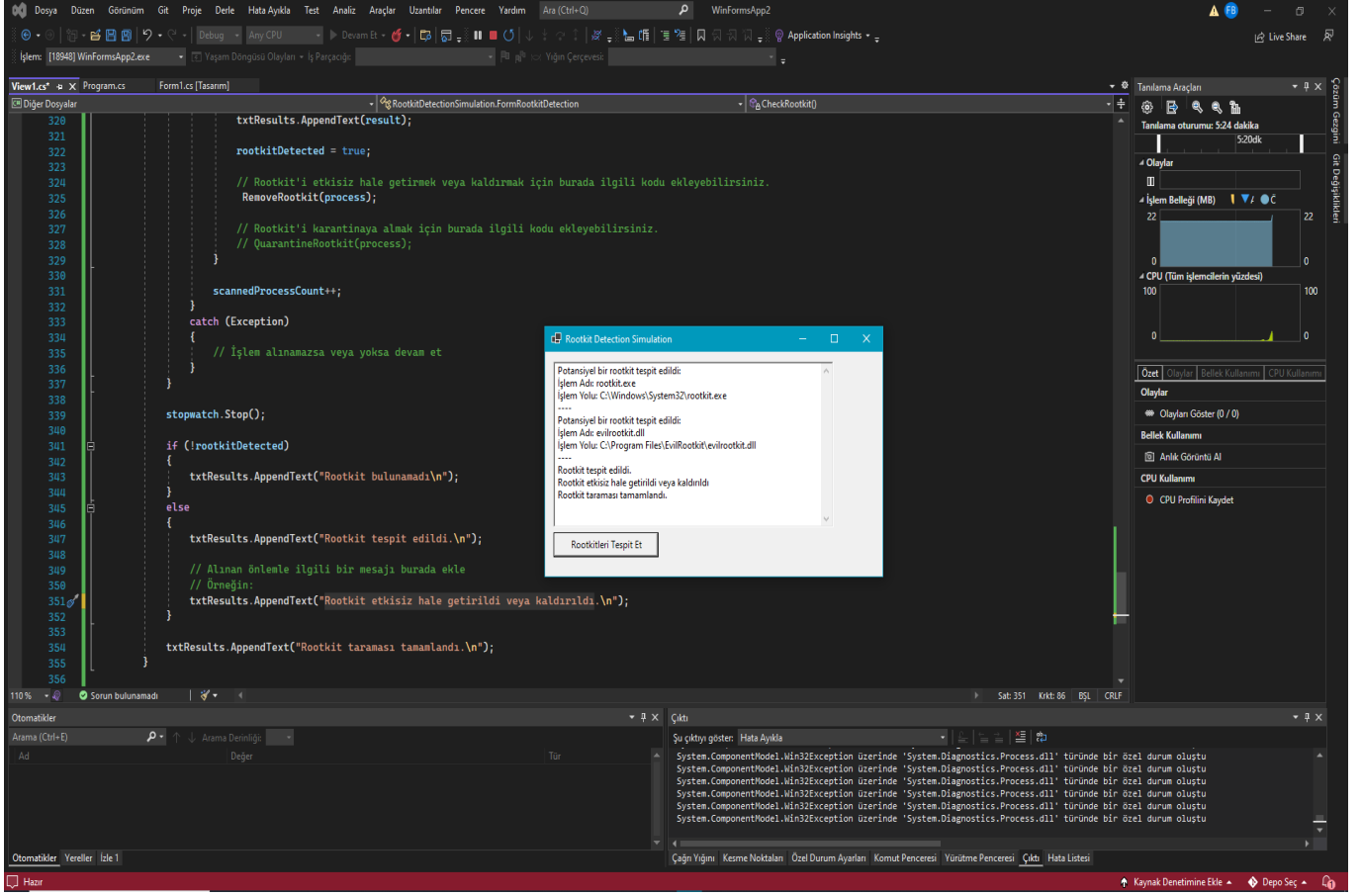
Rootkit bulunamadı.
Rootkit taraması tamamlandı.

Rootkitleri Tespit Et

Output Window:

```
Şu çıktıyı göster: Hata Ayıkla
'WinFormsApp2.exe' (CoreCLR: clrhost): 'C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.16\System.Collections.NonGeneric.
'WinFormsApp2.exe' (CoreCLR: clrhost): 'C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.16\System.ComponentModel.TypeConv
'WinFormsApp2.exe' (CoreCLR: clrhost): 'C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.16\System.ComponentModel.dll' yük
0x34 4c nancars0 0 (0x0) koduyla çıktı.
```

ROOTKİT TESPİT EDİLDİĞİNDE



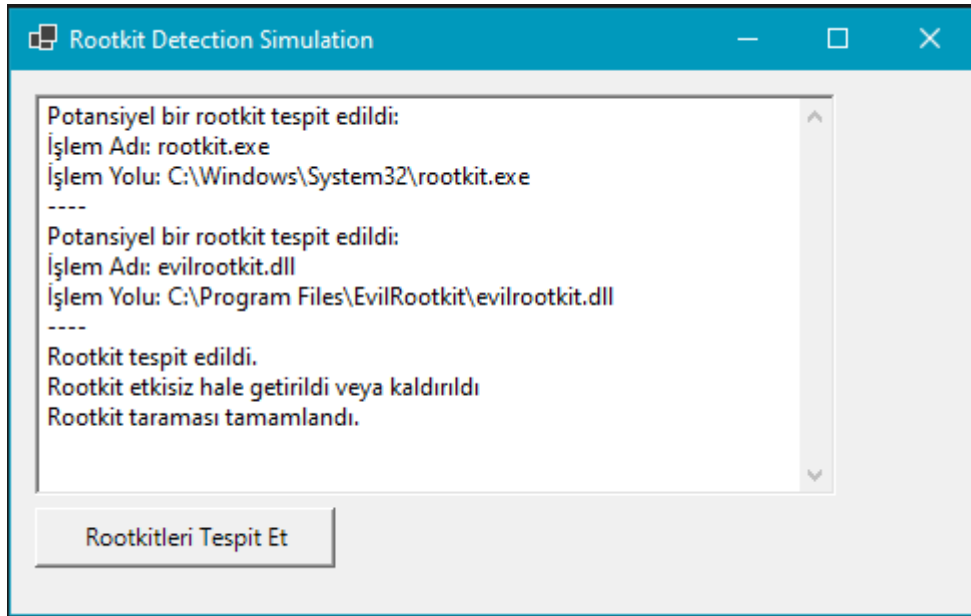
The screenshot shows a Visual Studio IDE with a C# project named 'WinFormsApp2'. The code in 'Program.cs' is as follows:

```
320 txtResults.AppendText(result);
321
322 rootkitDetected = true;
323
324 // Rootkit'i etkisiz hale getirmek veya kaldırmak için burada ilgili kodu ekleyebilirsiniz.
325 RemoveRootkit(process);
326
327 // Rootkit'i karantinaya almak için burada ilgili kodu ekleyebilirsiniz.
328 QuarantineRootkit(process);
329
330 scannedProcessCount++;
331
332 catch (Exception)
333 {
334     // İşlem alınmazsa veya yoksa devam et
335 }
336
337
338
339 stopwatch.Stop();
340
341 if (!rootkitDetected)
342 {
343     txtResults.AppendText("Rootkit bulunamadı.\n");
344 }
345 else
346 {
347     txtResults.AppendText("Rootkit tespit edildi.\n");
348     // Alınan önlemlerle ilgili bir mesajı burada ekle
349     // Örneğin:
350     txtResults.AppendText("Rootkit etkisiz hale getirildi veya kaldırıldı.\n");
351 }
352
353 txtResults.AppendText("Rootkit taraması tamamlandı.\n");
354
355
356
```

The 'Rootkit Detection Simulation' dialog box displays the following information:

- Potansiyel bir rootkit tespit edildi:
İşlem Adı: rootkit.exe
İşlem Yolu: C:\Windows\System32\rootkit.exe
- Potansiyel bir rootkit tespit edildi:
İşlem Adı: evilrootkit.dll
İşlem Yolu: C:\Program Files\EvilRootkit\evilrootkit.dll
- Rootkit tespit edildi.
Rootkit etkisiz hale getirildi veya kaldırıldı
Rootkit taraması tamamlandı.

The dialog box has a button labeled 'Rootkitleri Tespit Et'.



The dialog box titled 'Rootkit Detection Simulation' contains the following text:

Potansiyel bir rootkit tespit edildi:
İşlem Adı: rootkit.exe
İşlem Yolu: C:\Windows\System32\rootkit.exe

Potansiyel bir rootkit tespit edildi:
İşlem Adı: evilrootkit.dll
İşlem Yolu: C:\Program Files\EvilRootkit\evilrootkit.dll

Rootkit tespit edildi.
Rootkit etkisiz hale getirildi veya kaldırıldı
Rootkit taraması tamamlandı.

At the bottom of the dialog box is a button labeled 'Rootkitleri Tespit Et'.